Nelson Remolina Angarita
Manuel Miguel Tenorio Adame
Gustavo Arnulfo Quintero Navas

DE LA RESPONSABILIDAD DEMOSTRADA EN LAS FUNCIONES MISIONALES DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL

Hacia un programa de gestión de datos personales y la consolidación de un buen gobierno corporativo en el tratamiento de esa clase de información

REGISTRADURÍA NACIONAL DEL ESTADO CIVIL
cedae Centro de Estudios en Democracia y Asuntos Electorales
RA REMOLINA ANGARITA CONSULTORES

DE LA RESPONSABILIDAD DEMOSTRADA EN LAS FUNCIONES MISIONALES DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL

Hacia un programa de gestión de datos personales
y la consolidación de un buen gobierno corporativo
en el tratamiento de esa clase de información

EDITORIAL TEMIS
OBRAS JURÍDICAS

NELSON REMOLINA ANGARITA
MANUEL MIGUEL TENORIO ADAME
GUSTAVO ARNULFO QUINTERO NAVAS

DE LA RESPONSABILIDAD DEMOSTRADA EN LAS FUNCIONES MISIONALES DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL

Hacia un programa de gestión de datos personales
y la consolidación de un buen gobierno corporativo
en el tratamiento de esa clase de información

REGISTRADURÍA NACIONAL DEL ESTADO CIVIL
cedae Centro de Estudios en Democracia y Asuntos Electorales
RA REMOLINANGARITA CONSULTORES

De la responsabilidad demostrada en las funciones misionales de la Registraduría Nacional del Estado Civil: Hacia un programa de gestión de datos personales y la consolidación de un buen gobierno corporativo en el tratamiento de esa clase de información.

Registraduría Nacional del Estado Civil©. Centro de Estudios en Democracia y Asuntos Electorales (CEDAE). 2018.

216 páginas; 16.5 x 23.5 cm.
ISBN: 978-958-35-1183-7

Tratamiento de datos personales / Supremacía Constitucional / dato personal / Responsabilidad demostrada / Accountability / Programa integral de gestión de datos personales / Privacy management programmes.

Asistentes de investigación:
• Luisa Fernanda Álvarez Zuluaga
• María Mónica Pérez López

Primera edición: Bogotá D. C., junio de 2018

ISBN 978-958-35-1183-7
2952 20180026300

Centro de Estudios en Democracia y Asuntos Electorales (CEDAE)

Diagramación y diseño de cubierta:
Editorial Temis S. A., 2018

Impresión: Editorial Nomos

Impreso y hecho en Colombia
Printed and made in Colombia

REGISTRADURÍA
NACIONAL DEL ESTADO CIVIL

JUAN CARLOS GALINDO VÁCHA
Registrador Nacional del Estado Civil

JAIME HERNANDO SUÁREZ BAYONA
Registrador Delegado en lo Electoral

LUIS FERNANDO CRIALES GUTIÉRREZ
Registrador Delegado para el Registro Civil y la Identificación

ERIKA SARQUIZ MATTA
Coordinadora Grupo de Trabajo CEDAE

Nelson Remolina Angarita / Manuel Miguel Tenorio Adame
Gustavo Arnulfo Quintero Navas
Autores

Luisa Fernanda Álvarez Zuluaga / María Mónica Pérez López
Asistentes de Investigación

Bogotá, Colombia, 2018

PRESENTACIÓN

Las dos funciones misionales más importantes que el Estado colombiano le entrega a la Registraduría Nacional del Estado Civil están íntimamente relacionadas con el ejercicio de los derechos fundamentales de los colombianos a través de distintas vías, pero mediante un solo camino que es la democracia. Me refiero a las misiones electoral y registral que hoy después de 70 años de existencia de la institución se consolidan de manera efectiva para que los habitantes de este gran país las puedan ejercer como expresión de máxima libertad. Ningún colombiano concibe su día a día sin la certeza de la seguridad jurídica de los documentos y medios de registro que la Registraduría Nacional del Estado Civil le otorga para ejercer sus actividades. Desde las acciones más simples o más complejas, los instrumentos registrales que proporciona esta institución, brindan la certeza de la identificación de los ciudadanos frente a los entes privados y públicos.

El acompañamiento de la Registraduría Nacional del Estado Civil en todos los puntos cardinales de la geografía colombiana, va desde dar el reconocimiento de la personalidad jurídica a todos los hijos de esta patria, inclusive de los colombianos que nacen más allá de nuestras fronteras, por medio del registro civil de nacimiento. Después esta función registral reitera su convicción de certeza mediante la expedición de la tarjeta de identidad, que posteriormente se transformará en la cédula de ciudadanía, que permitirá el ejercicio de diversos derechos en los ámbitos públicos y privados. Inclusive hasta el final de la vida, la Registraduría Nacional del Estado Civil acompaña a cada uno de los habitantes, expidiendo su respectivo registro civil de defunción.

Las funciones en materia de registro civil y organización electoral, en el manejo de los datos personales convierte a la Registraduría Nacional del Estado Civil en el administrador de datos más grande de Colombia, con más de 49.743.000 registros de personas con datos de diversa índole, que se multiplican a su vez en diversas bases de datos entre las que destacan las de registro civil de nacimiento, tarjeta de identidad, cédula de ciudadanía, registro civil de defunción y el censo electoral. Así, la Registraduría Nacional del Estado Civil asume el gran reto de dar certeza y proteger el correcto uso de la información que identifica a todos los colombianos.

La Registraduría Nacional del Estado Civil surge como entidad encargada de la identificación de las personas con fines electorales a partir de la Ley 89 de 1948, la cual le otorga la responsabilidad de crear una organización electoral ajena de los partidos y con ello fomentar la práctica democrática en Colombia. Desde entonces se caracteriza por su neutralidad política cuyas regulaciones garantizan la plena responsabilidad y la imparcialidad en el ejercicio de sus funciones, trayendo como resultado elecciones trasparentes con certidumbre jurídica. En aquel entonces la Registraduría sirvió como

instrumento democrático para apaciguar las relaciones violentas propias de esa época, y hasta ahora esta institución registral sigue siendo la garante de los principales procesos democráticos que se desarrollan en Colombia.

La forma directa por la cual la Registraduría impulsa el ejercicio de los derechos fundamentales consiste en los procedimientos que implanta esta institución, que le son otorgados en virtud de su autonomía y sus facultades, constitucionalmente positivizados para la promoción democrática del Estado colombiano. Mientras que en forma indirecta esta institución coadyuva para el ejercicio del catálogo de garantías constitucionales al servicio de los particulares mediante el otorgamiento de la certeza y seguridad jurídica en el reconocimiento de la personalidad de los individuos.

Ambas misiones encargadas por la Ley Fundamental a esta institución autónoma del Estado colombiano implican un gran esfuerzo que combina el talento humano de todos los que integramos esta institución y la convicción de hacer una mejor patria conforme a los criterios democráticos exigidos por la Constitución. Esta idea de patriotismo constitucional que invade a la Registraduría Nacional del Estado Civil, comulga con la expresada por el filósofo alemán Jürgen Habermas[1], en el sentido de una concepción participativa de la ciudadanía a través de las herramientas que le son otorgadas a los ciudadanos por la Registraduría y, que están dirigidas a la promoción del bien común. La ciudadanía hace suyos los valores patrios inmersos en la Ley Fundamental y se define por la adhesión a unos principios comunes de carácter democrático plasmados en la Constitución. Así, la institución registral tiene la obligación de proporcionar ese camino común basado en criterios democráticos para ejercerlos.

La misión registral y la electoral encomendadas al gran equipo que integra la Registraduría Nacional del Estado Civil son de la esencia democrática del Estado social y de derecho que hemos decidido otorgarnos los colombianos. Estoy convencido de que Colombia puede seguir descansando gran parte de su acervo democrático en la Registraduría Nacional del Estado Civil, pues esta seguirá llevando con criterios de eficacia sus labores, como lo ha hecho desde 1948 y hasta este 2018, como lo ha logrado a partir del reconocimiento de las personas y en la elaboración de procesos democráticos certeros de decisión.

Así, en el Plan Estratégico para los años 2015-2019 se estableció como principal objetivo el "lograr que la Registraduría Nacional del Estado Civil se convierta en la entidad con mejores índices de transparencia, confiabilidad y alta calidad en la prestación efectiva del servicio y en la entrega de sus productos a todos los colombianos y a todas las empresas públicas y privadas que así lo requieran, dentro y fuera del territorio nacional"[2], por lo que ambas misiones se entrelazan a partir de un correcto funcionamiento de los datos personales para lograr los objetivos antes planteados.

[1] La idea del patriotismo constitucional nace después de la segunda postguerra mundial y busca apartar del nacionalismo clásico que dio origen a ese gran conflicto bélico, para pasar a dar impulso a la idea de construir el aglomerado social a partir de valores patrios de índole constitucional y por ende democráticos. Consultar, Jürgen Habermas, I*dentidades nacionales y postnacionales*, Madrid Tecnos, 1989.

[2] Registraduría Nacional del Estado Civil, Plan estratégico 2015-2019, pág. 29. Consultable en *https://wsr.registraduria.gov.co/IMG/pdf/Plan_Estrategico_RNEC_2015-2019_Version_Final-ilovepdf-compressed.pdf*

Esto explica la gran importancia que tiene la presente investigación, pues a partir de ella se establecerán las directrices adecuadas para que en materia de tratamiento de datos personales, la Registraduría Nacional del Estado Civil obtenga los mejores índices de transparencia, confiabilidad y alta calidad, en la prestación efectiva del servicio y en la entrega de sus productos a todos los ciudadanos colombianos.

Los datos personales de todos los colombianos constituyen uno de los patrimonios primordiales de nuestro Estado constitucional, por lo que el compromiso de la Registraduría Nacional del Estado Civil es cumplir con los más altos estándares nacionales e internacionales en su protección, pero siempre bajo la estructura y las facultades que la Constitución Política de 1991 le otorga a esta institución para la protección de los derechos de los colombianos.

Juan Carlos Galindo Vácha
Registrador Nacional del Estado Civil

ÍNDICE GENERAL

PÁG.

CAPÍTULO II

ASPECTOS MEDULARES DEL TRATAMIENTO DE DATOS PERSONALES EN DOCUMENTOS INTERNACIONALES Y SU REGULACIÓN EN ALGUNOS PAÍSES LATINOAMERICANOS Y ESPAÑA

CAPÍTULO III

BUENAS PRÁCTICAS Y RESPONSABILIDAD DEMOSTRADA SOBRE TRATAMIENTO DE DATOS PERSONALES EN EL CONTEXTO INTERNACIONAL

PÁG.

Capítulo IV

GUÍAS DE RESPONSABILIDAD DEMOSTRADA (*ACCOUNTABILITY*) Y PROGRAMAS INTEGRALES DE GESTIÓN DE DATOS PERSONALES

PÁG.

PÁG.

INTRODUCCIÓN

El tratamiento[1] de datos personales y el uso de bases de datos son actividades cotidianas e importantes para el Estado, las empresas y los particulares. Todos requieren dicha información para tomar y ejecutar decisiones de diversa naturaleza —económica, seguridad nacional, social, política, laboral, impuestos, estadísticas, profesional, académica, financiera, comercial, etc.—. Así las cosas, los datos personales son un activo estratégico para las organizaciones, pero su tratamiento no es solo cuestión que incide en ellas sino que afecta los derechos de las personas. Por eso, estas deben realizarlo con la debida observancia de unas pautas regulatorias.

Las TIC —tecnologías de la información y la comunicación—, por su parte, no sólo son consideradas como el "símbolo emblemático de la cultura contemporánea"[2] sino que han contribuido a la "datificación" de la sociedad contemporánea y a la consolidación del dato personal como el bien más apetecido de la economía digital.

El tratamiento de los datos personales (en adelante TDP) es uno de los asuntos que en los últimos cincuenta años ha llamado poderosamente la atención de los reguladores y las organizaciones. En un principio mereció reglamentación, pero en la última década estamos presenciando una eclosión mundial de normas sectoriales y generales, la revisión de las primeras iniciativas regulatorias, así como múltiples conferencias a todo nivel que ponen de presente la indiscutible relevancia social y económica del tratamiento de la información de las personas.

El derecho a la protección de datos personales que conocemos actualmente ha tenido cambios desde sus primeras manifestaciones regulatorias de la década de los setenta y los documentos emitidos posteriormente. A los motivos iniciales que dieron origen a su reglamentación se sumaron otros factores que han hecho que los retos de la protección de este derecho sean diferentes a los inicialmente previstos.

[1] A efectos del presente documento, las expresiones "tratar" o "tratamiento" se entenderán como cualquier operación o conjunto de operaciones aplicadas a datos personales, como la recolección, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.

[2] Aristeo García González (2007). "La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado", en *Boletín Mexicano de Derecho Comparado* (120), México, Universidad Nacional Autónoma de México, pág. 744.

El derecho al debido tratamiento de los datos personales, parte del supuesto de que la recolección y uso de los datos no es algo que solo le interesa a su titular, porque reconoce que los datos son necesarios para realizar muchas actividades lícitas, legítimas y de interés general o particular, según el caso. Por eso no es un derecho para oponerse al tratamiento, sino para exigir un correcto tratamiento de la información sobre las personas. No se opone al uso informático sino al abuso informático.

Además, las relaciones jurídicas en el marco de tratamiento de datos personales y de su titular, adquieren peculiaridades dependiendo los sujetos que estén involucrados. No es lo mismo el tratamiento de datos personales a partir de una relación entre particulares, que la que se produce entre sujetos de derecho público y los particulares; en ambas situaciones están inmersos derechos de los titulares de los datos personales pero las responsabilidades adquiridas para el tratamiento y, por ende, sus prerrogativas, adquieren una dimensión específica según los sujetos que están involucrados.

Varios países cuentan con regulaciones generales, sectoriales y jurisprudencia sobre el tratamiento de datos personales. Aunque se ha procurado armonizar internacionalmente los principales aspectos sobre el tratamiento de datos personales, en la práctica cada Estado cuenta con normas que parcialmente siguen dichos documentos internacionales pero que al mismo tiempo están impregnadas de las particularidades sociales, políticas, culturales y jurídicas de cada uno. Adicionalmente, cada sistema jurídico nacional cuenta con diversas herramientas jurídicas (constitucionales, administrativas, judiciales, entre otras) para proteger el derecho al debido tratamiento de datos personales (en adelante DDTDP).

Esta obra tiene los siguientes propósitos: en primer lugar, delimitar los elementos de las facultades de la Registraduría Nacional del Estado Civil (en adelante RNEC) respecto del tratamiento de datos personales. En segundo lugar, identificar los principales aspectos que irradian la recolección, uso, almacenamiento, circulación y cualquier otra actividad sobre datos personales desde la perspectiva de los aspectos cruciales del principio de responsabilidad demostrada —*accountability*—, las guías sobre la materia y los programas integrales de gestión de datos personales. Con esto se quieren dejar sentadas las bases para garantizar el debido tratamiento de datos en cualquier organización, lo cual redundará no solo en beneficio de la protección de los derechos de las personas sino en pro de las entidades para que maximicen el uso de la información y consoliden su reputación empresarial o institucional.

Para el efecto, en el primera capítulo, a partir de la democracia dentro de la estructura del Estado colombiano, el principio de división de poderes y los órganos autónomos constitucionales, analizaremos la naturaleza de la Registraduría Nacional del Estado Civil, sus antecedentes y su organización administrativa.

Adicionalmente, estudiaremos las dos facultades constitucionales principales para la RNEC: por un lado, la función electoral, y del otro la función registral. Finalmente, nos referiremos al derecho fundamental de habeas data y obligaciones constitucionales, legales y jurisprudenciales, aplicables a la Registraduría Nacional del Estado Civil como responsable del tratamiento de datos personales.

En el segundo capítulo, se hace un análisis de derecho comparado sobre el tratamiento de datos personales dividido en dos componentes. En el primero, nos referiremos al proceso de armonización internacional desde la perspectiva de los principales documentos que han emitido organizaciones como la Red Iberoamericana de Protección de Datos (en adelante RIPD), la Unión Europea (UE), la Organización de Estados Americanos (OEA), la Organización para la Cooperación y el Desarrollo Económico (OCDE), la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (CIAPDP), el Foro de Cooperación Económica Asia Pacífico (APEC) y la Organización de las Naciones Unidas (ONU). En el segundo, realizaremos un estudio de algunos aspectos sobre el tema respecto de la regulación en algunos países, que guardan cierta similitud con el sistema de protección de datos en Colombia, a saber: Argentina, Costa Rica, España, México, Perú y Uruguay.

En su tercer capítulo se desarrollarán las buenas prácticas en TDP comenzando por la expresión "buenas prácticas" que comúnmente se refiere a experiencias que han producido resultados positivos, demostrando su eficacia y utilidad en un contexto concreto. Dentro de estas se tendrán las que se derivan de documentos internacionales y las medidas proactivas sobre tratamiento de datos personales.

El capítulo IV se ocupa en el análisis de las guías de responsabilidad demostrada —*accountability*— y de los programas integrales de gestión de datos personales

En el último capítulo se analizarán las guías de *accountability* que se han redactado sobre la materia por las autoridades de Australia, Canadá, Colombia, Hong Kong y el GECTI. Luego se estudiarán los elementos más importantes que usualmente se incorporan en los Programa Integrales de Gestión de Datos Personales (PIGDP), determinando las medidas necesarias, apropiadas, útiles, eficientes, medibles y verificables para demostrar el cumplimiento de los criterios adoptados en materia de responsabilidad demostrada o *accountability*.

Con esto, se pretende destacar los principales insumos derivados de las buenas prácticas en la protección de datos personales en el derecho comparado, para hacer un contraste con las facultades derivadas de la autonomía de la RNEC, y así obtener los elementos relevantes para la elaboración de planteamientos jurídicos en el correcto tratamiento de los datos personales del mayor administrador de datos de Colombia.

Capítulo I

LA INGENIERÍA CONSTITUCIONAL DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL Y EL TRATAMIENTO DE DATOS PERSONALES

1. La ingeniería constitucional de la Registraduría Nacional del Estado Civil

Nuestra Constitución Política, en su artículo 1º establece que "Colombia es un Estado social de derecho, organizado en forma de República unitaria, descentralizada, con autonomía de sus entidades territoriales, democrática, participativa y pluralista, fundada en el respeto de la dignidad humana, en el trabajo y la solidaridad de las personas que la integran y en la prevalencia del interés general".

La fundamentación de la democracia en nuestro ordenamiento jurídico se encuentra en nuestra Constitución, desde su Preámbulo hasta el último título pues es la columna vertebral de la estructura actual del Estado. La Carta Política se configura como el marco de ejecución de un sistema integral que va desde las libertades de todos los ciudadanos hasta las facultades de las distintas autoridades que concluyen en la idea de país dentro de un sistema constitucional y, por ende, democrático. Ello significa la disposición de distintos escenarios y procesos donde el ciudadano tiene un papel central como soberano, que otorga legitimidad democrática al Estado social y de derecho.

Las actuaciones del Estado implican la conjunción de los derechos que ejercen las personas que adicionalmente se relacionan con las funciones que cumplen las instituciones políticas, que por tanto son susceptibles de distintos tipos de control. La democracia tiene un valor intrínseco que acogió el proceso constituyente de 1991, el cual se erigió sobre la base de dos ideas fundamentales que confluyen en el concepto que desarrolla este principio del Estado colombiano. La primera es que, como presupuesto de la organización de la estructura del Estado, esta se concibió según el principio de la división de poderes, pero, al mismo tiempo, a partir de la autonomía y la legitimidad de órganos autónomos constitucionales. La segunda implica la concepción de la democracia como presupuesto del ejercicio de derechos de los ciudadanos, que en principio son considerados como libertades que transmutan a la idea de patrimonio jurídico inherente a las personas. Ambas

concepciones, a partir y desde la democracia, convergen como idea central de esta investigación, pues los datos personales no solo son derechos inherentes a las personas, sino que su protección es una facultad que desde la institucionalidad colombiana se debe desarrollar.

A) *La democracia dentro de la estructura del Estado colombiano*

La democracia en nuestro Estado social y de derecho, implica en punto a las instituciones políticas una serie de engranajes en las facultades con el fin de lograr su efectivo ejercicio por los actores institucionales que integran este país. Su dinámica se desenvuelve mediante la visualización de la realidad social, lo que significa unas garantías mínimas de respecto de un sistema jurídico, político y social. Mientras que la democracia sea entendida como ejercicio de prerrogativas, ello implica la activación de la real garantía y goce de la totalidad de los derechos inherentes a la persona, entre los que se destaca el ejercicio de votar y ser elegido, como derecho fundamental para la conformación de las autoridades del Estado, siendo el sufragio el medio para que el soberano manifieste su voluntad, o el del libre desarrollo de la personalidad, a partir del reconocimiento de la personalidad jurídica de los colombianos por parte del Estado.

En virtud del principio democrático, la ciudadanía tiene participación directa o indirecta en cada uno de los ámbitos en los que se desenvuelve, tanto en el privado como en el público, es decir, en sus relaciones interpersonales y en sus relaciones con el Estado. Estos instrumentos están previstos en la Constitución, como mecanismos de participación ciudadana o como derechos autónomos e inherentes a las personas. Así, el artículo 103[1] constitucional consagra unos mecanismos de democracia participativa, como el voto, el plebiscito, el referendo, la consulta popular, el cabildo abierto, la iniciativa legislativa y la revocatoria del mandato; adicional a ello encontramos algunos derechos de los ciudadanos que lo relacionan con el ejercicio de sus derechos tan básicos como el reconocimiento de la personalidad.

Otro ejemplo que hace relación a la democracia y su ejercicio, se encuentra en el artículo 20[2] de la Constitución, el cual reconoce a toda persona el derecho de

[1] Art. 103. "Son mecanismos de participación del pueblo en ejercicio de su soberanía: el voto, el plebiscito, el referendo, la consulta popular, el cabildo abierto, la iniciativa legislativa y la revocatoria del mandato. La ley los reglamentará.

"El Estado contribuirá a la organización, promoción y capacitación de las asociaciones profesionales, cívicas, sindicales, comunitarias, juveniles, benéficas o de utilidad común no gubernamentales, sin detrimento de su autonomía con el objeto de que constituyan mecanismos democráticos de representación en las diferentes instancias de participación, concertación, control y vigilancia de la gestión pública que se establezcan".

[2] Art. 20. "Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.

expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial. Así mismo, en el artículo 23[3] de la Carta Política se establece el derecho de presentar peticiones respetuosas a las autoridades por motivos de interés general o particular y a obtener pronta resolución, lo cual es plena garantía del papel que cumple el ciudadano frente al Estado como legitimador democrático.

La legitimación ética y jurídica basada en el consentimiento del pueblo como valor democrático, el cual se expresa no solo mediante el voto, sino por medio de los mecanismos de democracia participativa y de participación ciudadana y los demás derechos que impliquen una participación, directa e indirecta, del ciudadano, en cumplimiento del mandato previsto en el artículo 3º[4] de la Constitución, que consagra el principio de soberanía popular, el cual da origen a la organización política colombiana. Este planteamiento, necesariamente nos lleva a la conclusión de que en el Estado colombiano, independientemente de que la democracia se practica de forma directa e indirecta, su razón de ser es el soberano popular.

De allí que a partir de la soberanía popular se infiere el proceso de legitimación democrática, puesto que es el soberano quien elige a sus representantes y ello deriva en una organización política. De nada sirve el poder sin una organización estructurada sobre la base de criterios constitucionales, que se encuentra plasmada en el pacto social que nos rige. Es por ello por lo que la estructura del Estado se encuentra fundamentada en nuestra Constitución, puesto que ningún poder debe ser absoluto dentro de régimen democrático. Y también por lo que la voluntad política legítima de la actuación de los órganos del Estado, parte del principio democrático de donde se infiere el poder y la estructura del Estado.

Al respecto, la Corte Constitucional reiteró el papel de la democracia dentro de nuestro diseño constitucional: "En el énfasis dado por el Constituyente al principio democrático, que aparece desde el Preámbulo, se repite en el artículo 1º como forma del Estado y en artículo 2º como fin del Estado para facilitar la participación. Además, en el artículo 3º se reconoce la soberanía popular y luego en los diferentes artículos que desarrollan el principio en sentido material como en la dimensión estructural del Estado [...] La consagración constitucional del principio

---

"Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura".

[3] Art. 23. "Toda persona tiene derecho a presentar peticiones respetuosas a las autoridades por motivos de interés general o particular y a obtener pronta resolución. El legislador podrá reglamentar su ejercicio ante organizaciones privadas para garantizar los derechos fundamentales".

[4] Art. 3º. "La soberanía reside exclusivamente en el pueblo, del cual emana el poder público. El pueblo la ejerce en forma directa o por medio de sus representantes, en los términos que la Constitución establece".

de la democracia demuestra que su contenido no se relaciona exclusivamente con los instrumentos de participación política sino se proyecta sobre diversos ámbitos"[5].

Esto explica que la democracia constitucional es la legitimación de las autoridades y órganos que integran el ordenamiento estadual, los cuales están obligados a cumplir los fines del Estado consagrados en la Constitución, la separación de poderes y la garantía de los derechos fundamentales, entre otros.

B) *División de poderes y órganos autónomos constitucionales*

En la declaración de los Derechos del Hombre y del Ciudadano de 1789, documento fundante del constitucionalismo actual en Occidente, se estableció en su artículo 16[6] la importancia de la separación de poderes dentro de un sistema constitucional, y cómo la limitación de estos poderes se convierte en la plena garantía de los derechos de las personas. Nuestra Constitución prevé como principios la democracia y la soberanía popular. Dentro del diseño institucional del Estado la Ley Fundamental en su artículo 113[7] establece la distribución del poder público, el cual no es divisible por venir inmerso en la suprema potestad que descansa en un sólo soberano, simplemente se distribuye entre las ramas ejecutiva, legislativa y judicial, que integran el Estado[8]. Por lo que se debe partir de la concepción básica de un solo soberano (el pueblo) el cual ostenta el poder dentro del régimen democrático, pero que para su ejercicio encuentra canales establecidos en la estructura del Estado, según se define en la teoría republicana colombiana a partir del numeral antes citado.

Además de las ramas del poder público, existen otros órganos autónomos e independientes los cuales están destinados a cumplir funciones específicas del Estado. Tanto los órganos que integran las ramas del poder público, como los órganos autónomos constitucionales tienen funciones separadas, pero colaboran

[5] Corte Const., sent. C-292 de 2003 (8 de abril),. revisión de constitucionalidad del proyecto de ley número 022 de 2001 Senado, 149 de 2001 Cámara, "por medio de la cual se reglamentan las veedurías ciudadanas". (M. P. Dr. Eduardo Montealegre Lynett).

[6] Art. 16. "Una sociedad en la que no esté establecida la garantía de los derechos, ni determinada la separación de los poderes, carece de Constitución".

[7] Art. 113. "Son ramas del poder público, la legislativa, la ejecutiva, y la judicial.

"Además de los órganos que las integran existen otros, autónomos e independientes, para el cumplimiento de las demás funciones del Estado. Los diferentes órganos del Estado tienen funciones separadas pero colaboran armónicamente para la realización de sus fines".

[8] Corte Const., sent. C-246 de 2004 (16 de marzo), demanda de inconstitucionalidad contra los arts. 4º y 6º (parciales) de la ley 18 de 1970; parg. 2° (parcial) del art. 41 de la ley 80 de 1993; parg. del art. 7º y art. 24 (parcial) de la ley 185 de 1995; y art. 38 de la ley 344 de 1996. Demandante: Andrée Viana Garcés (M. P. Dra. Clara Inés Vargas Hernández).

armónicamente para la realización de los fines a los que se refiere la Constitución Política de Colombia de 1991[9].

En relación con el principio de separación de poderes, la Corte Constitucional, en sentencia C-288 de 2012[10], sostiene que existen dos modelos:

A) El primero defiende una delimitación funcional del poder, lo que implica que cada uno de los órganos ejerza dentro de sus funciones preestablecidas sus facultades y así se aseguren las libertades del ser humano que se traducen en sus derechos, la democracia como presupuesto de la separación de poderes *transmuta* en el ejercicio de las garantías inherentes a las personas.

B) La segunda también implica una especialidad en cuanto a las labores de cada uno de los órganos que integran el poder público, pero en este caso las

[9] *Ibidem.*

[10] La jurisprudencia constitucional ha reconocido que existen "dos modelos de separación de poderes":

El primero de estos modelos defiende una delimitación funcional rigurosa, como medio para acotar el poder, a partir del entendimiento de que una distribución precisa y equilibrada de las labores estatales, en la cual cada órgano cumple una tarea preestablecida, es una condición suficiente para mantener a dichos órganos del poder dentro de sus límites constitucionales. A su vez, la separación funcional rígida es concebida como una estrategia que permite asegurar las libertades de los ciudadanos. Desde esta perspectiva, el equilibrio de los poderes es una consecuencia natural de la autonomía de órganos con funciones constitucionalmente bien delimitadas. En consecuencia, el control que ejerce un órgano sobre otro en relación con el cumplimiento de sus propias funciones, es básicamente un control político, que se da de manera tanto espontánea como ocasional, y solo frente a casos extremos. Precisamente, la rigidez de la separación de poderes condenaba este modelo al fracaso, por la dificultad para ponerlo en práctica, pues la falta de vasos comunicantes entre los distintos órganos estatales conducía a enfrentamientos difíciles de solucionar, cuyo resultado natural y obvio tendía a ser la reafirmación del poder en los órganos, autoridades o funcionarios que se estiman política y popularmente más fuertes.

El segundo modelo también parte de una especialización de las labores estatales, cada una de las cuales corresponde a un órgano específico, sin embargo, le confiere un papel preponderante al control y a las fiscalizaciones interorgánicas recíprocas, como reguladores constantes del equilibrio entre los poderes públicos. Este modelo constitucional denominado de frenos y contrapesos (*checks and balances*) no presupone que la armonía entre los órganos que cumplen las funciones clásicas del poder público sea una consecuencia espontánea de una adecuada delimitación funcional y de la ausencia de interferencias en el ejercicio de sus competencias. Por el contrario, el balance de poderes es un resultado que se realiza y reafirma continuamente, mediante el control político, la intervención de unos órganos en las tareas correspondientes a otros y las relaciones de colaboración entre las distintas ramas del poder público en el ejercicio de sus competencias. En otras palabras, cada órgano tiene la posibilidad de condicionar y controlar a los otros en el ejercicio de sus respectivas funciones. Entonces, la fórmula más apropiada para describir esta realidad es la de *separated institutions sharing powers*, acuñada por Neustadt al describir la forma de gobierno presidencial, esto es, instituciones separadas que comparten los mismos poderes.

labores de control *recíproco* tienen más preponderancia dentro del sistema. En el modelo de frenos y contrapesos de las ramas ejecutiva, legislativa y judicial, la Corte Constitucional colombiana reconoce que el principio de separación de poderes, adoptado en la Constitución de 1991, prohíja un sistema flexible en la distribución de las distintas funciones del poder público, el cual se rige por el principio de colaboración armónica de los diferentes órganos del Estado, en el cual se establecen diferentes mecanismos de frenos y contrapesos entre las ramas que integran el poder público.

Así la división de poderes implica la función de gobernar mediante separación clásica entre el poder ejecutivo, el poder legislativo y el poder judicial, que en la Constitución Política de 1991, se positiviza a partir de la idea de un solo poder público, con tres ramas que, a su vez, son órganos independientes unos de los otros, que ejercen control recíproco y que al mismo tiempo colaboran entre ellos. Pero, además de la división clásica republicana existen otros órganos autónomos e independientes, considerados por la doctrina jurídica como órganos autónomos constitucionales que no forman parte de la división clásica, pero que tienen rango constitucional con funciones específicas, y que son considerados órganos de la estructura de las instituciones políticas colombianas.

Como se observa, esta distribución del poder público[11] contenida en la Constitución implica un diseño institucional específico dentro del ordenamiento constitucional, por lo que los órganos del Estado cumplen una función específica y deben colaborarse armónicamente. Se busca garantizar un equilibrio en el ejercicio de cada uno de los poderes, porque si bien son específicos deben tener límites dentro del diseño institucional, límites que se ejercen entre cada uno de los órganos que integran el poder público o por parte del soberano.

La gestión pública del Estado debe perseguir la consecución de los fines establecidos en el artículo 2º[12] de la Constitución. Gracias a esta disposición se

[11] Acción pública de inconstitucionalidad contra los arts. 44, lit. d), y 66 lit. b) del decr. 2147 de 1989, "por el cual se expide el régimen de carrera de los empleados del Departamento Administrativo de Seguridad". Actor: Luis Arturo Victoria (M. P. Dr. Hernando Herrera Vergara), 6 febrero 1997. "El ejercicio del poder público sólo será legítimo si está dirigido a la realización de los fines esenciales del Estado y, en particular, a la promoción y garantía de los derechos fundamentales. Para garantizar el ejercicio legítimo del poder público, los Estados democráticos aseguran que la esfera pública se encuentre abierta al conocimiento y control de todos los ciudadanos. La publicidad garantiza la transparencia de la gestión estatal y facilita y permite el control sobre los actos de las autoridades".

[12] Art. 2º. "Son fines esenciales del Estado: servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar la participación de todos en las decisiones que los afectan y en la vida económica, política, administrativa y cultural de la Nación; defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo.

convierte en un deber la existencia de distintos planes y estrategias de ejecución de las actuaciones del Estado tendientes a satisfacer las finalidades del mismo. En este contexto de democracia, los controles pueden ser ejercidos por los ciudadanos o por las instituciones establecidas por la Constitución para tal efecto.

En el artículo 113 constitucional consagra la estructura básica del Estado para el ejercicio del poder público, que al ser este indivisible lo distribuye entre los órganos que integran las ramas del poder público; adicionalmente, existen órganos autónomos e independientes de las ramas tradicionales que integran el poder público, es decir la ejecutiva, la legislativa y la judicial.

La autonomía que nuestra Constitución de 1991 le reconoce a determinadas entidades estatales, implica que los órganos autónomos constitucionales no pertenecen a las ramas del poder público y tienen una clara independencia funcional de dichas ramas, para actuar por fuera de ellas dentro del ámbito de sus funciones, las cuales se rigen por el principio de legalidad enunciado en el artículo 6º[13] de la Constitución. Así mismo, estos organismos cuentan con potestad normativa orientada a ordenar su propio funcionamiento y al cumplimiento de la misión constitucional que se les ha ordenado. Este modelo de estructura del Estado consagrado en la Constitución, que se refiere a las ramas del poder público (legislativa, ejecutiva y judicial), además introdujo un concepto nuevo: *los órganos autónomos e independientes.*

Considerado lo anterior, existen límites entre la acción de los órganos de las ramas del poder público, respecto de los organismos definidos constitucionalmente como autónomos e independientes, en el ámbito de sus funciones. Es así como nos encontramos frente al desarrollo orgánico del Estado colombiano, sustentado entre otras disposiciones en el artículo 113 de la Constitución que define los órganos que representan al Estado colombiano, formen parte o no de lo que se denomina poder público, y que fueron instituidos para el cumplimiento de sus fines, es decir, existen órganos del Estado colombiano investidos de poder público los cuales se encuentran en las tres ramas originales de la división republicana, y otros que no están dentro de la división clásica de poder, pero que también tienen facultades específicas en de la estructura del Estado.

La estructura orgánica del Estado parte del supuesto de definir los elementos de los órganos que lo integran, es decir, lo relacionado con su marco de indepen-

---

”Las autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias, y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares”.

[13] Art. 6º. “Los particulares solo son responsables ante las autoridades por infringir la Constitución y las leyes. Los servidores públicos lo son por la misma causa y por omisión o extralimitación en el ejercicio de sus funciones”.

dencia, basado en la separación de funciones, su régimen jurídico, patrimonial y de personalidad jurídica que se les reconoce, así como su aspecto estructural, el cual se materializa en la conexión con las competencias de los demás órganos, en un primer momento en lo relacionado con la división de poderes (en el caso específico de los órganos que integran las ramas del poder público), y en el segundo mediante la colaboración armónica entre todos los órganos institucionales.

Con las precisiones anteriores, sobre el diseño institucional plasmado en el artículo 113 de la Constitución, se establecen los órganos de las ramas ejecutiva, legislativa y judicial, y también los órganos autónomos e independientes, que no se pueden enmarcar en las ramas del poder público del Estado. De esta suerte, se consagró la función de control disciplinario radicada en cabeza del ministerio público, la función de control fiscal radicada en la Contraloría General de la Nación y la función electoral que corresponde a la Organización Electoral, entre otros. Además, debe agregarse que se le reconoce autonomía constitucional al Banco de la República, a las corporaciones autónomas regionales, a las universidades oficiales autónomas y a la Comisión Nacional del Servicio Civil[14]. La característica esencial de los órganos autónomos constitucionales establecidos en el artículo 113, es definida por la Corte Constitucional en la sentencia C-401 de 2001, como "aquella que otorga a determinados organismos y significa, básicamente:

"a. No pertenencia a alguna de las ramas del poder.

"b. Posibilidad de actuación por fuera de las ramas del poder y por ende actuación funcionalmente independiente de ellas.

"c. Titularidad de una potestad de normación para la ordenación de su propio funcionamiento y el cumplimiento de la misión constitucional encomendada.

"d. La autonomía constitucionalmente otorgada marca un límite a la acción de los órganos de las ramas del poder sobre los órganos definidos constitucionalmente como autónomos"[15].

En relación con el marco de autonomía que se les garantiza a los órganos constitucionales ya mencionados, la Corte Constitucional en sentencia C-401 de 2001, manifiesta que las ramas del poder público en su actuar están limitadas por el núcleo esencial de la autonomía definido en la Constitución para cada entidad en concreto. Lo anterior se verá reflejado en las funciones y misiones especificas contenidas en la Carta Política frente a los órganos autónomos, por lo que, la competencia de los órganos que integran las ramas del poder público frente a los

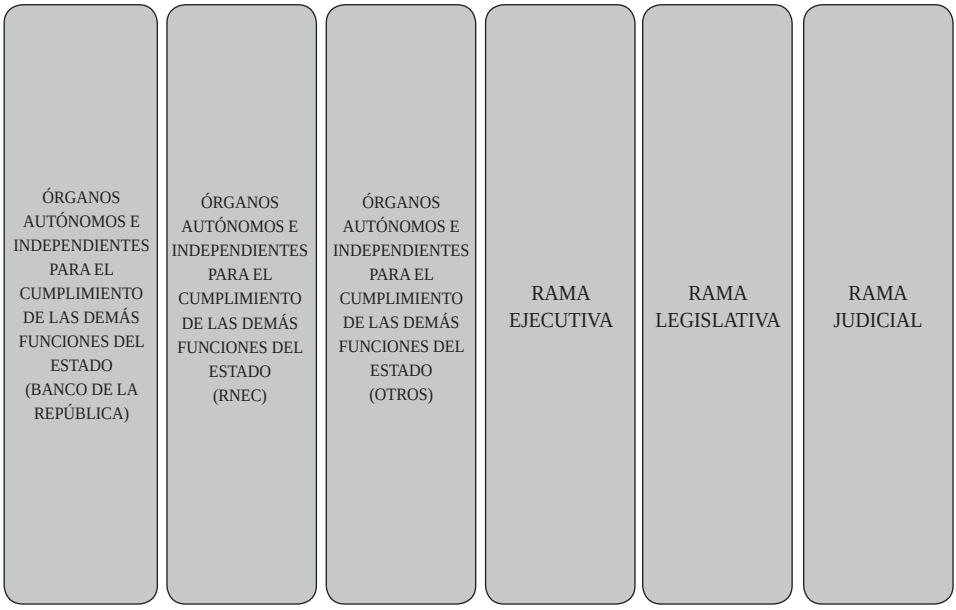
[14] Corte Const., sent. C-497 de 1995. Actor: María Teresa Garcés Lloreda. Demanda de inconstitucionalidad (parcial) contra los lits. c) y d) y el parágrafo del art. 6º de la ley 182 de 1995 (M. P. Dr. Eduardo Cifuentes Muñoz), 7 noviembre 1995.

[15] Corte Const., sent. C-401 de 2001. Demanda de inconstitucionalidad contra el art. 1º parcial, de la ley 573 de 2000. Actor: Pedro Alfonso Hernández M. (M. P. Dr. Álvaro Tafur Galvis), 19 abril 2001.

organismos autónomos se limita estrictamente a lo establecido en la Constitución, que como norma suprema es la encargada de definir sus funciones y establecer sus condiciones de autonomía dentro de los criterios que la misma ley fundamental establezca, los cuales podrán ser desarrollados por otras normas[16].

Los órganos autónomos constitucionales realizan funciones específicas de acuerdo con la personalidad y facultades que le son reconocidas constitucionalmente. Las facultades corresponden a la función ordinaria de las ramas del poder público para su eficaz ejercicio y adquieren rango supremo constitucional sin formar parte de la estructura del poder público, pero sí de la estructura del Estado.

Principio de democracia directa derivada del poder público, soberano, el cual crea un sistema de pesos y contrapesos, conforme al principio de colaboración armónica.



Estructura del Estado colombiano

[16] Corte Const., sent, C-401 de 2001. Demanda de inconstitucionalidad contra el art. 1º parcial, de la ley 573 de 2000. Actor: Pedro Alfonso Hernández M. (M. P. Dr. Álvaro Tafur Galvis), 19 abril 2001: "las acciones de las ramas del poder público se hallan limitada por el núcleo esencial de autonomía que resulta definido por los mandatos mediante los cuales la Constitución, de manera explícita y en cada caso, define el ámbito de autonomía. Lo anterior se traduce en que a mayor regulación constitucional menor será el ámbito de la regulación legal y viceversa. El respeto al núcleo esencial de autonomía que en cada supuesto aparecerá definido en función del cumplimiento de las misiones específicas encomendadas al órgano autónomo. Por lo anterior es pertinente determinar que, tratándose de los órganos constitucionalmente autónomos la extensión y cabal proyección de la cláusula general de competencia a favor de los demás órganos que integran la estructura del Estado se limita a los establecido a nivel cosntitucional".

La gran conclusión de la estructura jurídica y constitucional del Estado colombiano implica que las ramas del poder público están integradas por órganos que se limitan y colaboran entre sí, con legitimación democrática directa por parte del soberano. Mientras que los demás órganos autónomos constitucionales tienen legitimidad democrática, indirecta por las funciones que se traducen en las facultades que ejercen en virtud de sus misiones, pero ambas legitimaciones democráticas (directa e indirecta) son indispensables para cumplir los fines esenciales del Estado en su conjunto.

Lo anterior implica un deber de claridad frente a las facultades atribuidas a los órganos que integran el Estado, es decir los que forman las ramas del poder público y los demás órganos autónomos. La Carta Política de 1991 atribuyó a diferentes órganos las funciones que no encajaban directamente en la tridivisión tradicional del poder público, como ya lo vimos; por ello dedica su título V la organización del Estado, que se resume en el artículo 113, y posteriormente su título IX analiza las funciones del Estado que se encuentran revestidas de autonomía, lo que nos lleva al estudio de una estas, la que es titular de la función electoral a cargo del Estado.

C) *Registraduría Nacional del Estado Civil*

a) *Antecedentes*[17]. Históricamente la Registraduría Nacional del Estado Civil (RNEC), como entidad encargada de la identificación de las personas con fines electorales, nace con la ley 89 de 1948, cuyo objeto fue crear una organización electoral ajena a las influencias de los partidos para fomentar la práctica democrática, es decir completamente neutra, cuyo funcionamiento no obedezca a los intereses de ningún partido o grupo político que se traduzca en ventajas sobre los demás en la consecución de la cédula de ciudadanía para sus afiliados, ni en la formación de los censos electorales, ni en las votaciones y escrutinios. Sus regulaciones deben garantizar la plena responsabilidad y la imparcialidad política de sus funcionarios, que como resultado se concrete en elecciones limpias, con certidumbre jurídica, es decir, la función misional de la RNEC es, en gran parte, el sustento democrático del ejercicio de la soberanía del país[18].

Esta norma de conducta constituye un principio al cual se deben ceñir rigurosamente todas las personas encargadas de cumplir funciones dentro de los organismos electorales. En ese entonces la organización electoral estaba integrada por:

a) Una Corte Electoral, con sede en la capital.

[17] Este apartado se fundamenta en la información obtenida de la página web oficial de la RNEC y de la normativa correspondiente.

[18] Página Web de la Registraduría Nacional del Estado Civil *https://www.registraduria.gov.co*.

b) Las comisiones escrutadoras o de recuento de votos en los departamentos, intendencias, comisarías y municipios.

c) El registrador nacional del Estado Civil.

d) Los delegados del registrador nacional del Estado Civil en los departamentos.

e) Los registradores municipales y sus delegados en las mesas de votación.

El registrador tenía como funciones: dirigir la Oficina Nacional de Identificación, vigilar la cedulación y el movimiento de las oficinas de los registradores del Estado Civil, en todo el país directamente, o por medio de sus delegados, investigar directamente o por medio de sus agentes cualquier irregularidad que se le denuncie en materia de cedulación o en la elaboración de censos electorales, sancionar conforme a las normas existentes, actuar como secretario permanente de la Corte Electoral, elegir los delegados de distinta filiación política (como garantía del pluralismo), dar su aprobación a los nombramientos de registradores municipales que lleven a cabo los delegados departamentales dentro de sus respectivas zonas.

Esta norma tenía por objeto responder a la violencia política que asolaba el país, lo cual buscaba evitar la influencia de los partidos en la expedición de los documentos de identidad, tal como lo prevé la norma y particularmente en la elaboración del censo electoral en las votaciones y en los escrutinios[19].

Así se garantiza el fortalecimiento de la democracia, de su transparencia y la promoción de la participación política. Por ello, se vio la necesidad de buscar un mecanismo por medio del cual se certifique, con instrumentos idóneos, la situación civil de las personas, y se buscó la creación de sistemas electorales donde se consigne la voluntad popular.

Ahora bien, como se observa la organización electoral se creó tal como se conoce actualmente, es decir compuesta por dos órganos "independientes": por un lado, la Corte Electoral que mencionamos al hacer referencia a la ley 96 de 1985, que luego se transforma en Consejo Nacional Electoral: Y la RNEC, que en la fecha administra los diversos registros oficiales de los colombianos de la vida civil y la organización de los procesos electorales.

Por ello, son principios orientadores de los intérpretes de las normas concernientes a los procesos electorales: el principio de la imparcialidad, principio del secreto del voto y de la publicidad del escrutinio, principio de la eficacia del voto, principio de la capacidad electoral y el principio de la proporcionalidad.

Así mismo, la ley 96 de 1985 autorizó para contratar una "misión técnica extranjera" que pudiera recomendar los sistemas que debían emplearse para la identificación de los colombianos y la elaboración de los censos electorales. En virtud de lo dispuesto por la ley, se contrató la Misión Técnica Canadiense la cual presentó

[19] Consultado el 23 febrero 2018. 8:40 am. *https://www.registraduria.gov.co/-Historia,3652-.html*

al Ministerio de Gobierno un informe en el que manifestó: "la centralización de los archivos dactiloscópico, alfabético, numérico, fotográfico y estadístico y la adopción de la cédula de ciudadanía laminada, que empezó a expedirse a partir de 1952"[20].

Esta misión propuso como recomendaciones:

a) La centralización de los archivos dactiloscópicos, alfabética, numérica, fotográfica y estadístico.

b) La adopción de un sistema de clasificación de la dactiloscopia.

c) La adopción de un sistema fotográfico.

d) La organización de una oficina principal de identificación con comisiones permanentes.

e) El establecimiento de cupos numéricos en los departamentos.

f) La adopción de una *cédula* laminada.

g) La elaboración de un censo electoral, con el fin de *brindar* seguridad jurídica a las personas habilitadas para sufragar en las elecciones[21].

El primer colombiano cedulado fue el entonces presidente de la República, Laureano Gómez Castro. Y en 1956 se expidió la primera cédula para una mujer, a Carola Correa de Rojas, esposa del General Rojas Pinilla, presidente de Colombia en ese momento. Posteriormente, en 1985 se expidió el decreto 2441 de 1986 (Código Electoral) que creó nuevas disposiciones en materia de identificación y electoral, que fueron acogidas por nuestra actual Constitución Política de 1991, en su título IX (De las elecciones y de la organización electoral), reiterando la necesidad de la autonomía de la función electoral de las tres ramas del poder público, dándole rango constitucional a la organización electoral[22].

Esto significa que la Registraduría Nacional del Estado Civil, es un organismo de rango constitucional conforme al artículo 120[23] de nuestra Carta Política, tiene a su cargo la organización de las elecciones, su dirección y vigilancia, así como lo relativo a la identidad de las personas, que forma parte de la organización electoral y su objeto es garantizar la transparencia y confiabilidad del proceso electoral de nuestro país, contribuyendo así a la realización del principio constitucional democrático, al ser neutral y objetivo.

[20] Consultado el 23 febrero 2018. 10:00 am. *https://www.registraduria.gov.co/-Historia,3652-.html*

[21] Consultado el 23 febrero 2018. 11:11 am. *http://es.calameo.com/read/002720339963a51c706de*

[22] Consultado el 23 febrero 2018. 10:00 am. *https://www.registraduria.gov.co/-Historia,3652-.html*

[23] Art. 120. "La organización electoral está conformada por el Consejo Nacional Electoral, por la Registraduría Nacional del Estado Civil y por los demás organismos que establezca la ley. Tiene a su cargo la organización de las elecciones, su dirección y vigilancia, así como lo relativo a la identidad de las personas".

Así mismo, promueve la participación social de los ciudadanos, tiene como facultad la promoción y garantía de cada situación que afecta la vida de los seres humanos que deba registrarse, que lo debe certificar por medio de los instrumentos que garanticen su confiabilidad y seguridad plena. Actualmente la RNEC es una de las instituciones más sólidas y no se pudiera concebir la vida democrática desde el punto de vista electoral y registral sin los importantes aportes institucionales que durante más de 70 años ha producido esta institución para Colombia.

b) *Estructura administrativa de la RNEC*. a') El decreto 1010 de 2000, "por el cual se establece la organización interna de la Registraduría Nacional del Estado Civil y se fijan las funciones de sus dependencias; se define la naturaleza jurídica del Fondo Social de Vivienda de la Registraduría Nacional del Estado Civil; y se dictan otras disposiciones".

Esta norma establece como objeto de la Registraduría Nacional del Estado Civil, registrar la vida civil e identificar a los colombianos, organizar los procesos electorales y los mecanismos de participación ciudadana, en orden a apoyar la administración de justicia y el fortalecimiento de la democracia. Así mismo, en su artículo 3º[24] establece que la Registraduría Nacional del Estado Civil es un órgano que de conformidad con el artículo 120 de la Constitución Política integra la Organización Electoral, y le corresponde la organización de las elecciones y los mecanismos de participación ciudadana, su dirección y vigilancia, así mismo debe regular lo relativo a la identidad de las personas y el registro civil.

La Registraduría Nacional del Estado Civil tiene como misión garantizar la organización y transparencia del proceso electoral, la oportunidad y confiabilidad de los escrutinios y resultados electorales. Contribuir al fortalecimiento de la democracia mediante su neutralidad y objetividad, promover la participación social en la cual se requiera la expresión de la voluntad popular mediante sistemas de tipo electoral en cualquiera de sus modalidades, así como promover y garantizar el registro de la situación civil de las personas, y que se pueda entregar información a quien pueda legalmente solicitarla y se certifique, mediante los instrumentos idóneos establecidos por las disposiciones legales y se garantice su confiabilidad y plena seguridad.

Respecto de la autonomía el decreto 1010 de 2000 en sus artículos 6º, 7º y 8º prevé tres tipos de autonomía, a saber:

[24] Art. 3º. "*Naturaleza*. La Registraduría Nacional del Estado Civil es un órgano de creación constitucional, que de conformidad con el artículo 120 de la Constitución Política forma parte integrante de la Organización Electoral, el cual contribuye, conjuntamente con las demás autoridades competentes, a la organización de las elecciones y los mecanismos de participación ciudadana, su dirección y vigilancia, así como lo relativo a la identidad de las personas y el registro civil, en los términos y condiciones que señala la ley y el presente decreto".

• *Autonomía administrativa*. En ejercicio de su autonomía administrativa le corresponde a la Organización Electoral y a la Registraduría Nacional del Estado Civil, definir todos los aspectos relacionados con el cumplimiento de sus funciones en armonía con los principios consagrados en la Constitución y en la ley.

• *Autonomía contractual*. En ejercicio de la autonomía contractual, el Registrador Nacional del Estado Civil *suscribe* los contratos que debe celebrar en cumplimiento de sus funciones, sin perjuicio de la delegación que al efecto realice conforme a lo dispuesto en las disposiciones legales.

• *Autonomía presupuestal*. La elaboración del presupuesto, con sujeción a lo establecido en el Estatuto Orgánico del Presupuesto, y demás aspectos relacionados con la gestión presupuestal, son consecuencia de la autonomía de la organización electoral, en armonía con lo dispuesto en el Código Electoral y las disposiciones orgánicas que regulan la materia.

La Corte Constitucional[25] en el caso específico de la Registraduría Nacional del Estado Civil define la autonomía como el autogobierno que tiene la entidad por lo que es autónoma y aun cuando, en principio, para el cumplimiento de sus funciones, no depende de la autorización o aprobación de otro órgano[26], no se puede desconocer que dicha autonomía no es contraria a la importancia que tiene la necesaria coordinación con el Consejo Nacional Electoral, de especial relevancia en ciertas materias.

[25] Corte Const., sent. C-230A de 2008, demanda de inconstitucionalidad en contra de los arts. 10 y 102 y de algunos apartes de los arts. 12, 26, 32, 40, 47, 75, 79, 85, 101, 149 y 157 del decr. 2241 de 1986, "por el cual se adopta el Código Electoral" y en contra del art. 11 del decr. 111 de 1996, "por el cual se compilan la ley 38 de 1989, la ley 179 de 1994 y la ley 225 de 1995 que conforman el Estatuto Orgánico del Presupuesto". Actores: Rodrigo Uprimny Yepes, Nathalia Carolina Sandoval Rojas, Pedro Santana Rodríguez y Omar Hernández. (M. P. Dr. Rodrigo Escobar Gil), 6 marzo 2008.

[26] Corte Const., sent. C-230A de 2008, cit. "La autonomía es una cualidad que distingue a quien es capaz de decidir por sí mismo y se predica de la persona individualmente considerada y también de las entidades u organismos públicos. Una de las principales características inherentes a la autonomía es la facultad de autogobierno, de la cual hace parte la autodeterminación administrativa, jurídica y presupuestal que les procure a las entidades autónomas «la consecución de los altos objetivos que les ha trazado el constituyente». Si bien la Registraduría Nacional del Estado Civil y el Consejo Nacional Electoral son autónomos, esa autonomía no implica la total inexistencia de relaciones entre las dos entidades que, al fin de cuentas, son miembros de una misma organización y deben actuar coordinadamente. En este orden de ideas y dado que la Constitución no configuró un sistema de separación presupuestal, nada se opone a que haya un presupuesto de toda la organización electoral y a que la iniciativa presupuestal propicie un diálogo alrededor del respectivo proyecto. La índole de las funciones atribuidas permite predicar el carácter técnico de la Registraduría Nacional del Estado Civil, pues la preparación y el desarrollo de las jornadas electorales exigen manejar conocimientos y criterios técnicos, cuya estricta aplicación es garantía de la imparcialidad y transparencia de su actuación, así como fundamento de la confianza de los distintos actores políticos y de la ciudadanía en general".

La Corte Constitucional resalta las diferentes características de la autonomía de la Registraduría Nacional del Estado Civil, las cuales se distinguen por la facultad de autogobierno, *de la que forma parte la autodeterminación administrativa, jurídica y presupuestal pues con ellas la entidad cuenta con los instrumentos para lograr los objetivos que determinó el constituyente.*

Las características de la autonomía en la Registraduría Nacional del Estado Civil son: a) la facultad de autogobierno; b) la autodeterminación administrativa; c) la autodeterminación jurídica; d) la autodeterminación presupuestal, y e) la imparcialidad.

El decreto 1010 de 2000 establece que la Registraduría Nacional del Estado Civil se organizará en dos niveles:

1. Nivel central: el nivel central está integrado por las dependencias cuya competencia es nacional.

2. Nivel desconcentrado: el nivel desconcentrado está constituido por las dependencias de la Registraduría Nacional cuya competencia está circunscrita a una circunscripción electoral específica o en los términos territoriales que comprendan el ejercicio de funciones inherentes a la Registraduría Nacional y se configura con observancia de los principios de la función administrativa. En dicho nivel se radican las competencias y funciones que determinan las disposiciones legales.

Al respecto, la Corte Constitucional, en sentencia C-205 de 2005, resaltó las características de la desconcentración, como una atribución de competencia, que debe ser de inferior jerarquía, exclusiva del designado, que atiende más a la transferencia de funciones radicadas en cabeza de órganos administrativos superiores a instituciones u organismos dependientes de ellos, sin que el titular de esas atribuciones pierda el control y la dirección política y administrativa en el desarrollo de esas funciones.

La corporación manifestó que las características principales de la desconcentración son: la atribución de la competencia que realiza el mismo ordenamiento jurídico, la atribución debe ser realizada a un órgano medio o inferior dentro de la jerarquía de la entidad, la competencia desconcentrada se confiere de forma exclusiva al órgano designado por el ordenamiento, la responsabilidad del superior jerárquico se limita al ámbito de los poderes de supervisión propios de la relación jerárquica y el superior solo puede reasumir la competencia previa atribución legal que así lo determine[27].

[27] Corte Const., sent. C-205 de 2005, demanda de inconstitucionalidad contra los arts. 35 (parcial) de la ley 510 de 1999 y 72 de la ley 795 de 2003. Demandante: Elson Rafael Rodríguez Beltrán (M. P. Dr. Jaime Córdoba Triviño), 8 marzo 2005. "Entre las características principales de la desconcentración están las siguientes:

b') *Decreto 1011 de 2000*. Este decreto establece el Sistema de Nomenclatura y Clasificación de los Empleos de la Registraduría Nacional del Estado Civil. Así mismo, establece la noción de empleo, clasificación de los empleos, naturaleza general de las funciones, nomenclatura, los requisitos generales para el ejercicio de los empleos, la experiencia, equivalencias entre estudios y experiencia, disciplinas académicas y equivalencias para la incorporación.

c') *Decreto 1012 de 2000*, por el cual se establece la planta de personal de la Registraduría Nacional del Estado Civil y se dictan otras disposiciones. Establece la estructura interna de la planta de personal de la RNEC.

d') *Decreto 1013 de 2000*, por el cual se fija el sistema de remuneración de los empleos de la Registraduría Nacional del Estado Civil.

e') *Decreto 1014 de 2000*, por el cual se dictan las normas del régimen específico de carrera administrativa de la Registraduría Nacional del Estado Civil y se expiden otras disposiciones en materia de administración de personal.

Estos decretos contienen la organización interna de la entidad, las funciones de cada una de sus dependencias, su planta de personal y los diferentes niveles de la entidad.

Ahora bien, las cuestiones relativas al documento de identificación de los ciudadanos son de suma importancia, pues de este se desprende el ejercicio de varios derechos civiles y políticos, por lo que trasciende a diferentes ámbitos jurídicos y sociales. Pero ¿a qué nos referimos cuando mencionamos la "identidad"? La conformación de la identidad de una persona es autónoma, lo que implica que cada persona tiene derecho a definir su identidad sexual y de género, y a que los datos consignados en el registro civil correspondan a su definición identitaria[28], es decir que se encuentra protegido por diferentes garantías constitucionales a partir de los derechos fundamentales que derivan de los atributos de la personalidad.

"i. es una atribución de la competencia realizada por el mismo ordenamiento jurídico;

"ii. tal atribución es realizada a un órgano medio o inferior dentro de la jerarquía;

"iii. la competencia desconcentrada se confiere de forma exclusiva al órgano designado por el ordenamiento;

"iv. la responsabilidad del superior jerárquico se circunscribe al ámbito de los poderes de supervisión propios de la relación jerárquica. y

"v. el superior solo puede reasumir la competencia previa una nueva atribución legal que así lo determine".

[28] Corte Const., sent. C-063 de 2015, acción de tutela presentada por Sara Valentina López Jiménez contra la Registraduría Nacional del Estado Civil, con vinculación oficiosa de la Notaría Doce del Círculo de Medellín, el Ministerio de Relaciones Exteriores y la Oficina de Pasaportes de la Gobernación de Antioquia (M. P. María Victoria Calle Correa), 13 febrero 2015.

2. La función electoral, una facultad misional y un derecho fundamental

Los organismos electorales son los que la Constitución de 1991 les otorgó, en su Título IX, la llamada función electoral. Estos cuentan con dependencias desconcentradas en las circunscripciones electorales. La organización electoral está integrada por el Consejo Nacional Electoral, por la Registraduría Nacional del Estado Civil y por los demás organismos que establezca la ley. Tiene a su cargo la organización de las elecciones, su dirección y vigilancia, así como lo relativo a la identidad de las personas[29]. Esta organización está integrada por la Registraduría Nacional del Estado Civil, el Consejo Nacional Electoral y demás órganos que determine la ley, quienes actúan con autonomía e independencia respecto de las ramas del poder público.

En su conjunto, la organización electoral responde a una función pública permanente y de carácter nacional, consistente en la administración del proceso electoral que comprende la preparación, organización, dirección, vigilancia y promoción de los procesos electorales, la realización de los escrutinios, la resolución de las impugnaciones y la declaración oficial de la elección.

Esta función debe ser independiente. Cualquier Estado democrático en el mundo define su forma de gobierno a partir de su organización política, y con el fin de garantizar la participación se debe crear un sistema de elección de representantes, es decir elegir sus mandatarios. En nuestro ordenamiento constitucional se configura con una doble dimensión: "derecho" y "función".

Esta dualidad forma parte del principio democrático. Al respecto la Corte Constitucional afirmó que el derecho de elegir y ser elegido, no tiene carácter absoluto, por lo que debe ser entendido en su doble dimensión "*derecho-función*". De esta forma, la formación de la voluntad política y el buen funcionamiento del sistema democrático plasmado en la Ley Fundamental de 1991 al no ser una facultad absoluta, no puede interpretarse aisladamente del conjunto de mecanismos de participación y control ciudadano previstos y establecidos en la Constitución y en la ley. En el caso de otros derechos fundamentales, su núcleo fija mínimos de actuación los cuales operan como barreras contra injerencias indebidas del poder de las ramas públicas o de otras personas, pero ello no lo excluyen de tener un desarrollo legal que delimite su forma de ejercicio, disfrute, y brinde plenas garantías[30].

[29] Const. Pol., art. 120.

[30] Corte Const., sent. T-510 de 2006, acciones de tutela instaurada por Carlos Antonio Ardila Ballesteros y Esteban Flórez Sierra contra la Sección Quinta, Sala de lo Contencioso Administrativo del Consejo de Estado y la Registraduría Nacional del Estado Civil (M. P. Dr. Álvaro Tafur Galvis), 6 julio 2006. "El derecho de elegir y ser elegido cuya tutela se demanda, no tiene carácter absoluto

Es así como conforme al principio democrático se configura la función electoral de suma importancia, más cuando constituye el mecanismo por medio del cual el soberano confiere al poder público su legitimidad, al elegir sus representantes. En un sistema democrático como el establecido desde la Constitución Política de 1991 que garantiza la participación, se debe proteger el goce de los derechos a elegir y ser elegido por los ciudadanos, pues ellos son titulares de la soberanía. Lo atinente a la función electoral se convierte en esa independencia que garantizan las ramas del poder público y los demás órganos constitucionales.

De esta suerte, la función electoral tiene gran significado en la estructura del Estado, y dentro de esta debe ser independiente con el fin de no dejarse influir por ningún agente externo y así lograr la efectiva participación del soberano. Dentro del ejercicio de la función electoral se deben garantizar los derechos y garantías de los órganos que integran la organización electoral de acuerdo con sus facultades constitucionales.

Colombia se define como un Estado social democrático y de derecho, para la ejecución de los fines que ordena la Ley Fundamental en el sentido de que el tipo de Estado se define así mismo como democrático, lo cual excluye toda expresión que contradiga tal mandato; ello es de singular trascendencia, pues significa la posibilidad de ejercer la democracia de forma representativa y directa. La estructura democrática de las instituciones prevalece como presupuesto democrático en el sentido de que por medio de sus facultades se ejercen los derechos inherentes a las personas.

Entre los derechos que garantizan la función electoral se encuentran: la libertad, como garantía de la voluntad política y su ejercicio; la igualdad, puesto que se debe garantizar que ningún ciudadano tenga más derechos que otros; la justicia, que busca la garantía de los derechos a la libertad e igualdad. Estos tres derechos son elementos vitales en una democracia, se garantiza la paz como único escenario de respeto por la dignidad humana, siendo este, principio y fin constitucional.

La Constitución de 1991 es el instrumento político normativo en el cual encontramos la delimitación de funciones, facultades, derechos, limitaciones a los

---

y debe ser entendido en su doble dimensión derecho-función, como una forma de contribución a la formación de la voluntad política y al buen funcionamiento del sistema democrático, sujeto a las condiciones fijadas en la Constitución y la ley. [...] En consecuencia, como derecho-función, no es una facultad absoluta, ni puede interpretarse de manera aislada del conjunto de mecanismos de participación y control ciudadano previstos en la propia Constitución y en la ley, pues su ejercicio precisa de las formas y condiciones establecidos para el efecto. Tal como ocurre con otros derechos fundamentales, su núcleo fija mínimos irreductibles de actuación llamados a operar como barrera contra interferencias indebidas del poder o de otras personas, pero que, en todo caso, no excluyen la posibilidad de tener un desarrollo legal que delimite su forma de ejercicio y disfrute".

derechos, garantías y obligaciones, así como las reglas de juego que se encuentran consagradas allí, con el fin de que todos participen, lo que implica que son reglas que cobijan a todos[31].

3. La función registral, una facultad misional y los derechos fundamentales derivados de la personalidad jurídica

En una investigación realizada por el Centro de Estudios en Democracia y Asuntos Electorales (CEDAE)[32] sobre la relación entre las facultades registrales y los derechos, considerados desde la supremacía constitucional, se advierte que el registro civil es aquel documento en el que, de forma precisa, constan todos los hechos que se deriven de la identidad, filiación y estado civil de las personas, desde que nacen hasta que mueren.

En el registro civil se consignan diferentes circunstancias que inciden en la vida civil como: nacimientos, reconocimiento de hijos, adopciones, matrimonios, separaciones, divorcios, defunciones y declaraciones de presunción de muerte. La existencia del registro permite exigir la garantía de derechos y el cumplimiento de sus deberes a toda persona, frente a la sociedad y a su círculo social cercano.

En la actualidad existen tres tipos de registro civil:

A) *Nacimiento*

Con este registro la persona nace a la vida jurídica; la existencia misma de la persona es reconocida por este medio. El registro de nacimiento es un derecho de todos los niños y niñas, que les permite ser reconocidos legalmente como personas. En él se consigna el nombre y un número único de *identificación* personal el cual le permite ser reconocido como sujeto de derecho frente al Estado y a la sociedad. Además, se le garantiza al menor la *identificación* de su filiación; es decir, se deja constancia de la línea familiar de donde desciende. Aunque el registro deja constancia de quiénes son los padres del recién nacido, también es posible el registro de personas de las que se desconocen sus padres.

B) *Matrimonio*

Es el medio con el que se legaliza la unión entre un hombre y una mujer frente al Estado. El registro de matrimonio es un requisito esencial para la existencia jurídica de la sociedad patrimonial en Colombia, independientemente del tipo de

[31] Manuel Tenorio Adame, *De la relación entre las facultades registrales y los derechos, a través de la de supremacía constitucional*, Bogotá, 2018,págs. 135-159..

[32] *Ibidem.*

rito por el cual se haya llevado a cabo. Con el matrimonio como figura jurídica, surgen derechos y obligaciones para los contrayentes, que solo pueden ser exigidos con el acta de registro que pruebe la existencia de la unión.

C) *Registro de defunción*

Se expide para acreditar el fallecimiento de una persona por muerte natural, muerte violenta o presunción de muerte, en los casos en los que ha sido dictado un fallo judicial que así lo establece. Con la muerte concluye también la vida civil de las personas y surgen para sus herederos los derechos sucesorales.

Ahora bien, de los tres anteriores, solo el registro civil de nacimiento constituye un documento de identidad. A continuación, haremos una breve explicación de los únicos documentos válidos como certificados de identidad en la medida en que estos tienen suma importancia en el tratamiento de los datos personales.

a) *Del registro civil de nacimiento como documento de identidad*. La inscripción de una persona en el registro civil de nacimiento permite reconocer su existencia legal e individualizar con la designación de un nombre, de ordinario por los padres del menor, y con un número único de identificación personal otorgado por la RNEC (NUIP). Este registro permite que a la persona le sean reconocidos sus derechos y deberes como colombiano y frente a otros Estados, y le permite acceder a los bienes y servicios del Estado, además de ser reconocido por la sociedad. Constituye el primer reconocimiento jurídico como atributo de la personalidad.

Requisitos:

a) Conocer el grupo sanguíneo y el factor RH de la persona cuyo nacimiento va a ser inscrito.

b) Presentar a la persona que se va a registrar y acreditar su nacimiento con un certificado médico de nacido vivo, expedido por el centro hospitalario o por el médico o enfermera que haya asistido a la madre en el parto si el bebé tiene un mes de nacido o menos.

c) Si no se cuenta con el certificado de nacido vivo, se puede hacer la inscripción con declaración bajo juramento de dos testigos hábiles que hayan presenciado el hecho o hayan tenido noticia directa y fidedigna de él. El juramento se entenderá prestado por el solo hecho de la firma o la partida de bautizo, acompañada de la certificación de la competencia del párroco que celebró el bautismo, o la anotación de origen religioso acompañada del certificado expedido por el representante legal de la iglesia.

d) Presentar los documentos de identificación del denunciante y los testigos, de ser el caso.

e) Si el nacimiento ocurre en el extranjero, con el acta de nacimiento traducida oficialmente, si ha sido expedida en idioma diferente al español y apostillada o legalizada según corresponda[33].

b) *Tarjeta de identidad*. El formato de tarjeta de identidad vigente, tiene las mismas especificaciones técnicas y condiciones de seguridad que la cédula de ciudadanía. El formato biométrico de tarjeta de identidad trae en su anverso un código de barras bidimensional con la información biométrica del titular, lo cual impide la falsificación del documento.

Incluye la siguiente información: a) fotografía a color; b) firma; c) huella dactilar; d) lugar y fecha de nacimiento, y e) lugar y fecha de expedición.

La tarjeta de identidad contiene microtextos, impresión irisada y papel de seguridad, lo cual brinda mayores estándares de invulnerabilidad.

c) *Cédula de ciudadanía*. Desde mayo de 2000, se expide el actual formato de cédula de ciudadanía, basado en la tecnología AFIS (Automated Fingerprint Identification System), que ayuda a la verificación automática de la identidad de las personas a partir de la comparación de las huellas dactilares. Este sistema busca impedir casos de múltiple cedulación, es decir, que se le otorguen dos cédulas con identidades diferentes a una misma persona.

Este documento de identidad posee características físicas y tecnológicas que reducen al mínimo las posibilidades de falsificación, como:

a) Holograma laminado.

b) Fondo de seguridad antifotográfo.

c) Impresa con tintas metálicas micro texto.

d) Código de barras que contiene un algoritmo de seguridad, la información biográfica del ciudadano y la información biométrica de la huella dactilar.

A partir del 1º de enero de 2010, este es el único documento de identificación válido para todos los colombianos mayores de edad.

Como se advierte, los tres registros mencionados involucran a todos los colombianos, lo cual hace de la RNEC la principal institución del Estado colombiano que trata datos personales con 49’582.748[34] habitantes aproximadamente, con fundamento en los artículos 120, 262 y 263 de la Constitución. Así, el tratamiento de datos personales por la RNEC se convierte en parte esencial del núcleo de sus funciones constitucionales que deriva en la autonomía misional que le otorga la Constitución según lo han determinado las sentencias C-401 de 2001 y C-230 de 2008.

[33] *Ibidem*.

[34] *http://countrymeters.info/es/Colombia*

4. El tratamiento de datos personales y el "habeas data" en Colombia

A) *Consagración constitucional*

Constitucionalmente el derecho a la intimidad y al buen nombre, de los cuales deriva el derecho fundamental autónomo[35] al *habeas data*, están garantizados en el artículo 15 Constitucional:

"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 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. Solo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

"Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley."

Del artículo 15 superior se desprenden diferentes disposiciones normativas:

a) "Todas las personas tienen derecho a su intimidad personal y familiar". Todas las personas, independientemente de su origen, sexo, raza, etc., son titulares del derecho a la intimidad el cual hace referencia al ámbito particular de cada individuo como sujeto de derechos y obligaciones o a la familia como núcleo esencial de la sociedad. Está disposición normativa hace referencia a aquellos fenómenos, comportamientos, datos y situaciones que normalmente no son puestos en conocimiento de extraños. Lo íntimo, lo realmente privado y personal de los seres humanos es un derecho fundamental que faculta al individuo a no promulgar,

[35] Corte Const., sent. T-176A de 2014, acción de tutela instaurada por Robinson Blanco Parra, contra Transporte Humadea S. A., Defencarga y Colfecar. Derechos fundamentales invocados: trabajo, habeas data, mínimo vital (M. P. Jorge Ignacio Pretelt Chaljub), 25 marzo 2014: "El reconocimiento del derecho fundamental autónomo al habeas data, busca la protección de los datos personales en un universo globalizado en el que el poder informático es creciente. Esta protección responde a la importancia que tales datos revisten para la garantía de otros derechos como la intimidad, el buen nombre, el libre desarrollo de la personalidad, entre otros. Sin embargo, el que exista una estrecha relación con tales derechos, no significa que no sea un derecho diferente, en tanto conlleva una serie de garantías diferenciables, cuya protección es directamente reclamable por medio de la acción de tutela, sin prejuicio del principio de subsidiariedad que rige la procedencia de la acción".

publicar o dar a conocer a terceros tales circunstancias a no ser que, por voluntad del titular, trasciendan al dominio de la opinión pública[36].

b) "A su buen nombre". Patrimonio jurídico fundamental y personalísimo pues hace referencia directa a las valoraciones que del individuo se hacen en la sociedad. Esta garantía es inescindible de todos los actos y hechos que una persona realice para que con fundamento en ellos la sociedad haga un juicio de valor. Aunque está íntimamente relacionado con la honra, es un derecho que busca establecer un papel del individuo dentro de la sociedad[37].

c) "El Estado debe respetarlos y hacerlos respetar". Disposición que le impone una doble carga al Estado: la primera nos indica que tiene un deber de respeto por el ejercicio del derecho, y la segunda que, así como debe respetarlo también debe velar por que los demás respeten el ejercicio del derecho y brinden garantías para el pleno y efectivo ejercicio del derecho[38]. Nótese que la obligación es para el

[36] Corte Const., sent. SU-056 de 1995, demandados: Germán Castro Caycedo, Lucrecia Gaviria Diez y Editorial Planeta (M. P. Antonio Barrera Carbonell), 16 febrero 1995: "El derecho a la intimidad hace referencia al ámbito personalísimo de cada individuo o familia, es decir, a aquellos fenómenos, comportamientos, datos y situaciones que normalmente están sustraídos a la injerencia o al conocimiento de extraños. Lo íntimo, lo realmente privado y personalísimo de las personas es, como lo ha señalado en múltiples oportunidades esta Corte, un derecho fundamental del ser humano, y debe mantener esa condición, es decir, pertenecer a una esfera o a un ámbito reservado, no conocido, no sabido, no promulgado, a menos que los hechos o circunstancias relevantes concernientes a dicha intimidad sean conocidos por terceros por voluntad del titular del derecho o porque han trascendido al dominio de la opinión pública".

[37] "Es un derecho personalísimo toda vez que hace referencia directa a las valoraciones que tanto individual como colectivamente se hagan de una persona. Este derecho está atado a todos los actos y hechos que una persona realice para que a través de ellos la sociedad haga un juicio de valor sobre la real dimensión de bondades, virtudes y defectos los cuales a través de su existencia muestra como crédito una persona. El concepto del buen nombre es exterior y algunos tratadistas ven este derecho concatenado e íntimamente relacionado con el derecho a la honra. Es amplio en su concepción, no tiene límites en cuanto a su aplicabilidad y por ello entre más actos puedan valorarse respecto de la conducta de la persona, se tienen mejores elementos de juicio para ponderar su personalidad y asignarle un puesto dentro de la escala de valoración social del buen comportamiento que al efecto ha creado el hombre".

[38] Corte Const., sent. T-444 de 1992, peticionaria: Jackeline Campos Rincón, procedencia: Juzgado 29 Superior de Santa Fe de Bogotá (M. P. Alejandro Martínez Caballero), 7 julio 1992: "La regla general debe ser, en consecuencia, que como el Estado tiene por misión el servicio a todas las personas, para ello debe dotarse, respetando los derechos humanos y el debido proceso, de idóneas herramientas que le permitan mantener un clima de paz y convivencia, de suerte que pueda incluso recopilar y archivar información sobre una persona, en el marco de sus legítimas y democráticas funciones, siempre y cuando no divulgue ni dé a la publicidad por ningún medio la información sobre esa persona, salvo el evento que ella tenga antecedentes penales o contravencionales, esto es, que tenga una condena proferida en sentencia judicial definitiva, como lo dispone el artículo 248 constitucional, que se reproduce en el artículo 12 del Código de Procedimiento Penal, como principio rector del nuevo ordenamiento procedimental.

Estado en su conjunto, lo cual tiene implicaciones jurídicas nacionales e internacionales de gran envergadura.

d) "De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas". Esta disposición es el núcleo esencial del derecho de *habeas data*, que busca garantizar que el titular de la información que es administrada por el sujeto obligado pueda ser conocida, actualizada y rectificada por su titular. La línea jurisprudencial sobre el derecho al habeas data creada en la Corte Constitucional actualmente afirma que el derecho cuenta con un núcleo esencial autónomo que se compone de la autodeterminación informática y la libertad, donde se han establecido contenidos mínimos:

I. El derecho de las personas a *conocer* la información que sobre ellas reposa en las bases de datos.

II. El derecho a incluir nuevos datos con el fin de que se *actualice* la información.

III. El derecho de *rectificar y corregir* la información.

IV. El derecho a *excluir* información de una base de datos que sea indebidamente utilizada[39].

e) "En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución". Esta obligación es impuesta por el constituyente al sujeto obligado y a la autoridad de protección de datos, pues en su tratamiento y en la vigilancia del mismo se deben garantizar los postulados normativos y jurisprudenciales, en un entorno constitucional total[40].

[39] Corte Const., sent. T-260 de 2012, acción de tutela instaurada por AA, en representación de su menor hija XX contra BB (M. P. Humberto Antonio Sierra Porto), 29 marzo 2012: La línea jurisprudencial sobre el derecho al habeas data tiene tres etapas en el precedente constitucional. Una primera fase en la que se consideró que este derecho era una garantía de la intimidad. En un segundo período se concibió al *habeas data* como una manifestación del libre desarrollo de la personalidad. En el estado actual de la jurisprudencia se ha advertido que el referido derecho cuenta con un núcleo esencial autónomo que se compone de la autodeterminación informática y la libertad, del cual se derivan los siguientes contenidos mínimos: i) el derecho de las personas a conocer la información que sobre ellas reposa en las bases de datos; ii) el derecho a incluir nuevos datos con el fin de que se registre una imagen completa del titular; iii) el derecho a actualizar la información que se halla en los archivos; iv) el derecho a que la información contenida sea rectificada y corregida, y v) el derecho a excluir información de una base de datos que sea indebidamente utilizada o por voluntad del titular, salvo las excepciones legales.

[40] Corte Const., sent. C-748 de 2011, control constitucional del Proyecto de Ley Estatutaria 184 de 2010 Senado; 046 de 2010 Cámara, "por la cual se dictan disposiciones generales para la protección de datos personales" (M. P. Jorge Ignacio Pretelt Chaljub), 6 octubre 2011. Es cierto que el legislador estatutario hizo un esfuerzo por describir los deberes que le asisten a uno y otro sujeto que participan en el tratamiento del dato, pero ello no significa que el titular del derecho no pueda exigir otros que puedan resultar para su plena garantía en concordancia con los principios

Así, los titulares de los datos personales, los sujetos obligados y las autoridades encargadas de la vigilancia de la relación jurídica se deben regir por los criterios que consagra la Constitución Política de Colombia.

f) "La correspondencia y demás formas de comunicación privada son inviolables. Solo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley".

En esta disposición se garantiza la inviolabilidad de las comunicaciones, con el fin de proteger los derechos constitucionales derivados de la intimidad de las personas. La única forma de registrar las comunicaciones privadas es por medio de orden judicial[41].

g) "Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley". Por último, en esta disposición se impone una obligación a las sociedades, como personas jurídicas, fundadas en el control que de ellas debe hacerse con el fin de garantizar su ejercicio lícito[42].

La protección de datos personales en su vertiente de intimidad o de *habeas data* ya sea como obligación, facultad o como derecho debe tener un entorno constitu-

---

que regulan la administración de datos. En otras palabras, los deberes enunciados en los artículos bajo estudio, respecto del titular del derecho al habeas data, no son taxativos sino enunciativos, lo que significa que responsables y encargados tendrán otros deberes derivados del derecho al habeas data, que corresponderán a las prerrogativas que otorga el derecho, en tanto sujetos pasivos de dicha garantía constitucional.

[41] Corte Const., sent. C-748 de 2011, demanda de inconstitucionalidad contra el art. 52 (parcial) de la ley 1453 de 2011 "por medio de la cual se reforma el Código Penal, el Código de Procedimiento Penal, el Código de Infancia y Adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad", actor: Dagoberto José Lavalle Navarro (M. P. Jorge Ignacio Pretelt Chaljub), 20 agosto 2014:."El artículo 15 de la Constitución establece una serie de garantías para su protección: (i) el deber del Estado y de los particulares de respetarlo; (ii) la inviolabilidad de la correspondencia y demás formas de comunicación privada, salvo el registro o la interceptación por orden judicial, en los casos y con las formalidades de ley, y (iii) la reserva de libros de contabilidad y demás documentos privados, salvo su exigibilidad para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado, «en los términos que señale la ley»".

[42] Corte Const., sent. T-181 de 2014, accionante: Empresa de Telecomunicaciones de Bogotá S. A. E.S.P. -ETB S.A. E.S.P. Accionados: Tribunal Administrativo de Cundinamarca -Sección Primera, Subsección A- (M. P. Mauricio González Cuervo). Cuando se trate de documentos de carácter privado, contrario a lo dispuesto para el acceso a los documentos públicos, la regla general es la reserva, en tanto la ley no disponga excepcionalmente su exhibición o la expedición de copias. En ese sentido, el artículo 15 de la Carta Política, en el inciso 4º establece que "Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley".

cional total, en el sentido de que se debe visualizar como prerrogativa individual del gobernado o función institucional. Por ejemplo, lo que puede ser la regla del derecho fundamental al *habeas data* prevista en el artículo 15 superior, puede ser una excepción al derecho de petición reglamentado en el artículo 23 constitucional o el acceso a la información del artículo 74 fundamental, todos ellos derechos fundamentales, por lo que la cuestión adquiere magnitudes complejas derivadas de su sincronización constitucional compuesta por varios derechos y facultades a la vez. La interpretación conjunta de esta triple relación entre el titular de los datos personales, el sujeto obligado que los trata y las autoridades que intervienen en esta relación debe ceñirse a un entorno de constitucionalidad de forma total, lo que implica una interpretación holística de la Ley Fundamental[43].

B) *El derecho del habeas data y la RNEC*

Conforme a lo anterior, la Registraduría Nacional del Estado Civil es el mayor administrador de datos del país, pues administra los datos de cada una de las personas de nacionalidad colombiana y de los residentes en nuestro país, desde su origen, es decir el nacimiento (registro civil de nacimiento) hasta su final (registro civil de defunción), pero a su vez actúa como órgano constitucional autónomo dotado de *imperium*, con facultades que se fundamentan desde el punto de vista constitucional, de forma total.

La RNEC como principal sujeto obligado, tratante, recolector y administrador de datos personales de Colombia se encuentra sujeto a las obligaciones derivadas de la Constitución, la ley y la jurisprudencia, con el fin de garantizar los derechos relativos al tratamiento de datos personales y aquellos que puedan verse afectados por este.

Ahora bien, qué es un dato. El diccionario de la Real Academia Española da la siguiente definición:

Del lat. *datum* 'lo que se da'. 1. m. Información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho. A este problema le faltan datos numéricos.

2. m. Documento, testimonio, fundamento.3. m. Inform. Información dispuesta de manera adecuada para su tratamiento por una computadora"[44].

En la ley 1581 de 2012 (art. 3º), "por la cual se dictan disposiciones generales para la protección de datos personales", se define el dato personal como: "Cualquier

[43] Manuel Tenorio Adame, "La protección de datos personales desde el derecho al acceso a la información y como derecho fundamental autónomo, el caso mexicano", en *Revista Internacional de Protección de Datos Personales* , Bogotá, Universidad de los Andes, Facultad de Derecho, núm. 1, julio-diciembre de 2012.

[44] Consultado el 27 de febrero de 2018. 2:30 pm *http://dle.rae.es/?id=Bskzsq5|BsnXzV1*

información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables".

La Corte Constitucional mediante sentencia C-748 de 2011 señaló lo siguiente en relación con el dato personal:

"[E]n efecto, la jurisprudencia constitucional ha precisado que las características de los datos personales —en oposición a los impersonales— son las siguientes:

"i) estar referido a aspectos exclusivos y propios de una persona natural,

"ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos;

"iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita,

"iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación".

Estas definiciones mencionan el término *información*, lo que nos lleva a concluir que dato es todo aquello que nos permite obtener información del alguien, quien finalmente es el titular del dato. Jurídicamente, el concepto de dato personal es aquel que crea un vínculo entre un dato y una persona específica; de la relación que exista entre ambos (persona-dato) se deriva la concepción de datos personales.

La RNEC, es la entidad que maneja la mayor cantidad de datos en Colombia. Los registros de nacimiento, matrimonio y defunción, en sus distintas vertientes, constituye la base de datos pública más importante del país. En ellos se registran la forma como se define de manera autónoma a los colombianos en su identidad sexual, de género, nombre, fecha de nacimiento, matrimonio y defunción, entre otros. Los datos consignados en estos tres registros corresponden a su identidad como persona y frente a la sociedad.[45]

[45] Corte Const., sent. T-063 de 2015, acción de tutela presentada por Sara Valentina López Jiménez contra la Registraduría Nacional del Estado Civil, con vinculación oficiosa de la Notaría Doce del Círculo de Medellín, el Ministerio de Relaciones Exteriores y la Oficina de Pasaportes de la Gobernación de Antioquia (M. P. María Victoria Calle Correa), 13 febrero 2015: "El derecho de cada persona a definir de manera autónoma su identidad sexual y de género y a que los datos consignados en el registro civil correspondan a su definición identitaria, se encuentra constitucionalmente protegido por las disposiciones que garantizan el libre desarrollo de la personalidad (art. 16 C. P.), el reconocimiento de la personalidad jurídica (art. 14 C. P.), y el respeto de la dignidad humana en las tres manifestaciones antes identificadas: (i) derecho a vivir como uno quiere; (ii) derecho a vivir bien; (iii) derecho a vivir sin humillaciones. En el presente caso se ven concernidas las tres dimensiones, especialmente la primera y la tercera, en tanto la falta de correspondencia entre la identidad sexual y de género que asume una persona y la que aparece registrada en sus documentos de identidad implica negarle una dimensión constitutiva de su autonomía personal (del derecho a vivir como uno quiera), lo que a su vez puede convertirse en objeto de rechazo y discriminación por los demás (derecho a vivir sin humillaciones) y a dificultarle las oportunidades laborales que le permitan acceder a las condiciones materiales necesarias para una vida digna (derecho a vivir bien)".

Las relaciones que se establecen entre el sujeto obligado al tratamiento de datos personales y los particulares adquieren características muy específicas, que se deben adaptar a un marco constitucional y legal preciso, bajo dos vertientes específicas derivadas del principio de legalidad consagrado en el artículo 6º del Texto Fundamental:

a) La RNEC como órgano autónomo constitucional envestida de facultades para actuar como tratante y protector de datos personales.

b) Las personas que por obligación y derecho depositan los datos personales tienen las prerrogativas propias de los derechos fundamentales.

a) *Principio pro homine*. Las reglas de convivencia de los seres humanos se traducen en valores o principios de los cuales emana el derecho para asegurar el respeto por los demás, por lo que en el caso del principio *pro homine*, la Convención Americana sobre Derechos Humanos suscrita en la Conferencia Especializada Interamericana sobre Derechos Humanos (San José, Costa Rica 7 al 22 de noviembre de 1969) ha establecido los mandatos para las garantías mínimas, que permitan el ejercicio de los derechos humanos. El máximo intérprete de la Convención es la Corte Interamericana de Derechos Humanos, que en opinión separada del juez Rodolfo E. Piza Escalante" resaltó la importancia del principio *pro homine* pues considera que es un criterio fundamental, pues es este el que conduce a la conclusión de que su exigibilidad inmediata e incondicional constituye una regla. Lo anterior, en cuanto al análisis del derecho de rectificación el cual, como lo mencionamos en acápites anteriores, forma parte del derecho de *habeas data*.

Así manifestó que como primer mandato normativo está el respeto de su honra, como segundo mandato tenemos la protección de la ley contra posibles ataques al mencionado derecho; ahora bien, en la Convención también se protege la libertad de pensamiento y de expresión, de los cuales son titulares "todas las personas" en su condición de individuos dentro de una sociedad. La Convención también establece cuál es su alcance concreto.

Es decir, el derecho de rectificación o de respuesta es tal que no impide respetar y garantizar, independientemente de la falta de una ley reglamentaria, mediante simples criterios de razonabilidad y la aplicación del principio ya mencionado, lo que implica que beneficia al hombre como sujeto de derechos[46].

[46] Opinión separada del juez Rodolfo E. Piza Escalante", en CIDH, Exigibilidad del derecho de rectificación o respuesta (arts. 14.1, 1.1 y 2 Convención Americana sobre Derechos Humanos), Opinión Consultiva oc-7/86 de 29 agosto 1986. "En primer lugar, dada mi interpretación de los artículos 1.1 y 2 de la Convención, es necesario aclarar las razones, en adición a las de la opinión principal, por las cuales considero que el artículo 14.1 establece un derecho de rectificación o respuesta exigible por sí mismo, sin necesidad de las «condiciones que establezca la ley» a que la misma disposición se refiere. En efecto, a mi juicio, el meollo de las preguntas 1 y 2 del Gobierno

La protección de los derechos en el mundo implica una serie de garantías mínimas que van mucho más allá que los derechos, denominados principios. En cuanto al *habeas data*, por ser un derecho fundamental, se ciñe a diferentes principios constitucionales, para el caso específico el principio *pro homine* se encuentra plasmado en los artículos 1º y 2º de nuestra Carta Política puesto que conforme al fin constitucional de garantizar el respecto de la dignidad humana se impone el deber de interpretación de las normas jurídicas de tal forma que sean más favorables al hombre y al ejercicio de sus derechos.

Al respecto, el alto intérprete constitucional sostiene que el Estado colombiano, en cumplimiento del respeto de la dignidad humana tiene la obligación de preferir la interpretación de la norma más favorable a la persona, garantizando no solo el principio y fin constitucional, sino que también implica una plena garantía de parámetros internacionales por los cuales se propende por el respecto de las garantías mínimas que debe dar un Estado a las personas[47].

---

de Costa Rica está en la determinación de si esa alusión subordina o no el derecho mismo, o su ejercicio, en términos tales que, sin esas condiciones legales, el derecho de rectificación o respuesta no impondría a los Estados el deber inmediato e incondicional de respetarlo y garantizarlo.

”En este aspecto, me parece que el criterio fundamental es el que impone la naturaleza misma de los derechos humanos, la cual obliga a interpretar extensivamente las normas que los consagran o amplían y restrictivamente las que los limitan o restringen. Ese criterio fundamental —principio *pro homine* del Derecho de los Derechos Humanos—, conduce a la conclusión de que su exigibilidad inmediata e incondicional es la regla, y su condicionamiento la excepción, de manera que si, en los términos en que está definido por la Convención el derecho de rectificación o respuesta, podría ser aplicado aun a falta de las referidas «condiciones que establezca la ley», es un derecho exigible *per se*. Este es el caso precisamente: el artículo 14.1 define este derecho, en primer lugar, como un corolario del derecho de toda persona al «respeto de su honra» y a «la protección de la ley contra (esas) injerencias o (esos) ataques» a su «honra y reputación» (art. 11) y, en cierto modo, también del propio derecho «a la libertad de pensamiento y de expresión» (art. 13), derechos ambos que tienen una significación especial, si no preeminente, dentro de los reconocidos por la Convención; en segundo, establece los criterios básicos para determinarlo en sus alcances concretos: su titular es «toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio a través de medios de difusión legalmente reglamentados y que se dirijan al público en general», y sus efectos son los de permitirle «efectuar por el mismo órgano de difusión su rectificación o respuesta», de lo cual es evidente que pueden deducirse otros, como los de que tal rectificación o respuesta se publique gratuitamente, lo antes posible y en lugar y con notoriedad equivalentes a los de la publicación causante del agravio, sin «coletillas» que la desvirtúen etc.; condiciones todas estas que, a falta de las establecidas expresamente por la ley, pueden ser determinadas con solo utilizar los criterios de razonabilidad que deben presidir toda interpretación del derecho”.

[47] Corte Const., sent. C-438 de 2013, demanda de inconstitucionalidad contra los arts. 17, 19 (parcial), 27 (parcial), 28 (parcial), 37 (parcial), 41 (parcial), 46 (parcial), 47 (parcial), 64 (parcial), 86 (parcial) y 88 (parcial) de la ley 1448 de 2011, demandantes: Marco Romero Silva y otros (M. P. Alberto Rojas Ríos), 10 julio 2013: “El Estado colombiano, a través de los jueces y demás asociados,

A partir de los argumentos expuestos por la Corte Constitucional, que en el caso del derecho fundamental del *habeas data*, es regla de interpretación normativa la aplicación de la norma más favorable para el ser humano, es decir la más garantista de sus derechos en materia de protección de datos personales.

b) *Principio de universalidad*. Es una característica de los derechos humanos en general, pues su universalidad nos permite aplicarlos a todos los hombres y mujeres, más allá de criterios temporales o espaciales.

Los derechos humanos son la manifestación directa de la dignidad que está íntimamente relacionada con el concepto de ser humano, de la persona en particular. Ahora bien, el principio de universalidad es un elemento central del Estado social y democrático de derecho, pues es este tipo de Estado el que genera la idea de universalidad lo que no debe implicar homogeneidad.

La universalidad es el instrumento por el cual se debe concretar el principio de la dignidad humana, reconociendo la posibilidad de diversas aplicaciones fundamentadas en diferentes personas, o grupos sociales o culturales, pues el ser parte de un conglomerado social organizado llamado Estado, no significa que se sea iguales; al contrario, cada una de ellas es un individuo auto determinado en su raza, sexo, ideología política entre otros, pues es así como estas diferencias no implican una aplicación diferente de los derechos de los cuales todos son titulares.

---

por estar fundado en el respeto de la dignidad humana (artículo 1º de la Constitución) y tener como fines garantizar la efectividad de los principios, derechos y deberes (artículo 2º), tiene la obligación de preferir, cuando existan dos interpretaciones posibles de una disposición, la que más favorezca la dignidad humana. Esta obligación se ha denominado por la doctrina y la jurisprudencia "principio de interpretación *pro homine* o «pro persona». A este principio se ha referido esta Corporación en los siguientes términos: «El principio de interpretación *pro homine*, impone aquella interpretación de las normas jurídicas que sea más favorable al hombre y sus derechos, esto es, la prevalencia de aquella interpretación que propenda por [*sic*] el respeto de la dignidad humana y consecuentemente por la protección, garantía y promoción de los derechos humanos y de los derechos fundamentales consagrados a nivel constitucional». Este es entonces un criterio de interpretación que se fundamenta en las obligaciones contenidas en los arts. 1º y 2º de la Constitución antes citados y en el artículo 93, según el cual los derechos y deberes contenidos en la Constitución se deben interpretar de conformidad con los tratados sobre derechos humanos ratificados por Colombia. En lo que tiene que ver con los derechos, los mencionados criterios hermenéuticos se estipulan en el artículo 5º del Pacto Internacional de Derechos Civiles y Políticos y en el artículo 29 de la Convención Americana sobre Derechos Humanos. Adicionalmente, se debe afirmar que estos criterios configuran un criterio de constitucionalidad, pues impiden que de una norma se desprendan interpretaciones restrictivas de los derechos fundamentales. El principio pro persona, impone que «sin excepción, entre dos o más posibles análisis de una situación, se prefiera [aquella] que resulte más garantista o que permita la aplicación de forma más amplia del derecho fundamental»".

Esta aplicación y ejercicio es universal y aunque está sujeta a las mismas reglas de juego, es el individuo quien las ejerce personalmente y las opone a la sociedad[48].

En materia de universalidad, la protección de datos personales significa entonces, la aplicación y ejercicio de los derechos, sin discriminación alguna, por lo que, en pro de la garantía de su derecho de intimidad, y lo que el ser humano considere íntimo, su aplicación universal tiene gran trascendencia pues a partir de ella, cualquier persona, sin importar el momento, origen, espacio, lugar, raza, sexo o cultura, puede ejercer su derecho. Lo aparentemente paradigmático entre la universalidad y el derecho a la protección de datos personales radica en que, si bien estos datos hacen relación a singularidades específicas de las personas, estas no pueden ser objeto de discriminación.

c) *Interdependencia*. La interdependencia refleja el vínculo de los derechos humanos pues entre ellos, se establece una relación recíproca, no se pueden ver como elementos aislados y en su conjunto garantizan el respeto por los criterios mínimos de una buena convivencia.

Por lo que de la interdependencia de los derechos podemos afirmar:

• Un derecho puede ser efectivo mediante la garantía de otros derechos.

• Dos derechos o más son mutuamente dependientes para su efectivo goce.

• Sin el respeto, la garantía, protección y promoción de uno de los derechos se traducirá en detrimento en otro (s) o viceversa.

[48] Corte Const., sent. C-063 de 2010, demanda de inconstitucionalidad contra el lit. i del art. 14 de la ley 1122 de 2007, actor: Emigdio Velasco Calambás (M. P. Dr. Humberto Antonio Sierra Porto), 4 febrero 2010: "Una noción característica de los derechos humanos es la universalidad de los mismos, es decir, la posibilidad de aplicarlos a todos los hombres y mujeres más allá de criterios temporales y espaciales. Esto en razón a que los derechos humanos son manifestación directa de la dignidad que está íntimamente relacionada con el concepto de ser humano. Los derechos de los grupos indígenas son uno de aquellos casos en donde el concepto de universalidad se denota como insuficiente para dar solución a las necesidades de protección existentes. No se trata ahora de un evento de oposición radical a las ideas de dignidad que propugnan los derechos humanos; tampoco de un particularismo tan especial que obligue a replantear el principio nuclear de los estos derechos. Simplemente, los sistemas pluriculturales han puesto de presente que la protección que es inherente a los derechos humanos exige el reconocimiento de un contenido especial, que sea acorde con una forma de vida que tiene su propio concepto acerca de ideales como la dignidad y la solidaridad. Son los mismos ideales, con un contenido no muy distante y una especial aplicación, los que resultan un reto ineludible para el principio de universalidad como elemento central del Estado social. En este tipo de Estado la idea de universalidad no debe implicar homogeneidad, entendiendo por esta una aplicación de derechos humanos fundados en principios y contenidos idénticos para grupos poblacionales diversos. Por el contrario, la universalidad debe concretar el principio de dignidad humana, reconociendo la posibilidad de aplicaciones diversas fundamentadas en, como en el caso de los indígenas, una especial cosmovisión que implica expresiones culturales, religiosas, políticas, organizativas diferentes a las de la cultura mayoritaria".

La Corte Constitucional ha manifestado que los derechos constitucionales son derechos fundamentales, pues cada uno de ellos se encuentra en una relación de garantía al principio de dignidad humana, base del Estado social de derecho[49].

Conclúyese que la interdependencia en el derecho de *habeas data* consiste en que puede ser efectivo mediante la garantía de otros derechos, como la intimidad personal y familiar; su goce efectivo se ve materializado en la protección de la honra, el buen nombre, entre otros.

d) *Progresividad*. La progresividad implica la gradualidad evolutiva de las garantías de los derechos; así como el hombre evoluciona con la sociedad, los derechos atienden a las necesidades que implican estos cambios. Los derechos no se materializan de un momento a otro, y para lograrlo el Estado o quien lo dirija debe establecer metas de corto y mediano plazo para su efectivo cumplimiento.

Este principio de contenido normativo definido por la jurisprudencia constitucional:

• Cuestiona la inacción estatal.

• Ordena dar pasos en dirección a la adopción de medidas constantes.

• Prohíbe los retrocesos.

• Exige que las medidas respeten el principio de igualdad y el mandato de no discriminación.

En concepto de la Corte Constitucional, estas obligaciones permiten que el Estado, en la medida de lo posible, genere herramientas para garantizar los derechos humanos. El principio de progresividad le impone al Estado la obligación de avanzar continuamente en la satisfacción de las facetas prestacionales de los

[49] Corte Const., sent. C-520 de 2016, demanda de inconstitucionalidad contra el num. 1 (parcial) del art. 4º de la ley 1678 de 2013, "por medio de la cual se garantiza la educación de posgrados al 0.1% de los mejores profesionales graduados en las instituciones de educación superior públicas y privadas del país" (M. P. María Victoria Calle Correa), 21 septiembre 2016:. "las propiedades de indivisibilidad e interdependencia que les son atribuibles. Por ende, se ha concluido que todos los derechos constitucionales son derechos fundamentales, pues cada uno de ellos encuentra un vínculo escindible con el principio de dignidad humana, fundante y justificativo del Estado social de derecho". Con base en tales consideraciones, afirmó al Corte en sent. C-288 de 2012, las propiedades de interdependencia e indivisibilidad han permitido concluir a la jurisprudencia constitucional que "los derechos fundamentales son aquellos que (i) se relacionan funcionalmente con la realización de la dignidad humana, (ii) pueden traducirse o concretarse en derechos subjetivos y (iii) sobre cuya fundamentalidad existen consensos dogmáticos, jurisprudenciales o de derecho internacional, legal y reglamentario"[35] A su vez, la posibilidad de "traducción en derechos fundamentales subjetivos es un asunto que debe analizarse en cada caso y hace referencia a la posibilidad de determinar la existencia de una posición jurídica subjetiva de carácter iusfundamental en el evento enjuiciado o de establecer si están plenamente definidos el titular, el obligado y el contenido o faceta del derecho solicitado por vía de tutela, a partir de los citados consensos".

derechos fundamentales, hasta donde sus capacidades lo permitan. Y como correlato de este principio, el Estado tiene prohibido retroceder en el índice alcanzado de protección de los derechos[50].

El principio de progresividad se desarrolló en la ley estatutaria de *habeas data* pues a partir de él se reglamentó el derecho fundamental y se idearon herramientas para garantizar su ejecución, lo que impone al Estado y a sus organismos, diferentes obligaciones y facultades en relación con el tratamiento del dato.

C) *Transversalidad de los derechos*

El *habeas data* al ser un derecho fundamental y autónomo, goza de plenas garantías conforme a nuestro ordenamiento constitucional, pero ello no significa que sea absoluto o que su ejecución sea completamente independiente. Dogmáticamente estos derechos gozan de las propiedades de indivisibilidad e interdependencia pues como lo manifestó al Corte Constitucional en sentencia C-520 de 2016 son derechos fundamentales aquellos que:

• Se relacionan funcionalmente con la realización de la dignidad humana, por medio de los cuales se garantiza su goce y ejercicio.

• Pueden traducirse o concretarse en derechos subjetivos, y su ejercicio lo garantiza el Estado.

• Su fundamentalidad se basa en consensos dogmáticos, jurisprudenciales o de derecho internacional, legal y reglamentario.

A su vez, la posible "traducción" en derechos fundamentales subjetivos es asunto que debe analizarse en cada caso y que hace referencia a la aptitud de determinar la existencia de una posición jurídica subjetiva de carácter *iusfundamental*, y cómo este implica específicamente la realización como ser humano de cada individuo[51].

[50] Corte Const., sent. T-774 de 2015, acciones de tutela instauradas de forma separada por Raúl, Roberto y Juan contra el Instituto de los Seguros Sociales y Colpensiones. Igualmente, por Simón contra la Sala Laboral de Descongestión del Tribunal Superior de Bogotá, el Instituto de los Seguros Sociales y BBVA Horizonte (M. P. Luis Ernesto Vargas Silva), 18 diciembre 2015.

[51] Corte Const., sent. C-520 de 2016, cit. En cuanto a los inconvenientes dogmáticos, la jurisprudencia constitucional ha llegado a un consenso, nutrido por las normas del derecho internacional de los derechos humanos, acerca de la aplicación en el plano de la protección de los derechos constitucionales, de las propiedades de indivisibilidad e interdependencia que les son atribuibles. "Por ende, se ha concluido que todos los derechos constitucionales son derechos fundamentales, pues cada uno de ellos encuentra un vínculo escindible con el principio de dignidad humana, fundante y justificativo del Estado social de derecho. Por lo tanto, la tesis de la conexidad entre los derechos sociales y los derechos fundamentales, como presupuesto para la justiciabilidad de aquellos, perdería sustento al preferirse esta visión integradora del carácter iusfundamental de los derechos. Así se señaló en la sentencia T-016/07, en la que la Corte planteó las condiciones teóricas para la fundamentalidad del derecho a la salud". Con fundamento en tales consideraciones, afirmó al Corte en sent. C-288

La transversalidad consiste en el efecto que tienen los derechos y principios de superar situaciones de hecho y materializar su aplicación obligatoria. Conforme a los diferentes principios universales de la aplicación de la dignidad humana como mínima garantía, ello implica una obligatoriedad de su real y efectivo goce y una responsabilidad ante su inaplicación.

La transversalidad se ve entonces, como una aplicación de "tipo imperativa y derivada natural por su condición de aplicabilidad inmediata"[52], de cualquier situación concreta donde se vea necesaria la intervención del Estado. Con el fin de materializarlo utiliza como instrumento el principio de igualdad, y demás garantías constitucionales, como las ya mencionadas.

En conclusión y con fundamento en la dogmática constitucional y universal ya expuesta, el derecho de *habeas data* es de carácter pleno y transversal en cuanto hace a la protección de los derechos fundamentales, pues estamos frente a una obligación positiva en cabeza de los Estados, es decir frente a los particulares, instituciones y organismos, pues es quien, en el término de sus facultades, brinda plenas garantías al ejercicio y goce de los derechos[53].

D) *De las obligaciones del tratamiento de datos personales aplicables a la Registraduría Nacional del Estado Civil*

Como ya observamos, la RNEC es una entidad de orden constitucional, autónoma e independiente de los órganos de las ramas del poder público, conforme al principio de legalidad, el cual plantea el cumplimiento de normas como la Constitución Política, las leyes y tratados internacionales, bien sean convenios o acuerdos, y los reglamentos, cualquiera que sea su rango. También comprende los principios generales de derecho, que incluso no se encuentran en las disposiciones legales ni en la costumbre. Al respecto la Corte Constitucional ha señalado que el principio de legalidad es, a su turno, principio rector del ejercicio del poder y

---

de 2012, que las propiedades de interdependencia e indivisibilidad le han permitido concluir a la jurisprudencia constitucional que "los derechos fundamentales son aquellos que "(i) se relacionan funcionalmente con la realización de la dignidad humana, (ii) pueden traducirse o concretarse en derechos subjetivos y (iii) sobre cuya fundamentalidad existen consensos dogmáticos, jurisprudenciales o de derecho internacional, legal y reglamentario. A su vez, la posibilidad de "traducción" en derechos fundamentales subjetivos es asunto que debe analizarse en cada caso y hace referencia a la posibilidad de determinar la existencia de una posición jurídica subjetiva de carácter iusfundamental en el evento enjuiciado o de establecer si están plenamente definidos el titular, el obligado y el contenido o faceta del derecho solicitado por vía de tutela, a partir de los citados consensos.

[52] Corte Const., sent. C-520 de 2016, cit.

[53] Consultado el 21 mayo 2018. 9:40 am. *http://wp000068.ferozo.com/RIDT2016/CHEDRESE.pdf*

por ende de las facultades. En este sentido, toda actuación se debe encontrar regulada y debe entenderse que no existe competencia, función o acto que pueda ser desarrollado por los servidores públicos que no esté definido "en forma expresa, clara y precisa en la ley"[54], por lo que existe un deber de sujeción de los servidores públicos al ordenamiento jurídico.

Las obligaciones constitucionales tienen dos cuestiones específicas:

• Las obligaciones derivadas de las facultades que tiene la RNEC en virtud de sus funciones misionales.

• Las derivadas de los derechos fundamentales. Recordemos que al hablar de derechos fundamentales se deben entender desde el punto de vista de la Constitución en su conjunto.

E*) Norma general sobre tratamiento de datos personales*

a) Ley 1581 de 2012, cuyo objeto es 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. De donde se pueden extraer aproximadamente 65 obligaciones legales directas y conexas a los administrados del dato pues esta norma regula la protección y demás garantías del tratamiento de datos personales.

b) Decreto 1377 de 2013, incorporado en el decreto 1074 de 2015, el cual tiene como objeto reglamentar parcialmente la ley 1581 de 2012, por la cual se dictan disposiciones generales sobre protección de datos personales. De él se pueden extraer aproximadamente 36 órdenes al administrador de los datos personales que es quien regula la protección y demás garantías desde el punto de vista reglamentario.

F) *Acceso a la información o transparencia*

a) La ley 1712 de 2014, cuyo objeto es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de dicha información. De esta norma se desprenden aproximadamente 14 obligaciones directas e indirectas para el administrador de los datos personales.

b) Decreto 103 de 2015, que reglamenta parcialmente la ley 1712 de 2014 y se dictan otras disposiciones. De esta norma se desprenden aproximadamente 8 obligaciones directas e indirectas para el administrador de los datos personales.

[54] Corte Const., sent. C-200 de 2002, demanda de inconstitucionalidad contra los arts. 40 y 43 (parcial) de la ley 153 de 1887, actor: Juan Pablo Anaya Santana (M. P. Dr. Álvaro tafur Galvis), 19 marzo 2002.

G) *Regulación para entidades con funciones públicas*

1. Obligaciones legales. La ley 594 de 2000, tiene por objeto establecer las reglas y principios generales que regulan la función archivística del Estado. De donde se desprenden aproximadamente 8 obligaciones para el administrador de los datos personales.

2. Obligaciones jurisprudenciales. Como se vio en acápites anteriores, las obligaciones del administrador del dato no están taxativamente enunciadas en las leyes, por lo que ha de recurrirse a la interpretación de la Constitución así como de las leyes. En ese sentido, la rama judicial con el fin de garantizar el efectivo ejercicio de los derechos y de los principios que rigen la ejecución de los fines constitucionales puede encontrar obligaciones a cargo del administrador del dato.

Dentro de esos pronunciamientos destacan los siguientes:

a) Sentencia C-1011 de 2008 (exp. PE-029, revisión de constitucionalidad del Proyecto de Ley Estatutaria No. 27/06 Senado - 221/07 Cámara (acum. 05/06 Senado) "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" (M. P. Dr. Jaime Córdoba Triviño), 16 octubre 2008. En ella se mencionan aproximadamente 15 obligaciones, y se establece la definición jurisprudencial del derecho al *habeas data* y su naturaleza autónoma, el carácter de la información, se definen la información pública y su acceso sin reserva y sin que se requiera autorización para ello, la información semiprivada y su acceso por orden de autoridad judicial o administrativa, entre otros.

b) Sentencia C-748 de 2011, sobre control constitucional al Proyecto de Ley Estatutaria 184 de 2010 Senado; 046 de 2010 Cámara, "por la cual se dictan disposiciones generales para la protección de datos personales" (M. P. Jorge Ignacio Pretelt Chaljub), 6 octubre 2011. En ella se plantean aproximadamente cinco obligaciones. En esta ocasión establecen los contenidos mínimos del derecho fundamental y se hace el análisis comparativo del modelo centralizado de protección de datos, sus características y del modelo sectorial de protección de datos y sus respectivas características.

c) Sentencia C-540 de 2012, revisión de constitucionalidad del proyecto de ley estatutaria 263/11 Senado y 195/11 Cámara, "por medio del cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones (M. P. Jorge Iván Palacio Palacio), 12 julio 2012. En ella se relacionan aproximadamente nueve obligaciones. Para la corporación era muy importante determinar que el derecho a la intimidad no es

absoluto. Manifiesta la Corte que sus limitaciones deben respetar principios de razonabilidad y proporcionalidad, por razones de "interés general, legítimas y debidamente justificadas constitucionalmente", y dichas limitaciones deben respetar los principios de razonabilidad y proporcionalidad en el contexto del sistema democrático. También se menciona el desarrollo de acceso a la información en la jurisprudencia de la Corte Interamericana de Derechos Humanos.

d) Sentencia C-602 de 2016, expediente D-11332, demanda de inconstitucionalidad contra el artículo 55 (parcial) del decreto 1355 de 1970 "por el cual se dictan normas sobre policía", actor: Luis Felipe Blanco Ortega (M. P. Alejandro Linares Cantillo), donde se encontraron aproximadamente cuatro obligaciones. La Corte Constitucional se ocupa en la importancia del derecho a obtener información completa, veraz, transparente, oportuna, verificable, comprensible, precisa e idónea.

e) Sentencia T-987 de 2012, acción de tutela interpuesta por Gustavo Quintero Navas contra Aerovías del Continente Americano S. A. – Avianca S. A. (M. P. Luis Ernesto Vargas Silva), 23 noviembre 2012. La corporación resalta la importancia de la prohibición de las denominadas "listas negras", en las bases de datos.

f) Sentencia T-592 de 2013, fallos de tutela objeto revisió;, sentencia del Juzgado Primero Civil del Circuito, Cartago (Valle), de 15 marzo 2013, que confirma la sentencia de primera instancia; y la sentencia del Juzgado Promiscuo Municipal de El Cairo (Valle), con función de control de garantías de 30 de enero de 2013, que negó el amparo constitucional. Accionante: Jaime Antonio Castrillón Giraldo; accionado: Alcaldía Municipal de El Cairo (Valle) (magistrados de la Sala Segunda de Revisión: Mauricio González Cuervo, Luis Guillermo Guerrero Pérez y Gabriel Eduardo Mendoza Martelo; M. P. Mauricio González Cuervo). Se encontró una obligación; para la Corte, los principios del habeas data implican una serie de deberes constitucionales para las entidades que custodian y administran la información personal contenida en archivos y bases de datos. Por lo que las entidades deben observar con detenimiento la obligación general de seguridad y diligencia en la administración y conservación de los datos personales y una obligación específica de corregir e indemnizar los perjuicios causados por el mal manejo que de la información se haga.

g) Sentencia T-058 de 2013, acción de tutela instaurada por AA contra la Universidad BB (M. P. Alexei Julio Estrada), 7 febrero 2013. Para la Corte es de real importancia que en materia de las autorizaciones, el consentimiento otorgado al encargado del tratamiento o responsable del tratamiento debe ser previo, expreso e informado, con el fin de no configurar una finalidad ilegal o inconstitucional que facilite la vulneración de derechos fundamentales.

Nota: todas las normas relacionadas en los puntos anteriores son de carácter enunciativo y no taxativo.

H) *De la relación biunívoca entre la protección de datos personales y las facultades de la RNEC*

Los planteamientos jurídicos cambian de forma muy rápida: lo que era válido normativamente en un tiempo más o menos cercano ya no lo es hoy, máxime si se observan las características de los sistemas democráticos en los que están inmersos la protección de datos personales y facultades otorgadas a órganos constitucionales autónomos. La Constitución de 1991 ha sido reformada al menos en 45 ocasiones por el Congreso, lo cual trae como consecuencia una desarticulación entre las facultades otorgadas a los órganos del Estado en las ramas del poder público o en los órganos autónomos constitucionales y los derechos inherentes a las personas que forman parte de su patrimonio jurídico.

La seguridad y certeza jurídica que se traduce en el principio de legalidad en el sentido de definir los actos de autoridad que gozan de *imperium*, los cuales traducen las facultades de la RNEC en cuanto hace a su misión y la definición de los derechos plasmada en la Constitución, hacen del sistema en su totalidad la piedra de toque del concepto democrático. La democracia se puede definir por la adecuada división de los poderes y del actuar de los órganos constitucionales autónomos, que se traduce en las facultades que acatan los que gobiernan, como en el ejercicio de los derechos de que gozan los gobernados.

Así las cosas, la desarticulación entre las prerrogativas jurídicas individuales y colectivas y las funciones atribuidas a los órganos constitucionales autónomos, implican una doble violación de Ley Fundamental en sus elementos mínimos. En primer lugar, en la parte orgánica que involucra la organización política de las instituciones que le dan sentido a la representación democrática y a la función de los órganos autónomos en sus atribuciones que, por su trascendencia, son reglados en el texto constitucional. En segundo lugar, los derechos de las personas son esas libertades individuales y colectivas que se traducen en derechos que son desarrollados por la Carta Política y que solo pueden ser limitados por ella misma. No seguir lo que se delimita constitucionalmente entre los derechos y las facultades implica esa doble violación.

Todas las constituciones tienen al menos tres elementos mínimos que deben ser consideradas leyes fundamentales: a) parte orgánica, b) parte dogmática, y c) supremacía.

A partir de estos elementos se crea un sistema político-jurídico que rige los destinos de toda sociedad que se limita a una circunscripción llamada Estado. Los cambios constitucionales, por importantes que sean, deben respetar la estructura jurídica derivada de la Ley Fundamental; si las facultades y los derechos no se encuentran acorde con el texto constitucional se entiende que están por fuera del

sistema jurídico y son declarados inconstitucionales, lo que explica la importancia de que exista una relación biunívoca entre facultades y derechos que implica una correspondencia a partir de las funciones de la institucionalidad y las libertades de los particulares que no sólo se limita a una dirección sino que es recíproca basada en el principio de supremacía constitucional.

Esta investigación busca establecer la relación entre cada una de las facultades en materia de registro civil e identificación y la función electoral que tiene su fundamento en la parte orgánica de la Constitución, relacionadas con los atributos de la personalidad, que finalmente derivan en derechos inherentes a los individuos y que encuentran su sustento en la parte dogmática de la Ley Superior, que tiene a su cargo la Registraduría Nacional del Estado Civil (RNEC), y que necesariamente pasan por el concepto de datos personales de los colombianos.

Para desarrollarla se busca el contenido, la delimitación y el alcance desde una perspectiva dogmática y orgánica del ordenamiento jurídico colombiano, el cual implica los ámbitos constitucional, legal y de derecho internacional, en lo relacionado con los datos personales que se traducen en derechos fundamentales subjetivos y que finalmente tienen que concretarse en las facultades que le son encomendadas a la RNEC, los cuales forman una relación biunívoca entre la parte orgánica y dogmática de la Constitución, materializando la idea de Estado social y democrático de derecho, de una forma sincrónica entre los derechos como patrimonio jurídico de los individuos y las facultades de las instituciones políticas.

En el artículo 266 de la Constitución Política de Colombia se establece que la RNEC tiene tres misiones esenciales: a) la registral, b) la electoral y c) la contractual.

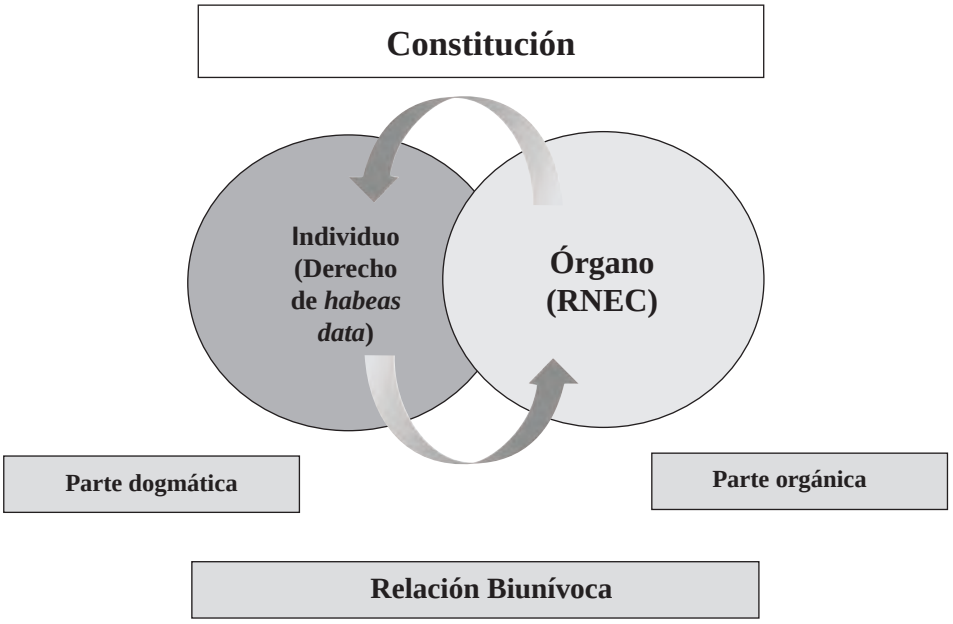
Esta investigación se concentra en la función registral y electoral, las atribuciones que tiene la institución derivada de ellas y los derechos que nacen a partir de las distintas modalidades que adoptan los atributos de la personalidad y los procesos electorales relacionados con la protección de los datos personales. No pretende hacer análisis relacionados con la función electoral, registral o contractual desde el punto de vista misional, sino que busca delimitar las funciones y su desarrollo por medio de la protección de los datos personales.

La teoría jurídica normalmente parte de la creación en la Constitución mediante facultades otorgadas a las ramas del poder público y a los órganos autónomos constitucionales, mediante leyes para el desarrollo de los derechos consagrados a las personas en el texto constitucional de forma positiva; sin embargo, en muchas ocasiones las facultades a dichas instituciones nacen a partir de criterios jurisprudenciales que le son ordenados a los órganos del Estado para que realicen sus funciones sin estar previstas legal o reglamentariamente.

Se busca hacer una relación directa y bidireccional entre las facultades y los derechos para así crear una sistematización, que cree certidumbre jurídica respecto del

actuar de las autoridades administrativas, pero que, al mismo tiempo, dé certeza al ejercicio de los derechos por los particulares, todo enmarcado en las funciones misionales de la RNEC y los datos personales de los colombianos.

Se establece que el derecho a la intimidad y a la protección de los datos personales es un fin constitucional. Ahora bien, se puede deducir que el concepto de este derecho constitucional autónomo no solo está inmerso como un fin constitucionalizado, sino que forma parte de esos valores que deben actuar en coordinación para obtener esos propósitos supremos. Es por lo anterior por lo que este concepto adquiere peso específico en la forma y estructura del sistema político constitucional, permeando en las distintas ramas del derecho, pues recordemos que por el principio de supremacía constitucional establecido en el artículo 4º de la Constitución de 1991, todas las normas se deben adaptar a los principios fundamentales allí plasmados.



Un factor esencial es la concepción de la protección de datos personales en nuestro sistema constitucional en sus vertientes de fin y valor, en virtud de que cada uno de estos preceptos contenidos en la Norma Fundamental forman parte de un sistema constitucional. Luego, al interpretarlos debe partirse por reconocer, como principio general, que el sentido que se les atribuya debe ser congruente con lo establecido en las diversas disposiciones constitucionales que integran ese sistema. Lo que se justifica por el hecho de que todos ellos se erigen en el criterio

de validez al tenor del cual se desarrolla el orden jurídico colombiano que es la Constitución Política de 1991, por lo que de aceptarse interpretaciones normativas que pudieran contradecir formalmente lo establecido en otras normas de la Constitución, se estaría atribuyendo a la voluntad soberana la intención de provocar grave incertidumbre entre los gobernados, situación que no corresponde a una correcta interpretación constitucional, porque ello implicaría regirse por una Norma Fundamental que es fuente de contradicciones; lo anterior sin perjuicio de que en ella puedan establecerse excepciones, las cuales deben preverse expresamente y no derivar de una interpretación que desatienda los fines del constituyente sino a una conclusión congruente y sistemática.

De este equilibrio del concepto constitucionalizado de la protección de datos personales se desprende claramente la relación biunívoca de este precepto en la parte orgánica y dogmática de nuestra Ley Fundamental, "la cual implica una correspondencia entre el ejercicio de las facultades de las instituciones y la participación de los ciudadanos mediante sus derechos de forma recíproca".

Así mismo, internacionalmente se han establecido diferentes criterios acerca de la administración y la protección de los datos personales, en especial en aquellas entidades que están encargadas de identificar a las personas. De esta suerte, en el siguiente capítulo resaltaremos las medidas normativas en tratamiento de datos personales en diferentes países y sus principales aspectos en documentos internacionales.

Capítulo II

ASPECTOS MEDULARES DEL TRATAMIENTO DE DATOS PERSONALES EN DOCUMENTOS INTERNACIONALES Y SU REGULACIÓN EN ALGUNOS PAÍSES LATINOAMERICANOS Y ESPAÑA

Para analizar el derecho comparado sobre el tratamiento de datos personales nos referiremos al proceso de armonización internacional desde la perspectiva de los principales documentos que han emitido organizaciones como la Red Iberoamericana de Protección de Datos (en adelante RIPD), la Unión Europea (UE), la Organización de Estados Americanos (OEA), la Organización para la Cooperación y el Desarrollo Económico (OCDE), la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (CIAPDP), el Foro de Cooperación Económica Asia Pacífico (APEC) y la Organización de las Naciones Unidas (ONU).

De dichos documentos enfatizamos lo atinente a los principios que deben observarse en el tratamiento de datos personales y los derechos de sus titulares. Unos y otros, elementos esenciales que debe considerar, aplicar y respetar cualquier responsable del tratamiento. No se describirá en detalle cada documento; apenas se subrayarán, en términos generales, los aspectos más relevantes.

Nos referiremos a ciertos antecedentes sobre el tratamiento de datos personales y luego nos enfocaremos en la armonización internacional sobre la materia, destacando su importancia y las principales entidades protagonistas. Luego se definen los principios generales y los derechos de los titulares, que comúnmente se denominan derechos ARCO, que surgen como consecuencia de la armonización internacional.

Utilizaremos tablas que nos ayudarán a sintetizar los principales temas y a evitar repeticiones innecesarias.

1. Del tratamiento de datos personales en documentos internacionales

A) *Antecedentes*

El tratamiento[1] de datos personales y el uso de bases de datos son actividades cotidianas e importantes para el Estado, las empresas y los particulares que requie-

[1] En este documento, las expresiones “tratar” o “tratamiento” se entenderán como cualquier operación o conjunto de operaciones aplicadas a datos personales, como la recolección, registro, organización, conservación, elaboración o modificación, extracción, indexación, consulta, utiliza-

ren dicha información para tomar decisiones de diversa naturaleza (económica, seguridad nacional, social, política, laboral, impuestos, estadísticas, profesional, académica, financiera, comercial, etc.). Los datos personales representan, en ciertos casos, el principal activo de aquellas empresas que se dedican a analizarlos, venderlos, alquilarlos o cederlos. En otros casos, se utilizan para tomar decisiones que afectan a las personas o para fijar políticas públicas, económicas, de riesgo, de marketing, entre otras.

Las TIC —*tecnologías de la información y la comunicación*—, por su parte, no solo son consideradas el "símbolo emblemático de la cultura contemporánea"[2] sino que han contribuido a la "datificación" de la sociedad contemporánea y a la consolidación del dato personal como el bien más apetecido de la economía digital.

El tratamiento de datos personales (en adelante TDP) es una de las cuestiones que en los últimos cincuenta años ha llamado la atención de los reguladores y de las organizaciones. En un principio su reglamentación fue prácticamente inexistente, pero en la última década presenciamos una eclosión mundial de normas sectoriales y generales, aunada a la revisión de las primeras iniciativas regulatorias, así como múltiples conferencias o debates en muy variados ámbitos, que ponen de presente la indiscutible relevancia social y económica del tratamiento de la información de las personas.

El derecho a la protección de datos personales que conocemos en 2018 ha sufrido cambios si consideramos sus primeras manifestaciones regulatorias de la década de los setenta y los documentos emitidos posteriormente. A los motivos iniciales que dieron origen a su reglamentación se sumaron otros factores que han hecho que los retos de la protección de este derecho sean diferentes a los previstos en sus orígenes.

La regulación sobre el derecho al debido tratamiento de los datos personales no solo tiene en cuenta los intereses del titular del dato sino que reconoce que esa información es necesaria para realizar muchas actividades lícitas, legítimas y de interés general o particular, según el caso. Por eso la normativa no se opone al tratamiento, sino que exige que esté rodeado de garantías mínimas para asegurar el correcto tratamiento de la información sobre las personas. En suma, la regulación no se opone al uso de los datos sino a su eventual abuso, porque ello puede constituirse en el hecho generador de la amenaza o vulneración de derechos humanos de los titulares de los datos.

---

ción, comunicación, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión, destrucción o desindexación.

[2] Aristeo García González, "La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado", en *Boletín Mexicano de Derecho Comparado*, núm. 120 , Ciudad de México, Universidad Nacional Autónoma de México, 2007, pág. 744.

Varios países cuentan con regulaciones generales y sectoriales así como con jurisprudencia sobre tratamiento de datos personales. Aunque se ha procurado armonizar internacionalmente los principales aspectos sobre el tratamiento de datos personales, en la práctica cada Estado expide normas que parcialmente siguen dichos documentos pero que están impregnadas de las particularidades sociales, políticas, culturales y jurídicas de cada uno, lo cual es inevitable. Además, cada sistema jurídico nacional cuenta con diversos instrumentos jurídicos (constitucionales, administrativos, judiciales, entre otros) para proteger el derecho al debido tratamiento de datos personales (en adelante DDTDP).

B) *Armonización internacional sobre el tratamiento de datos personales*

Resulta pretencioso intentar abordar en detalle todo lo atinente al tratamiento de datos personales desde la perspectiva del derecho comparado. No obstante, adviértase que a partir de los ochenta se identifica una labor muy importante de armonización internacional del derecho de la protección de datos personales[3].

Las respuestas normativas al tratamiento de datos personales se caracterizan por tener enfoque internacional y ser armonizadas. Por eso, la recolección, el almacenamiento, el uso, la circulación y demás actividades sobre los datos personales han sido objeto de una labor de armonización internacional regulatoria con miras a lograr un consenso jurídico coherente sobre temas cardinales de dicha materia[4]. En ese sentido, diferentes organizaciones internacionales, redes especializadas o grupos de autoridades han publicado documentos con reglas que deben observarse en el tratamiento de datos personales, dentro de las cuales se encuentran varios principios que evocan los grandes mensajes o propósitos que se deben materializar para lograr que los derechos de las personas no sean amenazados o vulnerados por la indebida recolección, almacenamiento, uso o circulación de la información.

En la siguiente tabla resumimos los principales documentos sobre tratamiento de datos personales que han aprobado diferentes organizaciones:

[3] Respecto del panorama internacional de la protección de datos personales puede consultarse de Nelson Remolina Angarita, *Data protection: panorama nacional e internacional*, en Internet, comercio electrónico y telecomunicaciones, Bogotá, Editorial Legis, 2002, págs. 99-172 .

[4] En la citada declaración de UE-EE.UU. sobre comercio electrónico, se puntualizó que "el papel de los gobiernos es proporcionar un marco legal claro y consistente, promover un entorno competitivo en el que el comercio electrónico pueda florecer y asegurar la protección adecuada de objetivos de interés público como la intimidad, los derechos de propiedad intelectual, la prevención del fraude, la protección del consumidor y la seguridad nacional".

ORGANIZACIÓN	PRINCIPALES DOCUMENTOS
Red Iberoamericana de Protección de Datos (RIPD)	Estándares de Protección de Datos Personales para los Estados Iberoamericanos (2017)
Unión Europea (UE)	(1) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril del 2016, relativo a la protección de las personas físicas en lo que respecta al 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); (2) Protocolos adicionales al Convenio 108 del Consejo para la protección de las personas respecto al tratamiento automatizado de datos de carácter tratamiento personal y relativo a la transferencia de datos (2001 y 2018); (3) Carta de los Derechos Fundamentales de la Unión Europea (2000); (4) Convenio 108 del Consejo para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal (1981)
Organización de Estados Americanos (OEA)	Principios de la OEA sobre la privacidad y la protección de datos personales con anotaciones (2015)
Organización para la Cooperación y el Desarrollo Económicos (OCDE)	Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales (2013, 1980)
Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (CIAPDP)	Estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal –Resolución de Madrid— (2009)
Foro de Cooperación Económica Asia Pacífico (APEC)	Marco de privacidad APEC (2004) APEC Cross Border Privacy Rules (CBPR) APEC Cros Border Privacy Enforcement Arrangement (CPEA)
Organización de las Naciones Unidas (ONU)	Resolución 45/95, de 14 de diciembre de 1990. Principios rectores para la reglamentación de los ficheros computadorizados de datos personales.

Tabla núm. 1. Principales organizaciones internacionales que han emitido documentos sobre tratamiento de datos personales

Fuente: elaboración de Nelson Remolina Angarita©

Los documentos enunciados son el fruto de la labor de armonización de los aspectos centrales del tratamiento de datos personales. En estos se procura asegurar unos mínimos en las actividades que impliquen la recolección, almacenamiento y uso de dicha información, estableciendo unos principios sobre la materia e imponiendo, en ciertos casos, criterios de comportamiento razonable. Dado su origen extranjero, reflejan conceptos, instituciones y finalidades de otras culturas y sistemas jurídicos que, según el país, pueden coincidir o ser consistentes con las tradiciones jurídicas locales. Muchos de ellos han sido el modelo o guía de referencia de normas locales y un referente para interpretar o suplir sus vacíos.

Es útil el análisis de estos documentos internacionales por varias razones: a) muestran que la protección de datos personales no es nueva y que no son crea-

ción original del legislador local sino fruto de una tendencia internacional para tratar de conciliar las necesidades de las empresas, de los Estados y el respeto de los derechos humanos; b) permiten determinar el origen y alcance de muchos términos, definiciones e instituciones utilizados en las regulaciones locales; c) proporcionan una idea de las tendencias de ciertos aspectos afines al tratamiento de datos personales y permiten tener una aproximación general a los principios e instituciones existentes en otras partes del mundo.

No obstante lo anterior, es necesario tener presente respecto de los documentos internacionales: a) las expresiones y alcances que le confieren a ciertos principios e instituciones no necesariamente coinciden con los términos de las regulaciones locales; b) no todos los documentos se ocupan de los mismos asuntos. Por ejemplo, la mayoría se refieren al principio de seguridad y a las reglas sobre transferencias internacionales, pero no todos definen qué es un dato personal, la autorización o el consentimiento; c) en algunos casos y para ciertas cuestiones los términos utilizados son muy amplios, poco claros y redactados en términos "gaseosos" que dificultan tener certeza objetiva acerca de lo que se quiere. Adicionalmente, las versiones originales de algunos documentos no fueron escritas en castellano y no existen, en todos los casos, versiones oficiales en dicho idioma. Finalmente, todas las organizaciones parten del supuesto de respetar derechos humanos pero la misión principal o razón de ser de algunas entidades son el crecimiento económico (APEC[5]), el bienestar económico y social (OCDE[6]), lo cual explica por qué en ciertos documentos se incluyen o excluyen algunas cuestiones o se hace énfasis en unas cosas y se dejan de lado otras.

Los documentos internacionales tienen origen en varias partes del mundo —Europa, Norteamérica, Latinoamérica— con dispares tradiciones jurídicas. Así las cosas, su interpretación y alcance deben considerar las diversas culturas jurídicas que están inmersas en cada texto. En otras palabras, si bien los textos establecen reglas generales aplicables al tratamiento de datos personales, estos fueron re-

[5] El Foro Económico Asia-Pacífico (APEC) tiene como principal objetivo apoyar el crecimiento económico sostenible y la prosperidad en la región Asia-Pacífico. Procuran defender el comercio y la inversión, promover y acelerar la integración económica regional, fomentar la cooperación económica y técnica, mejorar la seguridad humana, y facilitar un ambiente de negocios favorable y sostenible. (Cfr. *http://www.apec.org/About-Us/About-APEC/Mission-Statement.aspx* . Más información sobre APEC en: *http://www.apec.org/*

[6] La misión de la Organización para la Cooperación y el Desarrollo Económico (OCDE) es promover políticas que mejoren el bienestar económico y el bienestar social de las personas en todo el mundo. La OCDE es un foro en el que los gobiernos pueden trabajar juntos para compartir experiencias y buscar soluciones a problemas comunes e impulsar cambios económicos, sociales y medioambientales. (Cfr. *http://www.oecd.org/about/*. Más información sobre la OCDE en: *http://www.oecd.org/*

dactados en países con disímiles tradiciones jurídicas, condiciones económicas y políticas; siendo así, reflejan algunos conceptos comunes a varios sistemas jurídicos pero no reemplazan dichos sistemas ni borran absolutamente las normas, culturas y tradiciones jurídicas locales. En otras palabras, buscan armonizar mínimos para el tratamiento global de datos personales mas no unifican dichas reglas. Pese a lo anterior, recalcamos, no dejan de ser muy importantes y por ello haremos, cuando sea pertinente, las necesarias referencias a tales aspectos.

2. De los principios del tratamiento de datos en el contexto internacional

El respeto de los derechos de las personas cuando sus datos son tratados por terceros es el principal objetivo del derecho a la protección de los datos personales. ¿Cómo lograrlo? Exigiendo a los terceros un debido tratamiento de los datos personales. Recuérdese que "la protección de las personas respecto al tratamiento automatizado de datos de carácter personal"[7] forma parte del más antiguo instrumento jurídico internacional vinculante, ratificado por cuarenta y seis países: el Convenio 108 de 1981 del Consejo de Europa. Nótese que dicho Convenio no tiene como objeto proteger los datos sino "garantizar [...], a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales [...] con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona"[8].

Las regulaciones sobre tratamiento de datos personales no solo confieren facultades a los titulares de los datos (conocer, actualizar, corregir o eliminar) sino que se enfocan en exigir a quienes los poseen o administran (responsables, encargados o usuarios en general) una serie de requisitos y obligaciones dentro de las cuales se encuentra el deber de observar los principios sobre el tratamiento de datos personales. El desconocimiento de dichos principios implica, además de una infracción de la ley, una vulneración del debido proceso en el tratamiento de los datos.

Es necesario que el tratamiento sea debido (como sucede con el debido proceso), es decir, correcto o realizado conforme a la ley y que respete, entre otros, sus principios. No puede tratarse de cualquier tipo de tratamiento, pues debe ser

[7] Cfr. Consejo de Europa, 1981, Convenio 108 para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal.

[8] *Ibid*., art. 1. Ese mismo objetivo se replicó en el numeral 1 del art. 1 de la Directiva 95/46/CE según el cual "los Estados miembros garantizarán, [...], la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales".

correcto, ajustado a la ley y respetuoso de los derechos de las personas y de los principios establecidos para dicho efecto.

Así las cosas, en nuestra opinión, los principios cumplen varios objetivos:

1. Son un instrumento para garantizar el debido tratamiento de los datos personales y, por ende, el respeto de los derechos de los titulares de los datos.

2. Representan un límite al tratamiento de los datos personales en el sentido que no puede hacerse de cualquier manera sino de forma respetuosa de unos mínimos que son, precisamente, los principios.

3. Constituyen una herramienta de interpretación de la ley y de su aplicación correcta, así como el factor determinante de la solución de casos concretos que se sometan a consideración de las autoridades o de los jueces.

En efecto, para Ciro Angarita Barón, "los principios son normas que establecen un deber ser específico [...] y [...] tienen una mayor eficacia y, por lo tanto, una mayor capacidad para ser aplicados de manera directa e inmediata"[9]. Pese a los diversos significados del término "principios"[10], no debe perderse de vista que ellos recogen las ideas fundamentales que inspiran el derecho de la protección de datos. Como lo mencioné en otra ocasión, los principios "no son meras enunciaciones teóricas o elucubraciones retóricas sin uso práctico. Se trata de una serie de reglas materiales concebidas para desarrollar y asegurar la consecución de los fines de las normas sobre el tratamiento de datos. Estos principios tienen fuerza vinculante, aplicación práctica y son los que definen si un tratamiento de datos se está o no realizando de manera leal, lícita, transparente y adecuada"[11].

Así mismo, los principios son reglas fundamentales, de aplicación obligatoria, para garantizar el respeto de las personas cuando sus datos sean recolectados, almacenados, usados, circulados o cuando han sido objeto de cualquier actividad por parte de responsables o encargados del tratamiento. Por eso, señala la jurisprudencia que "los principios [...] consagran prescripciones jurídicas generales que suponen una delimitación política y axiológica reconocida y, en consecuencia, restringen el espacio de interpretación, lo cual hace de ellos normas de aplicación inmediata [...] Su alcance normativo no consiste en la enunciación de ideales que deben guiar los destinos institucionales y sociales con el objeto de que algún día se llegue a ellos; [...] Los principios expresan normas jurídicas para el presente; son el inicio del nuevo orden"[12]. En otras palabras, los principios son el camino

[9] Cfr. Corte Const., sent. T-406 de 1992 (M. P.Ciro Angarita Barón).

[10] Consúltese las múltiples definiciones de este término en el *Diccionario de la Lengua Española*.

[11] Cfr. Nelson Remolina Angarita, *Tratamiento de datos personales: aproximación internacional y comentarios a la ley 1581 de 2012*. (2013), Bogotá, Legis Editores, pág. 177.

[12] Cfr. Corte Const., sent. T-406 de 1992 (M. P. Ciro Angarita Barón).

que debe seguirse para garantizar la protección efectiva de los derechos de las personas cuando sus datos son tratados por terceros.

Los principios también pueden verse como los límites al tratamiento de los datos personales porque los responsables o encargados no pueden tratar esa información de cualquier manera sino respetando la ley y, por ende, sus principios. Refiriéndose a la función de estos, la jurisprudencia ha establecido definen "el contexto axiológico dentro del cual debe moverse el proceso informático. Según este marco general, existen unos parámetros [*sic*] generales que deben ser respetados para poder afirmar que el proceso de acopio, uso y difusión de datos personales sea constitucionalmente legítimo"[13].

Por otra parte, los principios no solo son instrumentos de obligatoria utilización y referencia en el desarrollo o reglamentación de la ley, sino que deben tenerse presentes para su interpretación y aplicación. En todos los casos, la ley se debe aplicar de manera armónica e integral conforme a los lineamientos que emergen de estos. En línea con lo anterior, la jurisprudencia ha señalado que "los principios [...] son una pauta de interpretación ineludible [...] y están dotados de toda la fuerza [...]. Sin embargo, no siempre son suficientes por sí solos para determinar la solución necesaria en un caso concreto"[14].

En la tabla de la página siguiente, destacaremos los principios contenidos en los documentos más emblemáticos que han emitido entidades internacionales en materia de tratamiento de datos personales:

Los documentos internacionales señalan de diversa manera el alcance de cada principio. Con miras a tener una aproximación a su contenido, nos referimos a los siguientes principios: legitimación, licitud, prevención del daño, lealtad, finalidad, proporcionalidad, elección, transparencia, calidad, responsabilidad, seguridad y confidencialidad[15]. Para el efecto, tendremos como principal referencia los "Estándares de protección de datos personales para los Estados Iberoamericanos"[16] de 2017, por tratarse del documento internacional más reciente y completo sobre la materia. No obstante, para algunos casos destacaremos temas puntuales como los principios de prevención del daño —*Preventing Harm*— y elección —*Choice*— contenidos en el APEC Privacy Framework de 2004.

[13] Cfr. Corte Const., sent. C-748 de 2011, num. 2.6.3.

[14] *Ibidem*.

[15] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 10.1.

[16] El texto oficial de los estándares puede consultarse en: *http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logo_RIPD.pdf*

PRINCIPIO	RIPD 2017	UE 2016	OEA 2015	OCDE 2013	CIAPDP 2009	APEC 2004	ONU 1990
Legitimación	✓	✓	✓	✓	✓	✓	X
Licitud	✓	✓	✓	✓	✓	✓	✓
Lealtad	✓	✓	✓	✓	✓	X	✓
Transparencia, aviso, apertura	✓	✓	✓	✓	✓	✓	X
Finalidad, uso limitado	✓	✓	✓	✓	✓	✓	✓
Proporcionalidad, pertinencia	✓	✓	✓	✓	✓	✓	X
Calidad, exactitud, veracidad	✓	✓	✓	✓	✓	✓	✓
Responsabilidad	✓	✓	✓	✓	✓	✓	X
Seguridad	✓	✓	✓	✓	✓	✓	✓
Confidencialidad	✓	✓	✓	X	✓	X	X
Temporalidad, caducidad	X	✓	✓	X	X	X	✓
Prevención del daño	X	X	X	X	X	✓	X
Elección	X	X	X	X	X	✓	X
No discriminación	X	X	X	X	X	X	✓

Tabla núm. 2. Principios sobre tratamiento de datos personales incorporados en los principales documentos internacionales

Dichos principios son de cardinal importancia a la hora de recolectar, almacenar, usar, circular o realizar cualquier actividad con datos personales. A continuación nos referiremos a estos principios, salvo el de responsabilidad demostrada que será objeto de estudio en capítulo aparte de esta obra:

A) *Principio de legitimación*

El principio se ocupa de establecer en qué situaciones el responsable está autorizado para tratar los datos personales. Para el efecto cita los siguientes supuestos que legitiman el tratamiento de datos por parte del responsable:

"a. El titular otorgue su consentimiento para una o varias finalidades específicas.

"b. El tratamiento sea necesario para el cumplimiento de una orden judicial, resolución o mandato fundado y motivado de autoridad pública competente.

"c. El tratamiento sea necesario para el ejercicio de facultades propias de las autoridades públicas o se realice en virtud de una habilitación legal.

”d. El tratamiento sea necesario para el reconocimiento o defensa de los derechos del titular ante una autoridad pública.

”e. El tratamiento sea necesario para la ejecución de un contrato o precontrato en el que el titular sea parte.

”f. El tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al responsable.

”g. El tratamiento sea necesario para proteger intereses vitales del titular o de otra persona física.

”h. El tratamiento sea necesario por razones de interés público establecidas o previstas en ley.

”i. El tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del titular que requiera la protección de datos personales, en particular cuando el titular sea niño, niña o adolescente”[17].

Sobre esta última hipótesis —intereses legítimos— se precisa que la misma no es aplicable a los tratamientos de datos personales realizados por las autoridades públicas en el ejercicio de sus funciones y que “se entenderá amparado por el interés legítimo el tratamiento de datos personales de contacto que sea imprescindible para la localización de personas físicas que prestan sus servicios al responsable, con la finalidad de mantener cualquier tipo de relación con esta”[18].

Como se observa, el consentimiento es uno de los elementos legitimadores del tratamiento. Es muy positivo que el consentimiento de la persona sea un factor legitimador del tratamiento de datos, pero es importante destacar que este no es un mecanismo de protección del titular sino una forma de reconocer que el ser humano es quien decide, por regla general, a quien entrega sus datos, para qué propósitos y a quien se puede circular o dar acceso. El consentimiento reconoce que la persona es el titular del dato y, por ende, ella es quien, en principio, tiene control sobre su información y algunos aspectos de su vida relacionados con su información.

Se ha manifestado que el consentimiento no sirve para nada o que es una barrera para el desarrollo de algunas actividades o porque afecta el modelo de negocios de

[17] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 11.1.

[18] Cfr. *Ibidem*.

algunas empresas u organizaciones. Aunque en la práctica el consentimiento tiene un efecto simbólico, no por ello deja de ser muy trascendental en las relaciones humanas. Eliminar el consentimiento sería tanto como permitir que cualquier persona ingrese a nuestra casa sin nuestra autorización, o que el día del matrimonio no se les pregunte a las personas si desean casarse. ¿El hecho de que una empresa u organización actúe de manera profesional, diligente y ética justifica que ella no obtenga nuestra autorización para tratar nuestros datos personales? Si una persona es "perfecta" o por lo menos la esposa o el esposo "ideal", ¿nos debemos casar con ella sin que nos consulten cuál es nuestra voluntad?

Los estándares señalan las condiciones que debe reunir el consentimiento y se refiere especialmente a la autorización de los menores de edad. Respecto del primer aspecto se impone una carga probatoria en cabeza del responsable de demostrar que obtuvo el consentimiento, el cual puede ser una "declaración o acción afirmativa clara". Adicionalmente se establece la facultad de revocar el consentimiento por parte del titular y la obligación de responsable de prever mecanismos gratuitos, sencillos y expeditos para dicho efecto[19].

En cuanto al consentimiento para el tratamiento de los datos de niñas, niños y adolescentes los estándares[20] ordenan que, por regla general, se debe obtener del titular de la patria potestad o tutela. Excepcionalmente se puede adquirir directamente del menor de edad, siempre que lo permita la regulación de cada país. Cuando el consentimiento se recoge utilizando medios tecnológicos, le corresponde al responsable realizar "esfuerzos razonables para verificar que el consentimiento fue otorgado por el titular de la patria potestad o tutela, o bien, por el menor directamente atendiendo a su edad de acuerdo con el derecho interno de cada Estado Iberoamericano, teniendo en cuenta la tecnología disponible" [21].

[19] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 12. "Condiciones para el consentimiento: 12.1. Cuando sea necesario obtener el consentimiento del titular, el responsable demostrará de manera indubitable que el titular otorgó su consentimiento, ya sea a través de una declaración o una acción afirmativa clara. 12.2. Siempre que sea requerido el consentimiento para el tratamiento de los datos personales, el titular podrá revocarlo en cualquier momento, para lo cual el responsable establecerá mecanismos sencillos, ágiles, eficaces y gratuitos".

[20] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 13.

[21] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 13.2.

B) *Principio de licitud*

Este principio (num. 14) exige a los responsables que el tratamiento de los datos personales lo realicen observando lo que ordena la ley[22]. De esta forma se busca que el tratamiento de datos personales no se efectúe de manera caprichosa o arbitraria sino objetiva y respetando el Estado de derecho, como elemento esencial de la democracia.

El principio de ilicitud pone de presente que el tratamiento de datos es una actividad reglada con facultades o atribuciones limitadas o definidas en la ley. Por lo tanto, no puede hacerse de cualquier forma sino como lo indica la ley.

Respecto del caso de las autoridades públicas, se recalca que estas solo pueden recaudar y administrar datos personales dentro del ámbito de sus deberes y competencias establecidos por la ley.

C) *Principio de prevención del daño*

De conformidad con el APEC Privacy Framework de 2004 este principio —*Preventing Harm*— tiene como finalidad evitar afectaciones a los derechos del titular del dato. Según APEC, "la protección de la información personal debe ser diseñada para prevenir el mal uso del tal información"[23]. Para el efecto, se deben tener presente los riesgos que implica el tratamiento y los eventuales perjuicios que por el uso indebido se genere al titular del dato. En consecuencia, se deben implementar medidas pertinentes que sean "proporcionales a la probabilidad y severidad del daño amenazado por la recolección, uso y transferencia de información personal"[24].

Por su claridad y conexión con el principio de responsabilidad demostrada nos parece importante transcribir los siguientes comentarios explicativos de APEC en cuanto al citado principio: "El principio de prevención del daño reconoce que uno de los objetivos fundamentales del Marco de Privacidad de APEC es prevenir el mal uso de la información personal y, por consiguiente, el daño a los individuos.

[22] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 14. "Principio de licitud

"14.1. El responsable tratará los datos personales en su posesión con estricto apego y cumplimiento de lo dispuesto por el derecho interno del Estado Iberoamericano que resulte aplicable, el derecho internacional y los derechos y libertades de las personas.

"14.2. El tratamiento de datos personales que realicen las autoridades públicas se sujetará a las facultades o atribuciones que el derecho interno del Estado Iberoamericano de que se trate les confiera expresamente, además de lo previsto en el numeral anterior de los presentes Estándares".

[23] Cfr. APEC Privacy Framework, num. 14.

[24] Cfr. APEC Privacy Framework, num. 14.

Por lo tanto, las protecciones a la privacidad, que comprende esfuerzos autorreguladores, campañas de educación y conciencia, leyes, regulaciones y mecanismos de seguridad deben ser diseñados para prevenir el daño a los individuos por la recolección ilegal y el mal uso de su información personal. Por consiguiente, deben ser diseñados remedios para violaciones a la privacidad para prevenir daños por la recolección ilegal o el mal uso de la información personal, y deben ser proporcionales a la probabilidad y severidad de cualquier daño amenazado por la recolección o uso de la información personal"[25].

D) *Principio de lealtad*

Lealtad significa tratar los datos sin engaño y de la forma como lo hemos prometido o anunciado, incluso en circunstancias adversas. El principio de lealtad no se cumple, cuando, por ejemplo, traicionamos la confianza que nos ha depositado el titular del dato.

Con el principio de lealtad[26] se proscribe el tratamiento tramposo, deshonesto, pícaro y no ético de la información sobre las personas. Nótese que los derechos del titular del dato dependen principalmente de lo que haga o deje de hacer el responsable. Al titular le es imposible controlar lo que hace el responsable con su información. Por eso, al titular no le queda más remedio que confiar en la buena fe, diligencia y ética del responsable. Así las cosas, no es consistente con este principio defraudar esa confianza y recurrir a mecanismos oscuros, ilegales o poco transparentes para recolectar y tratar los datos.

E) *Principio de finalidad*

Este principio (num. 17) busca que el tratamiento tenga como objetivo la realización de actividades concretas, legítimas y conocidas por el titular del dato[27]. El principio de finalidad busca evitar que se recolecten datos para hacer con ellos

[25] Cfr. APEC Privacy Framework, num. 14.

[26] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 15. "Principio de lealtad

"15.1. El responsable tratará los datos personales en su posesión privilegiando la protección de los intereses del titular y absteniéndose de tratar éstos a través de medios engañosos o fraudulentos.

"15.2. Para los efectos de los presentes Estándares, se considerarán desleales aquellos tratamientos de datos personales que den lugar a una discriminación injusta o arbitraria contra los titulares".

[27] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 17. "Principio de finalidad

17.1. Todo tratamiento de datos personales se limitará al cumplimiento de finalidades determinadas, explícitas y legítimas.

lo que sea y delimita los usos que pueda darle el responsable. No obstante, precisa el principio que el tratamiento "ulterior de datos personales con fines archivísticos, de investigación científica e histórica o con fines estadísticos, todos ellos, en favor del interés público, no se considerará incompatible con las finalidades iniciales"[28].

F) *Principio de proporcionalidad*

En línea con lo anterior, el numeral 18 ordena que el responsable "tratará únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento"[29]. En otras palabras, el tratamiento de datos personales debe circunscribirse a aquellos que resulten adecuados, relevantes y no excesivos en relación con la finalidad del tratamiento. Por lo tanto, no está permitido recolectar o usar datos que no guarden estrecha relación con la finalidad del tratamiento.

G) *Principio de elección*

Este es otro principio —Choice— previsto en el APEC Privacy Framework de 2004 cuya finalidad consiste que en ciertas ocasiones se le faciliten al titular del dato "mecanismos claros, prominentes, de fácil entendimiento, accesibles y asequibles para ejercitar la elección en relación con la recolección, uso y revelación de su información personal" [30]. Un ejemplo de ello es que el titular pueda escoger las finalidades para las cuales otorga su consentimiento y no que deba aceptar todas aquellas que preestablece el responsable del tratamiento.

La nota explicativa de este principio señala que "el propósito general del Principio de Elección es asegurar que los individuos tengan una opción con relación a la recolección, uso, transferencia y revelación de su información personal. Ya sea que la información sea transmitida electrónicamente, por escrito o por otros medios, aviso de tal elección debe ser comunicado y mostrado de manera clara y evidente. Del mismo modo, los mecanismos para llevar a cabo la elección deben ser accesibles y asequibles para los individuos"[31].

"17.2. El responsable no podrá tratar los datos personales en su posesión para finalidades distintas a aquellas que motivaron el tratamiento original de estos, a menos que concurra alguna de las causales que habiliten un nuevo tratamiento de datos conforme al principio de legitimación".

[28] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 17.3.

[29] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 18.

[30] Cfr. APEC Privacy Framework, num. 20.

[31] Cfr. *Ibidem*.

Recalcamos que este principio es de aplicación en situaciones concretas y que no opera en todos los casos. APEC, por ejemplo, cita estas situaciones en las que considera que no es procedente:

"Cuando información de contacto u otro tipo de información que identifique a un individuo en su capacidad profesional esté siendo intercambiada en un contexto empresarial, generalmente no es práctico ni necesario proporcionar un mecanismo para ejercitar la elección, porque en estas circunstancias los individuos esperarían que su información fuera usada de esta manera.

"Además, en ciertas situaciones no será práctico que a los patrones se les requiera proporcionar un mecanismo para ejercitar la elección relacionada a la información personal de sus empleados cuando usen esa información con propósitos de trabajo, Por ejemplo, si una organización ha decidido centralizar la información de recursos humanos, no se le requerirá proporcionar un mecanismo para ejercitar la elección a sus empleados antes de dedicarse a tal actividad"[32].

H) *Principio de transparencia*

Ser transparente significa, entre otras cosas, dar a conocer información relevante a los titulares de los datos y a la ciudadanía en general. En ese sentido el numeral 16 de los estándares precisa que el responsable "informará al titular sobre la existencia misma y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto". Este principio implica varias cosas:

Primero, que el responsable cuente con políticas para el tratamiento de datos personales. Segundo, que la información que se suministre al titular sea clara, completa, veraz y fácilmente entendible por culquier persona para que el titular del dato tenga suficiente conocimiento de los principales aspectos que regirán el tratamiento de su información. Finalmente, según establece el numeral 16.2, que el responsable informe al titular, como mínimo, lo siguiente:

"a. Su identidad y datos de contacto.

"b. Las finalidades del tratamiento a que serán sometidos sus datos personales.

"c. Las comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y las finalidades que motivan la realización de las mismas.

"d. La existencia, forma y mecanismos o procedimientos a través de los cuales podrá ejercer los derechos de acceso, rectificación, cancelación, oposición y portabilidad.

[32] Cfr. *Ibidem*.

”e. En su caso, el origen de los datos personales cuando el responsable no los hubiere obtenido directamente del titular”.

I) *Principio de calidad*

El numeral 19 demanda que los datos personales sean veraces, exactos, completos, correctos y actualizados. Le corresponde al responsable adoptar medidas para que ello sea así. En suma, la información de calidad[33] es una condición para el debido tratamiento de los datos y de ella dependen algunos derechos de las personas como su buen nombre o que las decisiones que se adopten con fundamento en los datos personales sean correctas, pertinentes o apropiadas. No debe perderse de vista que la información es, por excelencia, una herramienta para tomar decisiones. Si no se logra mantener sistemas de información de calidad, las organizaciones deben reflexionar si en su posesión tienen “bases de datos o basureros de datos”.

La redacción del principio da un espacio importante a la vigencia del dato de manera que se deje de tratar información que ya no es necesaria para cumplir las finalidades del tratamiento. La supresión de los datos debe ser definitiva y no se deben guardar copias de la misma. En suma, los datos personales no se deben tratar indefinidamente sino solo por el período de tiempo necesario para cumplir la finalidad para la cual fueron recolectados.

J) *Principio de responsabilidad*

Con este principio[34] se quiere que los mandamientos constitucionales y legales sobre tratamiento de datos personales sean una realidad verificable y redunden

[33] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 19. “Principio de calidad.

”19.1. El responsable adoptará las medidas necesarias para mantener exactos, completos y actualizados los datos personales en su posesión, de tal manera que no se altere la veracidad de estos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento.

”19.2. Cuando los datos personales hubieren dejado de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, el responsable los suprimirá o eliminará de sus archivos, registros, bases de datos, expedientes o sistemas de información, o en su caso, los someterá a un procedimiento de anonimización.

”19.3. En la supresión de los datos personales, el responsable implementará métodos y técnicas orientados a la eliminación definitiva y segura de éstos.

”19.4. Los datos personales únicamente serán conservados durante el plazo necesario para el cumplimiento de las finalidades que justifiquen su tratamiento o aquéllas relacionadas con exigencias legales aplicables al responsable. No obstante, la legislación nacional de los Estados Iberoamericanos aplicable en la materia podrá establecer excepciones respecto al plazo de conservación de los datos personales, con pleno respeto a los derechos y garantías del titular”.

[34] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 20.

en beneficio de la protección de los derechos de las personas. El principio de responsabilidad será objeto de análisis posteriormente pero es preciso dejar claro que busca que las normas sobre tratamiento de datos se materialicen en la práctica y no como a veces sucede, se conviertan en "letra muerta".

El *principio de responsabilidad* demanda menos retórica y más acción en el cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. El éxito dependerá del compromiso real de los directivos de los sujetos obligados ya que sin su apoyo franco y decidido todo esfuerzo será insuficiente para *diseñar, implementar, revisar, actualizar y evaluar los programas de gestión de datos*. Es necesario destinar recursos —*económicos y humanos*—para esta labor y poner a trabajar armónicamente varias dependencias de la organización ya que esto *no es sólo un tema jurídico* sino ante todo una cuestión de *gestión gerencial y estratégica de gobierno corporativo*.

Este principio exige implantar acciones concretas para garantizar el debido tratamiento de los datos personales. El éxito de esta tarea dependerá del compromiso de las directivas de la organización, ya que sin su apoyo decidido todo esfuerzo será insuficiente para diseñar, implantar, revisar, actualizar y evaluar el *programa de gestión de datos*. Es necesario destinar recursos —económicos y humanos— para esta labor y disponer que varias dependencias de la organización trabajen armónicamente porque esto no es solo un asunto jurídico sino, ante todo, cuestión de gestión gerencial y estratégica de buen gobierno corporativo.

K) *Principio de seguridad*

Sin seguridad[35] no habrá privacidad ni debido tratamiento de los datos personales. Es de cardinal importancia adoptar medidas tecnológicas, humanas, administrativas, físicas, contractuales y de cualquier otra índole que cumplan los siguientes objetivos:

- Evitar accesos indebidos o no autorizados a la información.
- Impedir manipulación de la información.
- No permitir destrucción de la información.
- Evadir usos indebidos o no autorización de la información.
- Evitar que se suministre la información a personas no autorizadas.

[35] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 21. "Principio de seguridad

"21.1. El responsable establecerá y mantendrá, con independencia del tipo de tratamiento que efectúe, medidas de carácter administrativo, físico y técnico suficientes para garantizar la confidencialidad, integridad y disponibilidad de los datos personales".

Las medidas de seguridad deben ser apropiadas[36] y deben tenerse en cuenta varios factores como los siguientes: (i) los niveles de riesgo del tratamiento; (ii) la naturaleza de los datos; (iii) la magnitud del daño que se puede causar a los titulares y al responsable; (iv) la cantidad de información; (v) el tamaño de la organización, y (vi) los recursos disponibles.

Dichas medidas debe ser objeto de revisión, evaluación y mejoras permanentes[37].

En caso de presentarse vulneraciones de seguridad de los datos se debe notificar a la autoridad de protección de datos y al titular de dicha información[38]. Sobre este

[36] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 21.2. "Para la determinación de las medidas referidas en el numeral anterior, el responsable considerará los siguientes factores:

"a. El riesgo para los derechos y libertades de los titulares, en particular, por el valor potencial cuantitativo y cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

"b. El estado de la técnica.

"c. Los costos de aplicación.

"d. La naturaleza de los datos personales tratados, en especial si se trata de datos personales sensibles.

"e. El alcance, contexto y las finalidades del tratamiento.

"f. Las transferencias internacionales de datos personales que se realicen o pretendan realizar.

"g. El número de titulares.

"h. Las posibles consecuencias que se derivarían de una vulneración para los titulares.

"i. Las vulneraciones previas ocurridas en el tratamiento de datos personales".

[37] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 21.3. "El responsable llevará a cabo una serie de acciones que garanticen el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de las medidas de seguridad aplicables al tratamiento de los datos personales, de manera periódica".

[38] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 22. "Notificación de vulneraciones a la seguridad de los datos personales.

"22.1. Cuando el responsable tenga conocimiento de una vulneración de seguridad de datos personales ocurrida en cualquier fase del tratamiento, entendida como cualquier daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales aun cuando ocurra de manera accidental, notificará a la autoridad de control y a los titulares afectados dicho acontecimiento, sin dilación alguna.

"22.2. Lo anterior, no resultará aplicable cuando el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de la vulneración de seguridad ocurrida, o bien, que ésta no represente un riesgo para los derechos y las libertades de los titulares involucrados.

"22.3. La notificación que realice el responsable a los titulares afectados estará redactada en un lenguaje claro y sencillo".

aspecto, los estándares detallan qué debe contener la notificación[39] y establecen la necesidad de documentar[40] lo sucedido frente a cada incidente, con las medidas correctivas adoptadas para responder a los mismos.

L) *Principio de confidencialidad*

Este principio buscar que quienes con ocasión de su trabajo o función en una organización tienen acceso a información privada, semiprivada o sensible se abstengan de comunicarla a terceros. En este sentido el numeral 23.1 dice lo siguiente: "El responsable establecerá controles o mecanismos para que quienes intervengan en cualquier fase del tratamiento de los datos personales mantengan y respeten la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el titular".

Nótese que se impone al responsable implantar mecanismos para lograr el objetivo necesario, lo cual es una manifestación concreta de lo que implica el principio de responsabilidad en esta materia.

Estos principios que deben observar los responsables y los encargados van acompañados de un conjunto de derechos de los titulares de los datos que serán objeto de estudio a continuación:

3. De los derechos Arco en el contexto internacional

La protección de datos personales no sería completa si solo se centra en exigir a los responsables el cumplimiento de varias obligaciones. Por eso, de la mano con lo anterior se ha dotado al titular de un conjunto de derechos que le permitan

[39] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 22.4. "La notificación a que se refieren los numerales anteriores contendrá, al menos, la siguiente información:

"a. La naturaleza del incidente.

"b. Los datos personales comprometidos.

"c. Las acciones correctivas realizadas de forma inmediata.

"d. Las recomendaciones al titular sobre las medidas que éste pueda adoptar para proteger sus intereses.

"e. Los medios disponibles al titular para obtener mayor información al respecto".

[40] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 22.5. "El responsable documentará toda vulneración de seguridad de los datos personales ocurrida en cualquier fase del tratamiento, identificando, de manera enunciativa mas no limitativa, la fecha en que ocurrió; el motivo de la vulneración; los hechos relacionados con ella y sus efectos y las medidas correctivas implementadas de forma inmediata y definitiva, la cual estará a disposición de la autoridad de control".

ser guardián de sus datos, mediante una serie de facultades orientadas a conocer y rectificar su información así como cancelar y oponerse al tratamiento de sus datos en determinadas circunstancias.

Los derechos ARCO[41] son un plexo de valiosos instrumentos de que dispone el titular del dato que lo convierten en un sujeto activo de su información personal. Estos le permiten controlar la cantidad, calidad y uso de sus datos personales.

Debe mencionarse que desde la perpectiva del *habeas data*, elemento de la protección de datos personales, existen pronunciamientos de importantes organismos en el contexto americano que se refieren a elementos cardinales de los derechos ARCO. En este sentido, la Comisión Interamericana de Derechos Humanos[42] (CIDH) ha reconocido que la acción de *habeas data*[43] se edifica sobre las siguientes tres premisas: "1) el derecho de cada persona a no ser perturbado en su privacidad, 2) el derecho de toda persona a *acceder* a información sobre sí misma en bases de datos públicos y privados para modificar, anular o *rectificar* información sobre su persona por tratarse de datos sensibles, falsos, tendenciosos o discriminatorios y 3) el derecho de las personas a utilizar la acción de habeas data como mecanismo de fiscalización"[44] (Subrayas fuera del original).

Si bien existen diferencias entre unos y otros documentos internacionales, dado que tienen ámbitos de aplicación diferentes y distintos grados de obligatoriedad, estos coinciden en señalar una serie derechos del titular del dato frente al tratamiento de su información que deben ser respetados por los responsables, por los encargados o por terceros. En la tabla que sigue se aprecia cómo en los diferentes documentos se incorporan explícitamente, total o parcialmente, los derechos que forman parte de lo que se conoce como derechos ARCO:

[41] Sobre los derechos ARCO consúltese el texto de Nelson Remolina Angarita, "Los derechos de acceso, rectificación, cancelación y oposición en la ley de datos personales y su reglamento", en *La protección de datos personales en México*, México, Tirant Lo Blanch, 2013, págs. 181-205.

[42] La Comisión Interamericana de Derechos Humanos (CIDH) es un órgano principal y autónomo de la Organización de los Estados Americanos (OEA), cuyo mandato surge de la Carta de la OEA y de la Convención Americana sobre Derechos Humanos, y que actúa en representación de todos los países miembros de la OEA. Su función principal consiste en promover la observancia y la defensa de los derechos humanos. Cfr. *http://www.cidh.oas.org/que.htm*

[43] Este reconocimiento se realizó a partir del principio 3º de la Declaración de Principios sobre Libertad de Expresión, según el cual "toda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o enmendarla".

[44] Relatoría para la Libertad de Expresión. Informe Anual CIDH, 2000, vol. 3, pág. 1, párrafos 12-15, citada por la Corte Constitucional en la sent. C-1011 de 2008.

PRINCIPIO	RIPD 2017	UE 2016	OEA 2015	OCDE 2013	CIAPDP 2009	APEC 2004	ONU 1990
Acceso	✓	✓	✓	✓	✓	✓	✓
Rectificación	✓	✓	✓	✓	✓	✓	✓
Cancelación	✓	✓	✓	X	✓	X	X
Oposición	✓	✓	✓	X	✓	X	X

Tabla núm. 3. Incorporación explícita de los derechos ARCO en los principales documentos internacionales

Como se puede observar, los derechos de acceso y rectificación no solo son comunes a todos los documentos internacionales sino que históricamente son las primeras facultades que se han otorgado a los titulares de los datos personales. Podría decirse que el acceso y la rectificación forman parte de la primera generación de derechos.

Lo que no sucede con las facultades de cancelación y de oposición, pues respecto de los primeros, forman parte de una segunda generación de medios de control en manos de los titulares. Sobre los dos primeros es claro a qué se refiere, pero sobre los últimos no sucede lo mismo o al menos no existe uniformidad respecto de los casos en que proceden y la forma en que operan[45]. Lo anterior, desde luego debe considerarse a la luz de cada regulación nacional pues el legislador local es quien define no solo las circunstancias sino los casos en que no es viable la aplicación de los citados derechos. De hecho, existen regulaciones recientes en las que no se consagran estos derechos, con lo cual se deja a los ciudadanos en un escenario insuficiente en el marco de la dinámica y necesidades del tratamiento de datos personales en el siglo XXI.

Otro punto digno de destacar, consiste en que el ejercicio de esos derechos depende del tipo de sujeto obligado. Las obligaciones consagradas para un sujeto de derecho público no son las mismas de las establecidas que para uno de derecho privado, pues en el primer caso se analizarán las características de las facultades o competencias que legal y constitucionalmente le son otorgadas, mientras que en el segundo dependerá de las relaciones privadas que se hayan desarrollado: por supuesto, en ambos casos se tendrá que privilegiar el ejercicio y protección de los derechos humanos.

Visto lo anterior, a continuación destacaremos los principales aspectos de la regulación sobre tratamiento de datos personales en algunos países.

[45] Cuando nos refiramos a los derechos de cancelación y oposición, retomaremos algunos aspectos del contexto internacional con el propósito de determinar los casos en que proceden.

4. Regulación del tratamiento de datos personales en algunos países latinoamericanos y en España

La protección de datos personales es asunto de importante relevancia constitucional en el escenario latinoamericano. Lo anterior se corrobora en el reporte realizado por Nelson Remolina Angarita[46] titulado *Latin America and Protection of Personal Data: Facts and Figures* (*1985-2014*), en el cual se pone de presente el estado del arte de la regulación sobre datos personales en veinte países de América Latina: Argentina, Bolivia, Brasil, Chile[47], Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Haití, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay y Venezuela.

Respecto de lo que dicen los textos de las Constituciones de dichos países se concluyó lo siguiente:

• El 70 por ciento de los países latinoamericanos incorporan en su Constitución disposiciones explícitas referentes a aspectos relacionados con la protección de datos personales

• El ciento por ciento de las disposiciones constitucionales consagran el derecho de acceso de la persona para conocer sus datos y el 92,85 por ciento menciona explícitamente el dato personal o la información personal.

• El 85,71 por ciento establece el derecho del titular del dato a solicitar rectificación o corrección de la información errónea, mientras que el 64,28 por ciento le confiere el derecho constitucional de solicitar la supresión, eliminación, destrucción o cancelación del dato.

• El 64,28 por ciento considera la actualización de la información como un derecho del titular del dato personal.

• El 57,14 por ciento establece el "habeas data" y el 7,14 por ciento la "acción de amparo" y "acción de protección de privacidad".

[46] Cfr. Nelson Remolina, *Latin America and Protection of Personal Data: Facts and Figures* (1985-2014) (March 20, 2014), available at SSRN: *https://ssrn.com/abstract=241209* or *http://dx.doi.org/10.2139/ssrn.241209*. El texto fue publicado inicialmente en el "Observatorio Ciro Angarita Barón sobre la protección de datos personales en Colombia", fundado el 17 de enero de 2008 en la Facultad de Derecho de la Universidad de los Andes. El observatorio representa un espacio académico de reflexión sobre la protección de los derechos de las personas cuando sus datos son recolectados, almacenados o utilizados por terceros. La página web del Observatorio es: *https://habeasdatacolombia.uniandes.edu.co*

[47] En mayo de 2018, el Senado de Chile aprobó un proyecto de reforma constitucional mediante el cual se garantiza la protección de los datos personales y se ordena que el tratamiento y la protección de esa información se efectuarán como lo indique la ley . (Cfr. Senado de Chile. Departamento de Prensa. Boletín núm. 9384-07: Protección a los datos personales como derecho constitucional será una realidad. Disponible en http*://www.senado.cl/proteccion-a-los-datos-personales-como-derecho-constitucional-sera-una/prontus_senado/2018-05-15/181511.html#vtxt_cuerpo_T0*.)

• El 50 por ciento prevé el derecho a conocer la finalidad del tratamiento de los datos y el 21,42 por ciento a saber el uso que se le está dando a los datos.

• El 28,57% erige como derecho constitucional el exigir la confidencialidad sobre los datos personales.

• El 14,28 por ciento de las constituciones analizadas otorgan expresamente protección constitucional a los datos personales

• Panamá (2004), Ecuador (2008), México (2009) y Chile (2018) consagran explícitamente el derecho a la "protección" de la "información personal" y a la "protección de los datos personales".

• República Dominicana (2010) es el único país que contiene un plexo de principios constitucionales (calidad, licitud, lealtad, seguridad y finalidad) que deben regir el tratamiento de datos personales

• Las Constituciones de Panamá y Ecuador exigen que los datos personales se recolecten previo el consentimiento del titular del dato.

En cuanto a las leyes se concluyó que el ciento por ciento de los países tienen normas sectoriales —sobre historias clínicas y censos de población— y el 50 por ciento cuenta con normas generales.

Visto lo anterior, mencionaremos los resultados de un ejercicio de derecho comparado realizado sobre la regulación general o especial en materia de tratamiento de datos personales en varios países latinoamericanos —Argentina, Costa Rica, México, Perú, Uruguay— y España. Este país lo mencionamos porque la normativa española ha sido un referente en la regulación colombiana y porque la labor de la Agencia Española de Protección de Datos ha sido reconocida por su liderazgo e incidencia en Latinoamérica.

Es necesario advertir que no realizaremos un estudio completo, detallado y profundo sobre la regulación de tratamiento de datos personales en Argentina, Costa Rica, España, México, Perú y Uruguay y España, sino que nos centraremos en ciertos temas puntuales que guardan relación con el propósito de esta obra.

Precisado lo anterior, respecto a cada país, se realizará el siguiente ejercicio:

En primer lugar, establecer la existencia de disposiciones constitucionales sobre el tratamiento de datos personales, con el propósito de resumir las líneas básicas de los mandatos constitucionales.

En segundo lugar, verificar si existe una norma general sobre tratamiento de datos personales. De ser así, referirnos a los siguientes aspectos: (i) el ámbito de aplicación y eventuales exclusiones; (ii) los principios de tratamiento de datos personales; (iii) los deberes del responsable del tratamiento, y (iv) la existencia del principio de responsabilidad demostrada.

Posteriormente, establecimos si existe una norma especial para el tratamiento de datos en el sector público o en el sector privado. De existir norma especial, indagamos sobre las cuatro cuestiones señaladas en el párrafo anterior. Adicio-

nalmente, procedimos a determinar si el país cuenta con regulación sobre acceso a la información y transparencia. De igual manera, de ser positiva la respuesta, indagamos por las cuatro cuestiones señaladas anteriormente.

Luego, investigamos si existe regulación especial de TDP para entidades como la RNEC, es decir que cumplan funciones registrales y electorales. Adicionalmente, verificamos si el país tiene regulación especial sobre TDP para funciones registrales o electorales. En caso positivo, destacamos los principales aspectos de esas regulaciones.

De otra parte, corroboramos si la Autoridad de Protección de Datos Personales (ATDP) ha emitido instrucciones sobre TDP en el sector público, o para el cumplimiento de la función registral o electoral. Finalmente, establecimos si existe una guía o instrucciones sobre el principio de responsabilidad demostrada. En caso positivo, referenciamos sus principales lineamientos.

El resultado del ejercicio anterior lo sintetizamos en la siguiente tabla:

	Argentina	Costa Rica	Colombia	España	México	Perú	Uruguay
Norma constitucional sobre TDP	✓	X	✓	✓	✓	✓	X
Norma general sobre TDP aplicable al sector público y privado	✓	✓	✓	✓	X	✓	✓
Norma sobre TDP solo aplicable al sector público	X	X	X	X	✓	X	X
Norma sobre TDP únicamente aplicable al sector privado	X	X	X	X	✓	X	X
Norma sobre AIT	✓	X	✓	✓	✓	✓	✓
Norma especial sobre TDP para entidades como la RNEC	X	X	X	X	X	X	X
Norma especial sobre TDP para funciones registrales	X	X	X	✓	X	X	X
Norma especial sobre TDP para funciones electorales	✓	✓	X	✓	✓	✓	X
Existe ATDP	✓	✓	✓	✓	✓	✓	✓
La ATDP ha emitido instrucciones sobre el TDP en el sector público	✓	X	X	X	X	✓	X
La ATDP ha emitido instrucciones sobre el TDP para la función registral	X	X	X	X	X	X	X
La ATDP ha emitido instrucciones sobre el TDP para la función electoral	X	X	X	X	X	X	X
La ATDP ha emitido instrucciones sobre el principio de responsabilidad	X	X	✓	✓	X	X	X

Tabla núm. 4. Comparación de ciertos aspectos sobre la regulación de tratamiento de datos personales en Argentina, Costa Rica, Colombia, España, México, Perú y Uruguay.

TDP: tratamiento de datos personales.
AIT: acceso a la información o transparencia
ATDP: autoridad de tratamiento de datos personales

A continuación mencionaremos los principales hallazgos existentes sobre la regulación de cada país.

A) *República Argentina*

En Argentina, la protección de datos personales se encuentra consagrada en el artículo 43 de la Constitución Nacional, como uno de los supuestos en los cuales procede interponer acción expedita y rápida de amparo. Dicho artículo, en lo pertinente, establece lo siguiente:

"[...] Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística"[48].

Del citado texto constitucional se deriva que todas las entidades públicas deben garantizar acceso a la información, confidencialidad y rectificación y supresión de los datos personales.

La reglamentación de la protección integral de datos personales se encuentra en la ley 25.326 sancionada el 4 de octubre de 2000. Cabe resaltar que, como sucede en Colombia, la ley no hace distinción entre protección de datos personales respecto de entidades privadas y entidades públicas[49]. Nótese que en Argentina no existe una norma especial para tratar los datos personales en el sector público debido a que todo se encuentra regulado en citada ley, aplicable tanto a entidades públicas como privadas.

El artículo 44 de la ley ordena que lo contenido en los capítulos I, II, III y IV al igual que el artículo 32 son normas de orden público y, como tal, deben ser aplicadas en todo el territorio nacional. Establece además que la jurisdicción federal va a regir respecto de los registros, archivos, bases o bancos de datos interconectados en redes interjurisdiccionales[50]. No menciona nada sobre exceptuar entidades públicas en la aplicación de la ley.

[48] Cfr. República Argentina, Constitución Nacional, art. 43. El texto puede consultarse en: *http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm*

[49] En el art. 2º de la ley 25.326 se establece como responsable de archivo, registro, base o banco de datos a cualquier persona física o de existencia ideal, sea pública o privada, que es titular de un archivo, registro, base o banco de datos.

[50] República Argentina, ley 25.326 de 4 octubre 2000, de Protección de Datos Personales, art. 44.

Existen supuestos especiales cuando se está ante el tratamiento de datos personales con fines de defensa nacional o seguridad pública por las fuerzas armadas, fuerzas de seguridad u organismos policiales o de inteligencia[51].

La ley 25.326 en su capítulo II establece los principios generales en materia de protección y tratamiento de datos personales. En primer lugar está el principio de licitud[52] para la formación de archivos de datos. En segundo lugar, se encuentra la calidad de datos[53], entendido como el que la recolección de datos no puede hacerse por medios desleales y que dichos datos deben ser ciertos y exactos, y su almacenamiento debe permitir el derecho de acceso a su titular. En tercer lugar se tiene el consentimiento, entendido como el que el titular debe dar un consentimiento libre[54], expreso e informado sobre el tratamiento de sus datos. Se consagra como cuarto principio el de la información[55] en el sentido de que se debe informar a los titulares para qué serán tratados los datos y quiénes serán sus destinatarios.

Dentro de los deberes del responsable del tratamiento de datos personales se destacan los de confidencialidad y de garantizar la seguridad de la información contenida en las bases de datos.

El acceso a la información pública se encuentra consagrado en la ley 27.275. Esta ley es aplicable a la administración pública nacional, es decir, a todos los órganos de la administración central al igual que los organismos descentralizados; por lo que indudablemente involucra a las entidades responsables de ejercer las funciones registrales y electorales[56]. No hay principios específicos consagrados para esta ley, pero se deduce que es un desarrollo del principio de acceso a la

[51] "1. Quedarán sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales. 2. El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquellos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad. 3. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento". Constitución Nacional, art. 23.

[52] República Argentina, ley 25.326, art. 3º.

[53] República Argentina, ley 25.326, art. 4º.

[54] República Argentina, ley 25.326, art. 5º.

[55] República Argentina, ley 25.326, art. 6º.

[56] República Argentina, ley 27275, art. 7º.

información, gratuidad y publicidad. El único deber que se encuentra en la ley es el del suministro de información cuidando la confidencialidad y la licitud del tratamiento de los datos personales que integran la base de datos.

Para la función registral, Argentina tiene un Registro Nacional de las Personas (RENAPER) el cual es un organismo autárquico y descentralizado que es dependiente del Ministerio del Interior, Obras Públicas y Vivienda, por conducto de la Secretaría del Interior[57]. Por otra parte, la función electoral está a cargo de la Cámara Nacional Electoral, que cuenta con facultades registrales, reglamentarias, operativas y de fiscalización del Registro Nacional de Electores[58].

No existe una regulación específica para entidades con funciones registrales y electorales debido a que estas se someten a la ley general de protección de datos personales y a la de acceso a la información pública.

De la autoridad de protección de datos personales, el tratamiento de datos en el sector público y el principio de responsabilidad demostrada. La Agencia de Acceso a la Información Pública es la encargada de supervisar que se cumplan las disposiciones contenidas en la Ley de Protección de Datos, en la Ley de Acceso a la Información, y en la Ley del Registro No Llame.

Dentro de las instrucciones que ha emitido dicha agencia para el tratamiento de datos del sector público vale la pena resaltar el Formulario FM-P mediante la cual se modifica la inscripción de tratamientos de datos personales de entes públicos estatales y no estatales.

Respecto de la función registral y electoral, en materia de protección de datos personales no hay mayor desarrollo por parte de la autoridad.

En cuanto al principio de responsabilidad demostrada, la Agencia creó una guía de buenas prácticas en políticas de privacidad para el ámbito público con claras instrucciones sobre el principio de responsabilidad demostrada[59]. Su ámbito de aplicación comprende a todas las entidades públicas. Adicionalmente, se basa en los siguientes principios: calidad, no automaticidad, datos sensibles, consentimiento y publicidad. Los deberes que tiene el responsable de la base de datos son los de inscripción, seguridad, secreto y respuesta conforme a lo establecido en la guía.

[57] Ministerio del Interior, Obras Públicas y Vivienda, Presidencia de la Nación. "Registro Nacional de las Personas" Web. 15 Feb 2018. <*http://www.mininterior.gov.ar/renaper/renaper.php*>

[58] Cámara Nacional Electoral "Competencia de la Cámara Nacional Electoral" Web. 15 Feb 2018. <*https://www.electoral.gov.ar/cne_competencia.php#competencia*>

[59] Dirección Nacional de Protección de Datos Personales. Guía de Buenas Prácticas en Políticas de Privacidad para las Bases de Datos del Ámbito Público. BS, As, 22/8/2008. Puede consultarse en: <*http://www.informaticalegal.com.ar/2008/08/22/disposicion-no-72008-direccion-nacional-de-proteccion-de-datos-personales-guia-de-buenas-practicas-en-politicas-de-privacidad-para-las-bases-de-datos-del-ambito-publico/*>

Adicionalmente, desde el año 2016 se han presentado propuestas sobre la necesidad de reformar la ley argentina vigente. En la versión pública más reciente del anteproyecto de ley publicada en la página web de la Agencia de Acceso a la Información Pública[60] se incorpora el principio de responsabilidad demostrada con el nombre de responsabilidad proactiva. El artículo 10 de dicho documento dice lo siguiente: "Principio de responsabilidad proactiva. El responsable o encargado del tratamiento debe adoptar las medidas técnicas y organizativas apropiadas a fin de garantizar un tratamiento adecuado de los datos personales y el cumplimiento de las obligaciones dispuestas por la presente ley, y que le permitan demostrar a la autoridad de control su efectiva implementación."

Posteriormente, en el artículo 37 del anteproyecto se sugieren las siguientes medidas de cumplimiento de la responsabilidad proactiva, la cuales "deben ser proporcionales a las modalidades y finalidades del tratamiento de datos, su contexto, el tipo y categoría de datos tratados, y el riesgo que el referido tratamiento pueda acarrear sobre los derechos de su titular": .

"a) la adopción de procesos internos para llevar adelante de manera efectiva las medidas de responsabilidad;

"b) la implementación de procedimientos para atender el ejercicio de los derechos por parte de los titulares de los datos;

c) la realización de supervisiones o auditorías, internas o externas, para controlar el cumplimiento de las medidas adoptadas"[61].

Recalca el anteproyecto que las "medidas deben ser aplicadas de modo que permitan su demostración ante el requerimiento de la autoridad de control" [62].

B) *República de Costa Rica*

La protección de los datos personales se puede inferir desde el artículo 24 de la Constitución Política de Costa Rica que, si bien no se refiere expresamente a dicho derecho, hace alguna alusión al derecho a la intimidad con el cual guarda cierta conexidad.

"Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones.

[60] Cfr. *https://www.argentina.gob.ar/normativa/anteproyecto-de-ley-de-proteccion-de-los-datos-personales* (última consulta: 29 de mayo de 2018).

[61] Cfr. República de Argentina. Antroproyecto de ley de protección de datos personales -*Versión elaborada luego de analizar los aportes y comentarios recibidos, durante la consulta pública de febrero de 2017, sobre el anteproyecto de Ley de Protección de los Datos Personales*- . Publicada en: *https://www.argentina.gob.ar/sites/default/files/anteproyecto_reforma_ley_proteccion_de_los_datos_personales_nueva_version.pdf* (última consulta: mayo 29 de 2018).

[62] *Ibidem*.

”Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier tipo de los habitantes de la República. [...] .

”No producirán efectos legales, la correspondencia que fuere sustraída ni la información obtenida como resultado de la intervención ilegal de cualquier comunicación”[63].

La reglamentación de la protección integral de datos personales se encuentra en la ley 8968 de 7 de julio de 2011[64], reglamentada por el decreto ejecutivo 40008-JP. Como en el caso de Colombia, la ley no hace distinción entre protección de datos personales a entidades privadas y entidades públicas[65]. Por otra parte, en lugar de consagrar la “acción de *habeas data*”, la denuncia es el mecanismo idóneo mediante el cual se ponen en conocimiento de la autoridad competente las infracciones a reglas o principios básicos en materia de protección de datos[66].

La ley 8969 de 7 de julio de 2011 se aplica a todos los datos personales que figuren en las bases de datos, automatizadas o manuales, de todos los organismos públicos y privados[67]. Quedan excluidas las bases de datos que tengan personas naturales o jurídicas para su uso interno, personal o doméstico, y que no sean vendidas o comercializadas de ninguna forma[68]. En Costa Rica la ley que regula el tratamiento de datos es la ley 8968 de 2011, y no existe norma especial sobre tratamiento de esa información para el sector público.

La ley no consagra el principio de *Accountability* o responsabilidad demostrada, pero establece otro como el de autodeterminación informativa[69], el cual es además un derecho fundamental que abarca un conjunto de garantías relativas al tratamiento legítimo de datos personales. Adicionalmente, se encuentra el principio de consentimiento informado[70], el cual implica la obligación de informar a los titulares de la existencia de sus datos en una base de datos y que el titular otorgue su consentimiento. En tercer lugar, se encuentra el principio de calidad

[63] República de Costa Rica, Constitución Política. Web 28 Feb. <*http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_norma.aspx?param1=NRM&nValor1=1&nValor2=871&nValor3=95479&strTipM=FN*>

[64] Publicada en la Gaceta 170 de 5 septiembre 2011.

[65] “Esta ley será de aplicación a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos” (ley 8968, art. 2º).

[66] República de Costa Rica, ley 8968 de 7 julio 2011, de Protección de la Persona frente al Tratamiento de sus Datos Personales, art. 25.

[67] República de Costa Rica, ley 8968, art. 2º inc. 1º.

[68] República de Costa Rica, ley 8968, art. 2º inc. 2º.

[69] República de Costa Rica, ley 8968, art. 4º.

[70] República de Costa Rica, ley 8968, art. 5º.

de la información[71], que va dirigido a que todos los datos estén actualizados y sean veraces y exactos.

Son deberes del responsable del tratamiento de datos adoptar medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y así poder evitar que personas no autorizadas tengan acceso a esas bases de datos[72]. Adicionalmente, el responsable de la base de datos debe velar porque los datos proveídos no sean alterados ni se destruyan accidental o ilícitamente. Asimismo, tiene el deber de confidencialidad encaminado a garantizar el cumplimiento del secreto profesional[73].

Respecto de las reglas sobre acceso a la información pública o transparencia, la Constitución Política de Costa Rica estipula que las personas deben tener libre acceso a la información sobre asuntos que sean de interés público, pero dicho país no cuenta con una ley que consagre el derecho al acceso a la información. No obstante, existe un compromiso para establecer bases técnicas con lineamientos mínimos para el acceso a la información y la transparencia que, a la fecha, no se ha traducido en ley sobre la materia[74].

El Tribunal Supremo de Elecciones (TSE) es el órgano encargado de cumplir con las funciones electorales y registrales en Costa Rica, pero no hay regulación específica para esta entidad en materia de tratamiento de datos personales, en cumplimiento de su función registral y electoral.

La autoridad de protección de datos personales, el tratamiento de datos en el sector público y el principio de responsabilidad demostrada. La ley 8968 de 7 de julio de 2011 creó un órgano de desconcentración adscrito al Ministerio de Justicia y Paz denominado Agencia de Protección de Datos de los Habitantes (en adelante "Prodhab"). Su objetivo es garantizar que a todas las personas se les respete su derecho a la autodeterminación informativa respecto de su persona o bienes[75]. Además, la Prodhab orienta al ciudadano y a las entidades públicas y privadas en el cumplimiento de los derechos y deberes en materia de protección de datos[76]. Asimismo, la Prodhab debe llevar un registro de las bases de datos reguladas por la ley 8968. Finalmente, cabe resaltar que la agencia tiene un Director Nacional, que

[71] República de Costa Rica, ley 8968, art. 6º.

[72] República de Costa Rica, ley 8968, art. 10.

[73] República de Costa Rica, ley 8968, art. 11.

[74] Gobierno Abierto. "Eje de transparencia y acceso a la información". Web. 27 Feb 2018. <*http://gobiernoabierto.go.cr/eje-de-transparencia-y-acceso-a-la-informacion/*>

[75] Agencia de Protección de Datos de los Habitantes Prodhab. "¿Quiénes Somos? Web. 10 Feb 2018. <*http://prodhab.go.cr/quienesomos/*>

[76] República de Costa Rica, ley 8968, art. 16 lit. b.

debe contar con un grado académico de licenciatura en una materia relacionada con el objeto de su función y debe reconocerse su "solvencia profesional y moral"[77].

La Prodhab no ha emitido instrucciones para el tratamiento de datos específicamente en el sector público, ni ha expedido lineamientos para que el TSE cumpla su función registral y electoral.

El principio de responsabilidad no está consagrado en la ley que regula los datos personales. De igual manera, la Prodhab aún no ha expedido una guía sobre este principio.

C) *Reino de España*

Antes de referirnos a España, es importante tener presente que en Europa la protección de datos es un derecho constitucional autónomo e independiente de otros derechos (como la privacidad). En efecto, la Carta de los Derechos Fundamentales de la Unión Europea del año 2000[78] expresa lo siguiente:

"*Artículo 8º.—Protección de datos de carácter personal*

"1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

"2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación.

"3. El respeto de estas normas estará sujeto al control de una autoridad independiente."

Esta carta tiene el mismo valor jurídico que los tratados internacionales tal y como lo establece el artículo 6.1 del Tratado de la Unión Europea, modificado por el Tratado de Lisboa del 13 de diciembre de 2007[79].

[77] República de Costa Rica, ley 8968, art. 17.

[78] Publicada en el *Diario Oficial* de la Unión Europea, núm. C. 364, de 18/12/2000.

[79] El art. 6.1. del Tratado de la Unión Europea dice lo siguiente: "1. La Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados.

"Las disposiciones de la Carta no ampliarán en modo alguno las competencias de la Unión tal como se definen en los Tratados.

"Los derechos, libertades y principios enunciados en la Carta se interpretarán con arreglo a las disposiciones generales del título VII de la Carta por las que se rige su interpretación y aplicación y teniendo debidamente en cuenta las explicaciones a que se hace referencia en la Carta, que indican las fuentes de dichas disposiciones".

En España, el fundamento del derecho a la protección de datos personales se encuentra consagrado en el artículo 18 de la Constitución Nacional, el cual establece lo siguiente:

"1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

"[...]

"4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"[80].

Ello explica que todas las entidades públicas deben velar por la confidencialidad de la información.

En el citado país, la norma sobre protección de datos personales es la ley orgánica 15 de 13 de diciembre de 1999[81]. Esta se aplica a toda modalidad de uso de datos personales tanto por el sector público como por el sector privado[82], lo cual se confirma en el artículo 2 del Real Decreto 1720/2007 que aprueba el reglamento de la mencionada ley[83]. El Capítulo I de la ley se ocupa de los ficheros o bases de datos de titularidad pública y establece un sin número de requisitos para la creación, modificación y supresión de dichos ficheros. Entre ellos, se tiene que para crear, modificar o suprimir un fichero debe publicarse disposición general en el Boletín Oficial del Estado e indicar la finalidad, de quién se pretende obtener datos, el procedimiento de recogida de dichos datos, todo lo que puede ejercerse sobre derechos de acceso, al igual que las medidas de seguridad del susodicho fichero[84].

La ley orgánica 15 de 1999 contiene un artículo sobre la comunicación de datos entre administraciones públicas. Dice la norma que los datos personales recogidos por una administración pública para desempeñar sus funciones no serán comunicados a otras para el ejercicio de competencias diferentes. Hace salvedad de que se podrá hacer si los datos se van a tratar para fines históricos, estadísticos y científicos[85].

[80] Reino de España, Constitución Política, art. 18. Web 27 Feb 2018. <*http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/Constitucion_es.pdf*>

[81] Reino de España, ley orgánica 15 de 1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, Jefatura del Estado, BOE num. 298 de 14 diciembre 1999, ref.: BOE-A-1999-23750.

[82] Reino de España, ley orgánica 15 1999, art. 2º.

[83] Cfr. Reino de España. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. El texto oficial se puede consultar en el *Boletín Oficial del Estado* (BOE) en: *https://www.boe.es/buscar/act.php?id=BOE-A-2008-979*

[84] Reino de España, ley orgánica 15 1999, art. 20.

[85] Reino de España, ley orgánica 15 de 1999, art. 21.

La ley orgánica 15 de 1999 se aplica al tratamiento de datos personales tanto en el sector público como en el sector privado[86]. Sin embargo, no será aplicable cuando se trate de bases de datos que conservan personas naturales en ejercicio de sus actividades personales o domésticas[87]. De igual manera, no se aplicará cuando se trata de bases de datos sometidas a las normas sobre protección de materia clasificada[88] o cuando son ficheros establecidos para realizar investigación de terrorismo y delincuencia organizada[89]. Por último, tanto las bases de datos reguladas por la legislación del régimen electoral como lo derivado del registro civil, se rige por sus disposiciones específicas y por lo que especialmente prevea la ley 15 de 1999 para estas[90].

La ley 15 en su Título II, establece los principios generales en materia de protección y tratamiento de datos personales. En primer lugar se menciona el principio de calidad de datos[91], entendido como aquel según el cual la recolección de datos no puede hacerse por medios desleales y dichos datos deben ser ciertos y exactos, y su almacenamiento debe permitir el derecho de acceso a su titular. En segundo lugar, el consentimiento que el titular debe dar ha de ser libre[92], expreso e informado sobre el tratamiento de sus datos. Se consagra como cuarto principio el de la información en el sentido de que se debe informar a los titulares para qué serán tratados los datos y quiénes serán sus destinatarios. No obstante, la ley no contiene expresamente el principio de responsabilidad demostrada.

Los responsables del tratamiento de datos personales, por su parte, deben garantizar su seguridad mediante la adopción de medidas técnicas y organizativas necesarias para evitar "la alteración, pérdida, tratamiento o acceso no autorizado"[93] a las bases de datos. Asimismo, tales responsables tienen un deber de secreto profesional[94].

En el régimen jurídico español no hay norma que regule expresamente el tratamiento de datos personales en el sector público. Sin embargo, la ley orgánica 15 de 1999, incluye un Título sobre disposiciones sectoriales, cuyo capítulo I[95] trata

[86] Reino de España, ley orgánica 15 de 1999, art. 2 num. 1

[87] Reino de España, ley orgánica 15 de 1999, art. 2 num. 2 lit. a).

[88] Reino de España, ley orgánica 15 de 1999, art. 2 num. 2 lit. b).

[89] Reino de España, ley orgánica 15 de 1999, art. 2 num. 2 lit. c).

[90] Reino de España, ley orgánica 15 de 1999, art. 2 num. 3 lits. a) y d).

[91] Reino de España, ley orgánica 15 de 1999, art. 5º.

[92] Reino de España, ley orgánica 15 de 1999, art. 6º.

[93] Reino de España, ley orgánica 15 de 1999, art. 9º.

[94] Reino de España, ley orgánica 15 de 1999, art. 10.

[95] Reino de España, ley orgánica 15 de 1999, Título IV: Disposiciones Sectoriales, Capítulo 1: Ficheros de titularidad pública.

de los ficheros de titularidad pública. En este capítulo se encuentran las disposiciones con respecto a la creación, modificación y supresión de bases de datos de las administraciones públicas[96]. Igualmente, existe un artículo sobre cómo debe realizarse la comunicación de datos entre administraciones públicas[97].

La ley 19 de 2013, por su parte, regula todo el tema de transparencia, el acceso a la información pública y el buen gobierno. Dicha norma se aplica a las administraciones públicas, que son los organismos y entidades consagrados en el artículo 2, dentro de las cuales se infiere están aquellas que ejercen funciones registrales y electorales.

Dentro de los principios consagrados en la ley 19 de 2013 los de transparencia y publicidad[98]. Hace salvedad la norma que si existe ley especial donde el principio de publicidad sea más amplio, esta primará. Por otra parte, son principios técnicos a los que debe adecuarse el portal de la transparencia los de accesibilidad, interoperabilidad y reutilización[99].

De la norma se puede inferir que los deberes de las entidades están íntimamente relacionados con la publicidad activa[100], razón por la cual las administraciones públicas deben publicar información de relevancia jurídica, presupuestaria, estadística, institucional, organizativa y de planificación[101]. Adicionalmente, existe

[96] Reino de España, ley orgánica 15 de 1999, art. 20.

[97] Reino de España, ley orgánica 15 de 1999, art. 21.

[98] Reino de España, ley orgánica 15 de 1999, art. 5º: "1. Los sujetos enumerados en el artículo 2.1 publicarán de forma periódica y actualizada la información cuyo conocimiento sea relevante para garantizar la transparencia de su actividad relacionada con el funcionamiento y control de la actuación pública [...] 3. Serán de aplicación, en su caso, los límites al derecho de acceso a la información pública previstos en el artículo 14 y, especialmente, el derivado de la protección de datos de carácter personal, regulado en el artículo 15. A este respecto, cuando la información contuviera datos especialmente protegidos, la publicidad sólo se llevará a cabo previa disociación de los mismos".

[99] Ley 19 de 9 diciembre 2013, art. 11:

"a. Accesibilidad: se proporcionará información estructurada sobre los documentos y recursos de información con vistas a facilitar la identificación y búsqueda de la información.

"b. Interoperabilidad: la información publicada será conforme al Esquema Nacional de Interoperabilidad, aprobado por el real decreto 4/2010, de 8 enero, así como a las normas técnicas de interoperabilidad

"c. Reutilización: se fomentará que la información sea publicada en formatos que permitan su reutilización, de acuerdo con lo previsto en la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público y en su normativa de desarrollo".

[100] Ley 19 de 9 diciembre 2013, Capítulo 2. "Se entiende por publicidad activa el proveer información institucional, organizativa y de planificación, en materia de transparencia y publicidad relativa a su función. Adicionalmente, también se entiende que debe incluirse información de relevancia jurídica como son las directrices, instrucciones, acuerdos, circulares, o respuestas a consultas que tengan efectos jurídicos".

[101] Ley 19 de 9 2013 arts. 6º, 7º, y 8º.

otro bloque de deberes relacionado con la transparencia para lo cual se ordena la creación de un portal de la transparencia[102].

Reglas especiales sobre tratamiento de datos para entidades con funciones registrales y electorales. En España, la función registral y electoral se somete a sus normas y a lo especialmente previsto en la ley orgánica 15 de 1999. Para ello, la Oficina Central del Registro Civil[103], a quien corresponde la función registral, debe tener en cuenta lo establecido en la ley 20 de 2011 Ley del Registro Civil. Por otro lado, la Junta Electoral Central, a quien corresponde ejercer la función electoral, debe tener en cuenta lo establecido en la ley orgánica 5 de 1985, que contiene todo el régimen electoral.

Respecto de las funciones registrales, la ley 20 del 2011 consolida todo lo referente al registro civil, base de datos única con universalidad de acceso[104]. Lo primero que vale la pena resaltar es que el registro civil es electrónico y se encuentra en una base de datos única cuya estructura y funcionamiento son responsabilidad y competencia del Ministerio de Justicia[105]. Esta base de datos puede ser accedida por todas las administraciones y funcionarios públicos, mediante un procedimiento electrónico que debe surtir ciertos requisitos y prescripciones técnicas[106].

A pesar de esto, por expresa remisión, las disposiciones aplicable al registro civil en cuanto a seguridad de los datos personales son las encontradas en la ley orgánica 15 de 1999[107].

El registro civil tiene una serie de principios de funcionamiento, entre los cuales se encuentran los de legalidad[108], oficialidad[109] y publicidad[110]. No hay nada

[102] Ley 19 de 9 diciembre 2013, art. 10 "La Administración General del Estado desarrollará un portal de transparencia, dependiente del Ministerio de la Presidencia, que facilitará el acceso de los ciudadanos a toda la información a la que se refieren los artículos anteriores relativa a su ámbito de actuación".

[103] Reino de España, ley 20 de 21 julio 2011, Ley del Registro Civil, art. 2º.

[104] Reino de España, ley 20 de 2011, Preámbulo III.

[105] Reino de España, ley 20 de 2011, art. 3 num. 2.

[106] Reino de España, ley 20 de 2011, art. 8 num. 2.

[107] Reino de España, l ey 20 de 2011, art. 3 num. 3.

[108] Reino de España, ley 20 de 2011, art. 13: "Los encargados del registro civil comprobarán de oficio la realidad y legalidad de los hechos y actos cuya inscripción se pretende, según resulte de los documentos que los acrediten y certifiquen, examinando en todo caso la legalidad y exactitud de dichos documentos".

[109] Reino de España, ley 20 de 2011, art. 14: "Los encargados del registro civil deberán practicar la inscripción oportuna cuando tengan en su poder los títulos necesarios. Las personas físicas y jurídicas y los organismos e instituciones públicas que estén obligados a promover las inscripciones facilitarán a los encargados del registro civil los datos e información necesarios para la práctica de aquellas".

[110] Reino de España, ley 20 de 2011, art. 15.

"1. Los ciudadanos tendrán libre acceso a los datos que figuren en su registro individual.

explícito sobre el principio de responsabilidad demostrada. No se consagran deberes especiales con respecto a la protección de datos en el registro civil, solo se consagran deberes de los individuos ante el registro civil[111].

Respecto de las funciones electorales, la ley orgánica 5 de 1985 sobre el régimen electoral general de España regula el acceso a los datos censales en la Sección IV. En primer lugar, establece que será por real decreto como se regularán los datos personales de los electores, requeridos para inscribirse en el censo electoral[112]. Adicionalmente, establece que la única manera de obtener información particularizada sobre el censo electoral es mediante orden judicial. Sin embargo, hace la aclaración de que la Oficina del Censo Electoral puede facilitar datos estadísticos siempre y cuando no revelen circunstancias personales de los electores[113].

En materia de datos personales, se permite que los representantes de cada candidatura obtengan una copia del censo del distrito que les corresponde. Esto debe entregarse con un soporte apto para que el tratamiento informático sea el adecuado[114].

La función electoral también está desarrollada en el real decreto 1799 de 2003 en el que se regula el contenido de las listas electorales y las copias del censo electoral. En este decreto se encuentra lo relacionado al contenido de las listas de votación, a aquello que es necesario para que un ciudadano consulte sus datos, y las personas que están excluidas en las copias del censo electoral. Sin embargo, no se hace mayor mención al tratamiento de datos personales.

De la autoridad de protección de datos personales, el tratamiento de datos en el sector público y el principio de responsabilidad demostrada.La autoridad de tratamiento de datos personales en España es la Agencia de Protección de Datos. Cuenta con un órgano denominado el Registro General de Protección de Datos[115]. En dicho registro se tiene conocimiento de los datos personales que están siendo tratados, la finalidad de dicho tratamiento, y la identificación de la autoridad que

”2. El registro civil es público. Las administraciones y funcionarios públicos, para el desempeño de sus funciones y bajo su responsabilidad, podrán acceder a los datos contenidos en el registro civil”.

[111] Reino de España, ley 20 de 2011, cap. 2.

[112] Reino de España, ley orgánica 5 de 1985, art. 41 num. 1.

[113] Reino de España, ley orgánica 5 de 1985, art. 41 num. 3: “No obstante, la Oficina del Censo Electoral puede facilitar datos estadísticos que no revelen circunstancias personales de los electores”.

[114] Reino de España, ley orgánica 5 de 1985, art. 41 num. 5: “Los representantes de cada candidatura pueden obtener, el día de la proclamación de candidatos, una copia del censo del distrito correspondiente, en soporte apto para su tratamiento informático. Alternativamente los representantes generales pueden obtener, en las mismas condiciones, una copia del censo vigente de los distritos donde su partido, federación o coalición presente candidaturas”.

[115] Reino de España, ley orgánica 15 de 1999, art. 39.

hace uso de dichos datos. En pro del derecho de acceso, el registro es de consulta pública y gratuita[116]. La ley establece que tanto las bases de datos de entidades públicas como las de entidades privadas son objeto de inscripción en el registro.

Dentro de las recomendaciones de la Agencia de Protección de Datos no se encuentran instrucciones para el cumplimiento de la función registral o electoral.

En cuanto al principio de responsabilidad demostrada, la autoridad publicó un artículo sobre el enfoque de riesgos en el reglamento de protección de datos donde establece las siguientes fases para implantar una política de riesgos: a) comunicación, b) contexto, c) identificar riesgos, d) analizar y evaluar el riesgo, e) gestionar el riesgo, y f) hacer seguimiento del riesgo[117]. Esto con el fin de que los responsables del tratamiento de datos personales estén en condiciones de demostrar la licitud del tratamiento de dichos datos.

D) *Estados Unidos Mexicanos*

Las reformas constitucionales recientes en los Estados Unidos Mexicanos[118] no sólo otorgan *status* especial a los datos personales como información constitucionalmente protegida sino que, entre otros, consagran explícitamente el derecho a la protección de los datos personales y establecen los derechos ARCO[119] como núcleo fundamental de dicho derecho.

En efecto, mediante la reforma constitucional de 2007[120] se incorporaron los datos personales como categoría de información de peculiar relevancia constitucional y se consagraron los derechos de acceso y rectificación de los datos, los cuales forman parte de los derechos ARCO. Dos años después, con la reforma de 2009[121], no solo se creó el derecho constitucional a la "protección de datos perso-

[116] Reino de España, ley orgánica 15 de 1999, art. 14.

[117] Agencia Española de Protección de Datos, 15 noviembre 2017. "El enfoque de riesgos en el Reglamento de Protección de Datos". Web. 27 Feb 2018. *<https://www.agpd.es/blog/el-enfoque-de-riesgos-en-el-reglamento-general-de-proteccion-de-datos-ides-idPhp.php>*

[118] Sobre este aspecto y la protección de datos personales en México, consúltese, entre otros: Ximena Puente de la Mora,. "Protección de datos personales en México ante del modelo norteamericano y el europeo", en *Derecho & TIC 10.0*, GECTI, Bogotá, Edit. Temis y Ediciones Uniandes, 2011,

[119] El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de 21 diciembre 2012, establece que los "Derechos ARCO" son los derechos de "acceso, rectificación, cancelación y oposición".

[120] Esta reforma constitucional fue publicada el 20 de julio de 2007 en el *Diario Oficial de la Federación* y desde ese entonces entró en vigencia el "*decreto por el cual se adiciona un segundo párrafo con siete fracciones al artículo 6 de la Constitución Política de los Estados Unidos de México*". En las partes II y III se incluyeron disposiciones atinentes a los datos personales junto con su acceso y rectificación.

[121] El 1º de junio de 2009 se publicó en el *Diario Oficial de la Federación* el "Decreto por el que se adiciona un segundo párrafo, recorriendo los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos", de 21 de abril de 2009.

nales" sino que se incluyeron explícitamente los derechos ARCO al ordenar en el artículo 16 que las personas tienen derecho al "acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición en los términos que fije la ley". Adicionalmente, en ese artículo se establecieron la seguridad nacional, las disposiciones de orden público, la protección de los derechos de los terceros, la seguridad y la salud pública como motivos constitucionalmente válidos para que mediante ley y de forma excepcional se limiten "los principios que rijan el tratamiento de datos".

La Constitución mexicana dice lo siguiente:

"Artículo 16. [...]

"Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros".

Con esto no solo se le da a los derechos ARCO importancia del más alto nivel jerárquico en el ordenamiento jurídico mexicano sino que ellos forman parte del ámbito medular del derecho de la protección de los datos personales. Así las cosas, en nuestra opinión, los derechos de acceso, rectificación, cancelación y oposición (ARCO) forman parte del núcleo esencial del derecho constitucional de la protección de datos porque sin la posibilidad para que la persona ejerza esas cuatro facultades carecería de efectividad el precitado derecho. En este sentido, y refiriéndose al caso español, el doctor Antonio Troncos Reigada ha precisado que los derechos de acceso, rectificación, cancelación y oposición "forman parte, como lo ha determinado la jurisprudencia constitucional, del contenido esencial del derecho fundamental a la protección de datos personales a la luz de la opinión generalmente admitida de lo que este derecho significa —sin los cuales este derecho no es reconocible como perteneciente a su tipo previo— y sin cuyo ejercicio los intereses jurídicos que dan vida a este derecho resultan desprotegidos"[122].

A principios de 2017, en Estados Unidos Mexicanos se expidió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Nótese que se hace expresa mención de que en el ámbito federal, estatal y municipal son sujetos obligados por la Ley "cualquier autoridad, entidad, órgano y organismo de los poderes ejecutivo, legislativo y judicial, órganos autónomos, partidos políticos,

[122] Antonio Troncoso Reigada, *La protección de datos personales. En busca del equilibrio*, Valencia, Tirant lo Blanch, 2006, pág. 548.

fideicomisos y fondos públicos"[123]. En este sentido, los particulares, sean personas naturales o jurídicas, no se someten a esta Ley sino a las disposiciones de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[124].

El artículo 4 de la citada ley establece que se aplica a cualquier tratamiento de datos personales. Siendo así, no hace distinción entre soportes físicos y electrónicos. De igual manera, no discrimina entre la forma y modalidad de la creación de la base de datos; el tipo de soporte que tiene; ni su procesamiento, almacenamiento, y organización[125].

En el capítulo I[126] del Título segundo de la mencionada ley, se encuentran consagrados un conjunto de principios que el responsable del tratamiento debe cumplir cuando recolecta, almacena, usa, circula o realiza cualquier actividad con datos personales, a saber: principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados incorporó los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales. Estos principios son consistentes con los que internacionalmente se han desarrollado durante varias décadas.

El capítulo I[127] del Título segundo de la ley enuncia un conjunto de principios que el responsable del tratamiento debe cumplir cuando recolecta, almacena, usa, circula o realiza cualquier actividad con datos personales. Los siguientes son los principales aspectos de dichos preceptos:

El principio de licitud (art. 17) exige a los responsables que el tratamiento de los datos personales lo realicen observando lo que ordena la ley. De esta forma se

[123] Estados Unidos Mexicanos, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados DOF 26-01-2017, art. 1º inc. 5º: "Son sujetos obligados por esta ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los poderes ejecutivo, legislativo y judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos".

[124] Estados Unidos Mexicanos, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados DOF 26-01-2017, Artículo 1 Inc. 7 "En todos los demás supuestos diferentes a los mencionados en el párrafo anterior, las personas físicas y morales se sujetarán a lo previso en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares"

[125] Estados Unidos Mexicanos, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados DOF 26-01-2017, art. 4º: "La presente ley será aplicable a cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización".

[126] Estados Unidos Mexicanos, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, arts. 16 al 30.

[127] *Ibidem*.

busca que el tratamiento de datos personales no se efectúe de manera caprichosa o arbitraria, sino objetiva y respetando el Estado de derecho, el cual es un elemento esencial de la democracia. Este principio pone de presente que el tratamiento de datos es una actividad reglada con facultades o atribuciones limitadas o definidas en la ley. Por lo tanto, no puede hacerse de cualquier forma sino de la manera que lo indica la ley.

El principio de finalidad (art. 18) busca que el tratamiento tenga como objetivo la realización de "finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera". Así, quien trate datos no puede usarlos para cualquier propósito sino para aquellas establecidas en el aviso de privacidad, salvo que "cuente con atribuciones conferidas en la ley y medie el consentimiento del titular", situación en la cual excepcionalmente podrá tratar los datos para otras finalidades.

El línea con lo anterior, el artículo 25 (principio de proporcionalidad), ordena que solo se pueden tratar los "datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento". Mediante el principio de lealtad se proscribe el tratamiento engañoso de la información sobre las personas. Por eso, entre otras, el artículo 19 ordena que "el responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad".

La ley define el consentimiento como la *"manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos*" (art. 2º) y precisa que este será "libre" cuando no "medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular", "específico" cuando las finalidades sean "concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento" e "informado" cuando el "*titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales*" (art. 20). Además, ordena que el consentimiento puede ser expreso o tácito, indicando que es tácito "*cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario*" (art. 21). El concepto, la obligatoriedad del uso de los avisos de privacidad y su contenido fueron regulados principalmente en los artículos 3 y 26 a 28 de la ley.

El artículo 23 (principio de calidad) exige que los datos personales sean veraces, exactos, completos, correctos y actualizados. Le corresponde al responsable adoptar medidas para que ello sea así. En suma, la información de calidad es una condición para el debido tratamiento de los datos y de ella dependen algunos derechos de las personas como su buen nombre o que las decisiones que se adopten con fundamento en los datos personales sean correctas, pertinentes o apropiadas. No

debe perderse de vista que la información es, por excelencia, una herramienta para tomar decisiones. Si no se logra mantener sistemas de información de calidad, las organizaciones deben reflexionar si tienen "bases de datos o basureros de datos".

La redacción del principio confiere espacio importante a la vigencia del dato de manera que se deje de tratar información que ya no es necesaria para cumplir las finalidades previstas en el aviso de privacidad. En estos casos, los datos "deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos". Estos plazos de conservación están vinculados a la finalidad del tratamiento o las exigencias legales. En ese sentido, la parte final del artículo 23 señala que "los plazos de conservación de los datos personales no deberán exceder aquellos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales".

Para cumplir lo anterior, el artículo 24 ordena al responsable "*establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleve a cabo*". En estos casos, continúa la norma, "el responsable deberá incluir mecanismos que le permitan cumplir con los plazos fijados para la supresión de los datos personales, así como para realizar una revisión periódica sobre la necesidad de conservar los datos personales".

Con el principio de información se busca que el titular tenga conocimiento de los principales aspectos que regirán el tratamiento de sus datos personales. En ese sentido, el artículo 26 ordena al responsable "informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto".

El aviso de privacidad, como se observa, se constituye en el mecanismo para informar al titular los aspectos indicados. Por eso, la norma es enfática en exigir que dichos avisos cumplan algunos requerimientos: (i) estar redactados y estructurados de manera clara y sencilla para que puedan ser entendidos por el titular; (ii) contener cierta información indicada en los artículos 27 y 28[128] según

[128] El art. 27 dice lo siguiente: "El aviso de privacidad a que se refiere el artículo 3, fracción II, se pondrá a disposición del titular en dos modalidades: simplificado e integral. El aviso simplificado deberá contener la siguiente información:

"I. La denominación del responsable;

"II. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquellas que requieran el consentimiento del titular;

"III. Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar:

se trate del aviso de privacidad simplificado o integral respectivamente, y (iii) ser difundido por los medios electrónicos y físicos con que cuente el responsable.

Finalmente, el principio de responsabilidad pone de presente que el reto de la ley es su cumplimiento real y efectivo. Por eso, los artículos 29 y 30 de la ley envían un mensaje contundente a los sujetos obligados, ordenándoles que adopten medidas de buen gobierno corporativo de datos, que garanticen que los principios de la ley y sus demás disposiciones se cumplan en la práctica.

La ley indica en el artículo 30 las acciones básicas que el sujeto obligado debe adelantar para implantar el principio de responsabilidad, ordenándose que (i) destinen recursos para cumplir los programas de gestión de datos; (ii) elaboren políticas y programas de protección de datos de carácter obligatorio en cada sujeto obligado; (iii) capaciten permanentemente a los funcionarios para consolidar una cultura de tratamiento responsable de datos personales; (iv) revisen periódicamente las medidas de seguridad; (v) pongan en práctica procesos de control interno y externo respecto de las políticas y los programas de protección de datos; (vi) habiliten herramientas y administren procesos para atender consultas y reclamos de los titulares; (vii) desarrollen el principio de protección de datos desde el diseño y por defecto en todas las gestiones o procesos que realice el sujeto obligado y que implique el tratamiento de datos personales.

”a) Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales, y

”b) Las finalidades de estas transferencias;

”IV. Los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular, y

”V. El sitio donde se podrá consultar el aviso de privacidad integral”.

Art. 28. “El aviso de privacidad integral, además de lo dispuesto en las fracciones del artículo anterior, al que refiere la fracción V del artículo anterior deberá contener, al menos, la siguiente información:

”I. El domicilio del responsable;

”II.Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles;

”III. El fundamento legal que faculta al responsable para llevar a cabo el tratamiento;

”IV. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquellas que requieren el consentimiento del titular;

”V. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO;

”VI. El domicilio de la Unidad de Transparencia, y

”VII. Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad”.

El Capítulo II del Título Segundo contiene los deberes del responsable del tratamiento de datos personales. El deber más importante es el de seguridad, que comprende varias dimensiones, debido a que la seguridad debe ser de carácter administrativa, física y técnica[129], esto con el fin de que el responsable del tratamiento de datos personales pueda garantizar que los datos no van a sufrir de daño, pérdida, alteración o destrucción. Asimismo, la ley menciona los deberes de confidencialidad, integridad y disponibilidad de la información[130].

De otra parte, en México se expidió en 2015 la Ley General de Transparencia y Acceso a la Información Pública, reglamentaria del artículo 6º de la Constitución Política. Vale aclarar que son sujetos obligados todas las autoridades, entidades, órganos y organismos de los poderes ejecutivo, legislativo y judicial, al igual que los órganos autónomos, los partidos políticos, los fideicomisos y los fondos públicos. Como consecuencia de esto, no son sujetos obligados las personas jurídicas que no reciben recursos públicos ni ejercen actos de autoridad en el ámbito federal o municipal y las personas naturales[131].

Todos los organismos que sean garantes del derecho de acceso a la información deben tener en cuenta una serie de principios entre los cuales se destaca el de transparencia[132] que consiste en dar publicidad a las deliberaciones de los actos relacionados con las atribuciones de cada organismo y dar acceso a la información que generen en el desarrollo de sus funciones. También se rige dicha ley por los principios de certeza, eficacia, imparcialidad, independencia, legalidad, máxima publicidad, objetividad y profesionalismo[133].

[129] Estados Unidos Mexicanos, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados DOF 26-01-2017, art. 31: "Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad".

[130] Estados Unidos Mexicanos, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados DOF 26-01-2017, art. 31.

[131] Estados Unidos Mexicanos, Ley General de Transparencia y Acceso a la Información Pública DOF 04-05-2015, art. 23.

[132] Estados Unidos Mexicanos, Ley General de Transparencia y Acceso a la Información Pública DOF 04-05-2015, art. 8º "[...] IX. Transparencia. Obligación de los organismos garantes de dar publicidad a las deliberaciones y actos relacionados con sus atribuciones, así como dar acceso a la información que generen".

[133] Estados Unidos Mexicanos, Ley General de Transparencia y Acceso a la Información Pública DOF 04-05-2015, art. 8º. "Los organismos garantes del derecho de acceso a la información deberán regir su funcionamiento de acuerdo a [*sic*] los siguientes principios:

Existe deberes que los sujetos obligados deben cumplir dentro de los cuales vale la pena resaltar los de constituir un comité de transparencia, unas unidades de transparencia, y proporcionar capacitación continua y especializada al personal que forme parte de estos. Asimismo, deben proteger y resguardar la información clasificada a la vez que promueven la generación y publicación de la información en formatos abiertos y accesibles[134].

En México, no hay una sola entidad que ejerza las funciones registrales y electorales. Siendo ello así, por una parte, se tiene el Instituto Nacional Electoral (INE) que ejerce la función electoral al organizar los procesos electorales en la federación y coadyuva en la organización de elecciones locales[135]. Por otra parte, la función registral se encuentra en cabeza de la Dirección General del Registro Civil que es una institución de orden público que autoriza todos los actos y hechos relacionados con el estado civil de las personas[136]. Ambas entidades deben atender a lo

---

”I. Certeza. Principio que otorga seguridad y certidumbre jurídica a los particulares, en virtud de que permite conocer si las acciones de los organismos garantes son apegadas a derecho y garantiza que los procedimientos sean completamente verificables, fidedignos y confiables;

”II. Eficacia. Obligación de los organismos garantes para tutelar, de manera efectiva, el derecho de acceso a la información;

”III. Imparcialidad. Cualidad que deben tener los organismos garantes respecto de sus actuaciones de ser ajenos o extraños a los intereses de las partes en controversia y resolver sin favorecer indebidamente a ninguna de ellas;

”IV. Independencia. Cualidad que deben tener los organismos garantes para actuar sin supeditarse a interés, autoridad o persona alguna;

”V. Legalidad. Obligación de los organismos garantes de ajustar su actuación, que funde y motive sus resoluciones y actos en las normas aplicables;

”VI. Máxima publicidad. Toda la información en posesión de los sujetos obligados será pública, completa, oportuna y accesible, sujeta a un claro régimen de excepciones que deberán estar definidas y ser además legítimas y estrictamente necesarias en una sociedad democrática;

”VII. Objetividad. Obligación de los organismos garantes de ajustar su actuación a los presupuestos de ley que deben ser aplicados al analizar el caso en concreto y resolver todos los hechos, prescindiendo de las consideraciones y criterios personales;

”VIII. Profesionalismo. Los servidores públicos que laboren en los organismos garantes deberán sujetar su actuación a conocimientos técnicos, teóricos y metodológicos que garanticen un desempeño eficiente y eficaz en el ejercicio de la función pública que tienen encomendada, y

”IX. Transparencia. Obligación de los organismos garantes de dar publicidad a las deliberaciones y actos relacionados con sus atribuciones, así como dar acceso a la información que generen”.

[134] Estados Unidos Mexicanos, Ley General de Transparencia y Acceso a la Información Pública DOF 04-05-2015, art. 24.

[135] Instituto Nacional Electoral. Web 7 marzo. *https://www.ine.mx*

[136] Consejería Jurídica y de Servicios Legales. “Dirección General del Registro Civil” Web 07 marzo. <*http://www.rcivil.cdmx.gob.mx*>

consagrado en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y en la Ley General de Transparencia y Acceso a la Información Pública por ser sujetos obligados.

Como ya se dijo, el INE debe cumplir con lo establecido en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Adicionalmente, el 15 de diciembre de 2017 se aprobó el reglamento de protección de datos personales[137] cuya función es adecuar la normativa interna a las obligaciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, deber que adquirió el INE en el artículo 7º transitorio de la mencionada ley[138].

El ámbito de aplicación del reglamento cubre todo tratamiento de datos personales que estén en soportes físicos, electrónicos y mixtos, que se encuentren a cargo de los sujetos obligados en el ordenamiento electoral[139]. Adicionalmente, el reglamento tiene como guía los principios de certeza, legalidad, independencia, imparcialidad, máxima publicidad y objetividad[140].

Los deberes atribuibles al responsable del tratamiento son los establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados: el de seguridad y confidencialidad[141].

Por su parte, la Dirección General del Registro Civil todavía no ha emitido el reglamento interno para la protección de datos personales, pero se espera que ello suceda antes de julio de 2018.

De la autoridad de protección de datos personales, el tratamiento de datos en el sector público y el principio de responsabilidad demostrada. La autoridad mexicana encargada del tratamiento de datos personales es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales[142] (INAI).

En materia de protección de datos personales para el sector público, el INAI no ha publicado documentos de interés, contrario a lo que ha sucedido con el sector privado. Adicionalmente, ha difundido gran variedad de estudios en materia de protección de datos, algunos de los cuales sirven como estudio para elaborar guías

[137] Instituto Nacional Electoral-Consejo General- INE/CG557/2017.

[138] Además del reglamento, el INE en su página web se puede consultar la Manifestación de Protección de Datos Personales del Registro Federal de Electores, que contiene una explicación de protección de datos personales para los ciudadanos que la consulten. Se puede acceder a ella en *<https://www.ine.mx/credencial/manifestacion-proteccion-datos-personales-del-registro-federal-electores/>*

[139] Instituto Nacional Electoral-Consejo General- INE/CG557/2017, art. 4º.

[140] Instituto Nacional Electoral-Consejo General- INE/CG557/2017, arts. 16 a 30.

[141] Instituto Nacional Electoral-Consejo General- INE/CG557/2017, arts. 31 a 36.

[142] El sitio web del INAI es: *http://inicio.inai.org.mx/SitePages/ifai.aspx*

para el cumplimiento de obligaciones de protección de datos[143]. Sin embargo, no hay nada concreto sobre protección de datos en cumplimiento de la función electoral y la función registral.

El INAI aún no ha expedido guías sobre el principio de responsabilidad demostrada, pero está trabajando para publicarlas en 2018.

E) *República de Perú*

En Perú, la protección de datos personales se encuentra consagrada en el artículo 2, numerales 5 y 6 de la Constitucional Política:

"Toda persona tiene derecho:

"[...] 5. A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional.

"El secreto bancario y la reserva tributaria pueden levantarse a pedido del juez, del Fiscal de la Nación, o de una comisión investigadora del Congreso con arreglo a ley y siempre que se refieran al caso investigado.

"6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar"[144].

De allí se deriva que las entidades deben garantizar el acceso a la información y también su confidencialidad.

La ley 29.733 de 21 de junio de 2011 tiene por objeto garantizar el derecho fundamental a la protección de datos, por lo cual regula la materia íntegramente. Dicha ley es aplicable a los datos personales contenidos en bases de datos de la administración pública y de los entes privados en todo el territorio peruano[145]. No se someten al régimen previsto en la ley, los bancos de datos personales creados por personas naturales para fines relacionados con su vida privada[146] y aquellos bancos personales que tratan datos para la defensa nacional, seguridad pública, y desarrollo de investigaciones en materia penal[147].

[143] INAI- Documentos de Interés. Web 7 marzo. *http://inicio.inai.org.mx/SitePages/Documentos-de-Interes.aspx?a=m4*

[144] República de Perú, Constitución Política, art. 6º nums. 5 y 6. Web 28 febrero 2018 <*http://www4.congreso.gob.pe/ntley/Imagenes/Constitu/Cons1993.pdf*>

[145] República de Perú, ley 29.733 de 2011, Ley de protección de Datos Personales, art. 3º.

[146] República de Perú, ley 29.733 de 2011, art. 3º num. 1.

[147] República de Perú, ley 29.733 de 2011, art. 3º num. 2.

El Título I de la ley 29.733 de 2011 se ocupa de los principios rectores. Así, se encuentran consagrados el principio de legalidad[148], el de consentimiento[149], el de finalidad[150], de proporcionalidad[151], de calidad[152], de seguridad[153], de disposición de recurso[154] y de nivel de protección adecuado[155]. El principio de *accountability* o responsabilidad demostrada no se encuentra previsto en dicha ley.

El título IV contiene el marco normativo de las obligaciones del titular y responsable del banco de datos personales. Entre sus obligaciones se encuentran las de efectuar el tratamiento de datos personales solo con previo consentimiento informado, no recopilar datos mediante medios fraudulentos, actualizar la información y suprimir y sustituirla en los casos necesarios[156].

En Perú, la ley 29.733 de 2011 consagra el régimen de tratamiento de datos personales en su integridad, por lo cual no hay norma especial sobre tratamiento de datos personales para el sector público y para el sector privado.

La ley 27.806 de 2003 es la ley de transparencia y acceso a la información pública, que debe leerse en concordancia con la Directiva 1 de 2018 que contiene

[148] República de Perú, ley 29.733 de 2011, art. 4º: "El tratamiento de los datos personales se hace conforme a lo establecido en la ley. Se prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos".

[149] República de Perú, ley 29.733 de 2011, art. 5º: "Para el tratamiento de los datos personales debe mediar el consentimiento de su titular".

[150] República de Perú, ley 29.733 de 2011, art. 6º: "Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización".

[151] República de Perú, ley 29.733 de 2011, art. 7º: "Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados".

[152] República de Perú, ley 29.733 de 2011, art. 8º: "Los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados. Deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento".

[153] República de Perú, ley 29.733 de 2011, art. 9º: "El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate".

[154] República de Perú, ley 29.733 de 2011, art. 10: "Todo titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales".

[155] República de Perú, ley 29.733 2011, art. 11.

[156] República de Perú, ley 29.733 de 2011, art. 28.

los lineamientos para el reporte de solicitudes de acceso a la información de las entidades de la administración pública.

En concordancia con el artículo 2º, la ley 27.806 aplicable a todas las entidades de la administración pública, que se mencionan en el artículo 1º del Título Preliminar de la Ley de Procedimiento Administrativo General.

El pilar de la ley 27.806 es el principio de publicidad, el cual consagra que toda información que posee el Estado es pública, salvo los casos del artículo 15 de la ley, por lo que el Estado debe adoptar medidas para garantizar y promover la transparencia (segundo principio consagrado)[157]. En el texto normativo no se menciona el principio de responsabilidad demostrada de manera expresa.

La obligación más importante para el Estado es la de entregar la información que las personas demanden para así darle completo alcance al principio de publicidad[158].

En Perú, la función registral es competencia del Registro Nacional de Identificación y Estado Civil (RENIEC)[159] mientras que la función electoral está a cargo de la Oficina Nacional de Procesos Electorales. No hay regulación específica para estas entidades, razón por la cual se someten a lo previsto en la Ley de Protección de Datos, la Ley de Transparencia y Acceso a la Información y la Directiva 1 de 2018. Se resalta que las entidades públicas deben remitir toda su información a la Dirección de Transparencia y Acceso a la información Pública mediante formatos especiales[160]. Si no se envía el reporte anual de acceso a la información, este no formará parte del reporte que la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos entrega al Congreso de la República y la Contraloría General de la República adoptará las medidas pertinentes[161].

De la autoridad de protección de datos personales, el tratamiento de datos en el sector público y el principio de responsabilidad demostrada. La Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales es la autoridad competente en materia de tratamiento de datos personales en Perú.

La Directiva 1 de 2018 que contiene lineamientos para desarrollar la ley 27.806 a que ya hemos hecho referencia, contiene instrucciones para el Sector Público con respecto a los lineamientos a seguir para entregar el reporte de solicitudes de acceso a la información pública. Su ámbito de aplicación comprende todas

[157] República de Perú, ley 27.806 de 2003, Ley de Transparencia y Acceso a la Información Pública, art. 3º.

[158] República de Perú, ley 27.806 de 2003, art. 3 num. 3.

[159] Registro Nacional de Identificación y Estado Civil. Web 18 febrero 2018 *<https://www.reniec.gob.pe/portal/intro.htm>*

[160] República de Perú, Directiva 1 de 2018, arts. 7º, 8º, y 9º.

[161] República de Perú, Directiva 1 de 2018, art. 10.

las entidades de la administración pública[162]. Vale aclarar además que no hay instrucciones puntuales sobre la función registral y electoral.

En la actualidad no hay instrucciones sobre el principio de responsabilidad y tampoco se encuentra una guía sobre el mismo.

F*) República Oriental del Uruguay*

El derecho a la protección de datos personales no está expresamente previsto en la Constitución. Sin embargo, se puede afirmar que tácitamente está comprendido en la Constitución Política en el artículo 72, que establece "la enumeración de derechos, deberes y garantías hechas por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno"[163].

La ley 18.331 de 11 de agosto de 2008 regula la materia de tratamiento de datos personales en su integridad. Dicha ley se aplica a los datos personales que hayan sido registrados sin importar en qué soporte se hagan y si pertenecen al sector público o privado[164]. Se exceptúan de la obligación de cumplir la ley aquellas bases de datos que contengan personas naturales en ejercicio de sus actividades personales, las que tienen como objetivo garantizar la seguridad pública y las que están reguladas por leyes especiales[165].

El Capítulo II contiene los principios generales, que son los siguientes: legalidad, veracidad, finalidad, previo consentimiento informado, seguridad de los datos, reserva y responsabilidad[166]. En cuanto al principio de responsabilidad la

[162] República de Perú, Ley de Procedimiento Administrativo General, art. 1º.

[163] República Oriental del Uruguay, Constitución Política de 1997, Web 28 febrero <*https://parlamento.gub.uy/documentosyleyes/constitucion*>

[164] República Oriental del Uruguay, ley 18.331 del 11 de agosto de 2008, artículo 3 inc 1

[165] República Oriental del Uruguay, Ley 18.331 de 2008, art. 3º lits. a, b y c.

[166] República Oriental del Uruguay, Ley 18.331 de 2008, art. 5º: "Valor y fuerza. La actuación de los responsables de las bases de datos, tanto públicos como privados, y, en general, de todos quienes actúen en relación a datos personales de terceros, deberá ajustarse a los siguientes principios generales:

"A) Legalidad.

"B) Veracidad.

"C) Finalidad.

"D) Previo consentimiento informado.

"E) Seguridad de los datos.

"F) Reserva.

"G) Responsabilidad.

"Dichos principios generales servirán también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de las disposiciones pertinentes".

ley establece que "el responsable de la base de datos es responsable de la violación de las disposiciones de la presente ley"[167].

Dicha ley no consagra un capítulo destinado a los deberes del responsable de tratamiento de datos personales pero se entiende que deben cumplir a cabalidad con lo establecido en los principios.

Tampoco existe una norma especial sobre tratamiento de datos personales en el Sector Público, pero sí hay un capítulo dedicado a las bases de datos de titularidad pública en la ley 18331 de 2008, la cual contiene indicaciones para la creación, modificación o supresión de dichas bases de datos.

La ley 18.381 de 2008, por su parte, estipula el derecho de acceso a la información pública. Su ámbito de aplicación se extiende a todas las entidades públicas y no establece ningún artículo que liste los principios que regirán, por lo cual se entiende que toda la ley desarrolla el principio de acceso a la información.

La función registral y electoral en Uruguay está a cargo de la Corte Electoral. Esta Corte emite la credencial cívica para ciudadanos nacionales y la carta de ciudadanía para ciudadanos extranjeros. No hay regulación especial sobre el tratamiento de datos personales en las funciones registrales y electorales más allá de las normas que se aplican a las bases de datos del sector público.

De la autoridad de protección de datos personales, el tratamiento de datos en el sector público y el principio de responsabilidad demostrada. La Unidad Reguladora de Control de datos es un órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) que funge como autoridad de tratamiento de datos personales. No hay mayor desarrollo sobre instrucciones para el cumplimiento de la función registral y electoral. Tampoco existen orientaciones o directrices sobre el principio de responsabilidad demostrada.

[167] República Oriental del Uruguay, ley 18.331 de 2008, art. 12.

Capítulo III

BUENAS PRÁCTICAS Y RESPONSABILIDAD DEMOSTRADA SOBRE TRATAMIENTO DE DATOS PERSONALES EN EL CONTEXTO INTERNACIONAL

La expresión *buenas prácticas* comúnmente se refiere a experiencias que han producido resultados positivos, demostrando su eficacia y utilidad en un contexto concreto. Se trata de iniciativas exitosas dirigidas a mejorar lo que se hace para satisfacer las necesidades y expectativas de los clientes, de los usuarios, de terceros, etc. Tal y como lo anota el *International Bureau of Education* (IBE) de la Unesco, definir el concepto de buena práctica no es fácil, pues se utiliza en varios contextos: "Se puede considerar que las «buenas prácticas» corresponden a casos en los cuales procesos y comportamientos han obtenido resultados positivos, es decir, que las «buenas prácticas» son comparables a las "mejores prácticas»". Otros definen una *buena práctica* de manera más general, "considerándola como un enfoque que frecuentemente es innovador, que ha sido probado y evaluado y que tiende a tener éxito en otros contextos. Una buena práctica es la innovación que permite mejorar el presente y por lo tanto es o puede ser un modelo o norma para determinado sistema"[1].

Señala Beatriz Boza que una buena práctica es "una actividad o proceso que ha producido destacados resultados en el manejo de una organización y que puede ser replicada en otras organizaciones para mejorar la efectividad, eficiencia e innovación de las mismas"[2]. En suma, una buena práctica es una experiencia que puede servir de modelo para otras organizaciones. Estas experiencias también comprenden las recomendaciones, guías o sugerencias que emiten algunas organizaciones.

Visto lo anterior, en este libro se entenderá por buenas prácticas no solo las experiencias que se han replicado en otras partes del mundo por ser exitosas, sino

[1] Cita traducida de Anne Abdoulaye, "Conceptualisation et dissémination des bonnes pratiques en éducation: essai d'une approche internationale à partir d'enseignement tirés d'un projet", en *Développement curriculaire et "bonne pratique" en éducation*, 2003, PDF 324 KB (en francés). Publicado en *http://www.ibe.unesco.org/Spanish/AIDS /BPractices/BPratiques_home.htm*

[2] Beatriz Boza, *Acceso a la información del Estado: marco legal y buenas prácticas*, Lima, Konrad Adenauer Stiftung, 2004, pág. 71.

los documentos y las medidas proactivas plasmadas por diferentes autoridades de protección de datos y por organizaciones dedicadas al tratamiento de protección de datos.

En este sentido, a continuación se hará un análisis del principio de responsabilidad demostrada (*accountability*, su denominación en inglés) en documentos internacionales para luego tratar las eventuales mejores prácticas en materia de *accountability* en algunos países (Argentina, España, México, Perú y Uruguay).

1. Análisis del principio de responsabilidad demostrada en documentos internacionales

El término "responsabilidad" (*accountability*) proviene del mundo anglosajón[3] y a pesar de las diferentes acepciones que puedan darse sobre su significado, se ha entendido que en la protección de datos dicha expresión se refiere al modo como una organización debe cumplir en la práctica las regulaciones sobre la materia y a la manera como debe demostrar que lo hecho es útil, pertinente y eficiente.

A continuación nos referiremos a los principales aspectos sobre el principio de responsabilidad demostrada en los documentos emitidos por la Red Iberoamericana de Protección de Datos (en adelante RIPD); la Unión Europea (UE); la Organización de Estados Americanos (OEA); la Organización para la Cooperación y el Desarrollo Económico (OCDE); la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (CIAPDP); el Foro de Cooperación Económica Asia Pacífico (APEC) y la Organización de las Naciones Unidas (ONU).

Este análisis tiene por propósito extraer las principales ideas o buenas prácticas que surgen de dichos documentos para tenerlos presentes en la elaboración del Programa Integral de Gestión de Datos Personales (en adelante PIGDP) de la Registraduría Nacional del Estado Civil.

Se observa que los primeros documentos fueron escritos en la década de los ochenta y que posteriormente algunos fueron modificados para ampliar su contenido e incluir la obligación de estar en capacidad de probar que los mecanismos son útiles, adecuados y eficientes. Así las cosas, iniciaremos con una breve referencia a las organizaciones que primero se pronunciaron sobre el tema.

A) *Organización para la Cooperación y el Desarrollo Económico (OCDE)*

a) *Recomendaciones OCDE de 1980*. En 1980 la Organización para la Cooperación y el Desarrollo Económico (OCDE) incorporó el principio de responsabilidad en los siguientes términos:

[3] Cfr. Grupo de Trabajo de Protección de Datos (art. 29). Dictamen 3/2010 sobre el principio de responsabilidad, pág. 8.

"14. El controlador[4] de datos debería ser responsable de cumplir con medidas que den efecto a los principios establecidos anteriormente"[5]. Como se observa, esa disposición no se refiere a ninguna medida en especial para materializar la aplicación de los principios sobre tratamiento de datos sino que deja a los responsables total libertad para que adopten las herramientas que consideren adecuadas.

b) *The OECD privacy framework de 2013*. En 2013, mediante el documento titulado "The OECD privacy framework"[6] se actualizó la guía de 1980, dejando intactos los principios salvo el de responsabilidad el cual se desarrolló en los términos que mencionamos a continuación:

En primer lugar, se introdujo el concepto de los "Privacy management programmes" o "programas de gestión de privacidad", que son el mecanismo operativo por medio del cual las organizaciones implantan la protección de privacidad y de los datos personales[7].

En segundo lugar, en la parte III se introducen sugerencias para poner en práctica la responsabilidad demostrada[8] señalando que el responsable debería: (a) tener un programa de gestión de datos; b) estar en capacidad de demostrar que dicho

[4] "Controlador" equivale a "responsable" del tratamiento de datos personales.

[5] Cfr. Recomendación del Consejo relativa a las directrices que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales (23 de septiembre de 1980). El texto original se redactó en idioma inglés (*Organisation for Economic Cooperation and Development. Guidelines governing the protection of privacy and transborder flows of personal data*) y el texto del artículo dice lo siguiente: "*Accountability Principle. 14. A data controller should be accountable for complying with measures which give effect to the principles stated above*". El texto en castellano es traducción libre del autor.

[6] El texto oficial puede consultarse en la página web de la OCDE: *http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf*

[7] Cfr. OECD Privacy Guidelines (2013). En: *http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm*

[8] El texto original en idioma inglés dice lo siguiente:

"*Part three. implementing accountability.*

"*15.A data controller should:*

"*a) Have in place a privacy management programme that:*

"*i. gives effect to these Guidelines for all personal data under its control;*

"*ii. is tailored to the structure, scale, volume and sensitivity of its operations;*

"*iii. provides for appropriate safeguards based on privacy risk assessment;*

"*iv. is integrated into its governance structure and establishes internal oversight mechanisms;*

"*v. includes plans for responding to inquiries and incidents;*

"*vi. is updated in light of ongoing monitoring and periodic assessment;*

"*b) Be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible*

programa es apropiado para cumplir los principios de la OCDE, y c) notificar a las autoridades y a los titulares de los datos sobre las fallas o brechas de seguridad que afecten los datos personales.

Respecto del programa de gestión de datos, la OCDE establece que deben cumplir estos requisitos:

a) Ser vinculante u obligatorio para todas las personas que están bajo control o trabajan para el responsable del tratamiento.

b) Tener en cuenta la estructura, escala o tamaño, volumen y sensibilidad de sus operaciones o actividades.

c) Proporcionar medidas apropiadas teniendo en cuenta los riesgos asociados al tratamiento de datos personales.

d) Estar integrado a la estructura de gobierno del responsable.

e) Establecer mecanismos internos de supervisión.

f) Incluir planes de respuesta a solicitudes de los titulares de los datos o frente a incidentes (de seguridad, por ejemplo).

g) Ser objeto de actualización, monitoreo y evaluación periódica.

B) *Organización de las Naciones Unidas (ONU)*

La ONU no hace referencia al principio de responsabilidad en los términos expuestos hasta aquí. Solo se refiere a la adopción de medidas apropiadas para cumplir el principio de seguridad.

En efecto, en el documento "Principios rectores para la reglamentación de los ficheros computadorizados de datos personales", adoptado por la Asamblea General en su resolución 45/95, de 14 de diciembre de 1990, se dispone lo siguiente:

"*Principio de seguridad. Se deberían adoptar medidas apropiadas* para proteger los ficheros contra los riesgos naturales, como la pérdida accidental o la destrucción por siniestro, y contra los riesgos humanos, como el acceso sin autorización, la utilización encubierta de datos o la contaminación por virus informático" (Destacamos).

C) *Foro de Cooperación Asia Pacífico (APEC)*

En 2004 se expidió el "Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico" (APEC) o APEC Privacy Framework". En dicho documento, se hace referencia al principio de responsabilidad en los siguientes términos:

---

for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines; and

"*c) Provide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects*".

"26. Un controlador de información personal deberá ser responsable de cumplir con medidas que causen efecto al Principio estipulado arriba. Cuando la información personal vaya a ser transferida a otra persona u organización, nacional o internacional, el controlador de la información personal debe obtener consentimiento del individuo o actuar con la debida diligencia y tomar las medidas razonables para asegurar que la persona u organización receptora, protegerá la información consistentemente con estos Principios".

La redacción del principio se presenta dentro del contexto de las transferencias internacionales pero la parte primera hace mención al principio de responsabilidad en los mismos términos que lo hizo la OCDE en sus directrices de 1980, es decir sin hacer alusión específica a mecanismo alguno para cumplir el principio de responsabilidad.

D) *Red Iberoamericana de protección de datos personales (RIPD)*

a) *Documentos de autorregulación de protección de datos (2006)*

La labor de la Red Iberoamericana de Protección de Datos (en adelante RIPD) en relación con el principio de responsabilidad demostrada, inició en 2006. Entonces, se expidió un documento[9] sobre autorregulación y protección de datos personales que guarda cercana relación con la materia en la medida en que su materialización depende, en gran parte, de lo que internamente realicen las organizaciones. En otras palabras, dicho principio se engloba dentro del concepto de autorregulación y desde esa perspectiva es necesario tener presente lo que plantea la RIPD: en primer lugar, el éxito de la responsabilidad demostrada dependerá, entre otras, de la existencia de instrumentos que use el responsable para garantizar el cumplimiento de las normas sobre protección de datos: "La autorregulación sólo redundará en beneficio real de las personas en la medida que sea bien concebida, aplicada y cuente con mecanismos que garanticen su cumplimiento de manera que no se constituyan en meras declaraciones simbólicas de buenas intenciones sin que produzcan efectos concretos en la persona cuyos derechos y libertades pueden ser lesionados o amenazados por el tratamiento indebido de sus datos personales".

En segundo lugar, es crucial evaluar y medir la eficacia de las herramientas o procesos creados para materializar las normas sobre protección de datos en la gestión de las organizaciones: "Resulta imprescindible que los instrumentos de autorregulación estén acompañados de herramientas que los hagan eficaces. Dentro de estos mecanismos se sugieren los siguientes: (1) establecer medios ágiles,

[9] Cfr. Red Iberoamericana de Protección de Datos. Grupo de trabajo temporal sobre autorregulación y protección de datos personales, 5 mayo 2006. El texto puede consultarse en: *https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/RIPD-AUTORREGULACI%C3%93N-Y-PROTECCI%C3%93N-DE-DATOS-PERSONALES-BOLIVIA-2006.pdf*

efectivos y gratuitos en caso de inobservancia del código para que la persona no sólo exija el respeto de sus derechos y libertades sino que se convierta en un «fiscalizador» de la gestión del administrador de sus datos personales; (2) consagrar mecanismos de control interno y externo de verificación del cumplimiento de los códigos, y (3) prever sanciones por el incumplimiento de los códigos".

En tercer lugar, los mecanismos deben ser consistentes con lo que dicen las regulaciones y útiles para cumplir sus mandatos: "Las medidas de autorregulación deben evaluarse desde dos perspectivas concomitantes: La objetiva y la funcional. La primera apunta a determinar si el contenido de los mismos consagra un valor añadido y si es acorde con la regulación local o, en caso de inexistencia de la misma, con los principios internacionales sobre protección de datos que se han establecido en documentos emitidos por, entre otros, la ONU, la Unión Europea y la OCDE. La segunda, por su parte, busca establecer el nivel de efectividad práctica de dichas normas. Un análisis de los anteriores factores permitirá determinar el verdadero grado de contribución de los instrumentos de autorregulación a la protección de los datos personales".

En cuarto lugar, la RIPD sugiere que exista transparencia y claridad sobre las políticas de protección de datos así como mecanismos para que el titular de la información personal pueda ejercer sus derechos: "Los instrumentos de autorregulación deben establecer mediante una redacción clara y accesible la política de protección de datos que van a aplicar a los tratamientos de datos personales [...]. También deben recoger los procedimientos mediante los que se va a facilitar a los afectados el ejercicio de los derechos de acceso, rectificación, oposición y cancelación de los datos".

Finalmente, la RIPD recalca la necesidad de evaluar con cierta frecuencia la eficacia de los mecanismos diseñados para cumplir las normas sobre protección de datos personales: "Se considera oportuno que se prevean fórmulas para evaluar periódicamente la eficacia de los instrumentos de autorregulación, midiendo el grado de satisfacción de los afectados y, en su caso, actualizando el contenido para adaptarlo a la normativa general o sectorial de protección de datos existente en cada momento".

b) *Estándares de protección de datos personales para los Estados Iberoamericanos (2017)*

La RIPD aprobó en 2017 los "Estándares de protección de datos personales para los Estados Iberoamericanos", aplicables tanto al tratamiento de datos personales en el sector privado como en el público. Respecto del último, señala expresamente el citado documento que comprende a "*autoridades y organismos públicos, que*

traten datos personales en el ejercicio de sus actividades y funciones"[10]. Adicionalmente, los estándares cobijan tanto el tratamiento físico como automatizado de dicha información[11].

Respecto del principio de responsabilidad, el artículo 20, de una parte, ordena al responsable del tratamiento implantar mecanismos para demostrar el cumplimiento de lo que establecen los estándares[12] y, de otra, establece a título enunciativo los siguientes medios para cumplir el principio de responsabilidad:

"20.3. Entre los mecanismos que el responsable podrá adoptar para cumplir con el principio de responsabilidad se encuentran, de manera enunciativa más no limitativa, los siguientes:

"a. Destinar recursos para la instrumentación de programas y políticas de protección de datos personales.

"b. Implementar sistemas de administración de riesgos asociados al tratamiento de datos personales.

"c. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable.

"d. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales.

"e. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.

"f. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

"g. Establecer procedimientos para recibir y responder dudas y quejas de los titulares".

[10] En este sentido el art. 3 dice lo siguiente: "3. Ámbito de aplicación subjetivo 3.1. Los presentes estándares serán aplicables a las personas físicas o jurídicas de carácter privado, autoridades y organismos públicos, que traten datos personales en el ejercicio de sus actividades y funciones".

[11] En efecto, el num. 4.1 del art. 4 (ámbito de aplicación objetivo) dice lo siguiente: "Los presentes estándares serán aplicables al tratamiento de datos personales que obren en soportes físicos, automatizados total o parcialmente, o en ambos soportes, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización".

[12] El num. 20.1 del art. 20 establece lo siguiente:

"20. Principio de responsabilidad

"20.1. El responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en los presentes Estándares, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de control, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines".

Por último, dispone que el responsable debe efectuar revisiones y evaluaciones de los mecanismos utilizados con miras a establecer su grado de eficacia y cumplir sus deberes sobre tratamiento de datos personales[13].

c) *Medidas proactivas para mejorar el cumplimiento de las normas y fortalecer el debido tratamiento de datos personales en la organización*

La Red Iberoamericana de Protección de Datos (RIPD) propone a los Estados que reconozcan y establezcan medidas que promuevan "el mejor cumplimiento de su legislación y coadyuven a fortalecer y elevar los controles de protección de datos personales implementados por el responsable"[14]. Este tipo de medidas son consistentes con el principio de responsabilidad demostrada y se constituyen, entre otras, en buenas prácticas para asegurar el debido tratamiento de datos personales:

a') Privacidad por diseño y privacidad por defecto. Esta medida tiene un enfoque netamente preventivo porque exige a los responsables que la privacidad y la protección de datos personales sea otro "ingrediente" que deben considerar o abordar cuando emprendan proyectos que impliquen la recolección, el uso, la circulación, el acceso y demás actividades con datos personales.

Así las cosas, la privacidad desde el diseño implica que, por ejemplo, en palabras de la RIPD, el responsable aplique "desde el diseño, en la determinación de los medios del tratamiento de los datos personales, durante el mismo y antes de recabar los datos personales, medidas preventivas de diversa naturaleza que permitan aplicar de forma efectiva los principios, derechos y demás obligaciones previstas en la legislación nacional del Estado Iberoamericano que le resulte aplicable"[15].

La privacidad por defecto busca que los procesos, las tecnologías o mecanismos utilizados para tratar datos incorporen medidas que automáticamente —por defecto— minimicen la cantidad de datos que se deben tratar o el acceso a ellos y aseguren, sin la intervención humana, el cumplimiento mecánico e instantáneo de los principios y demás deberes que impone la regulación de tratamiento de datos al responsable del mismo. En ese sentido, la RIPD establece lo siguiente: "El responsable garantizará que sus programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen un tratamiento de datos personales, cumplan por defecto o se ajusten a los prin-

[13] El num. 20.4. ordena lo siguiente: "El responsable revisará y evaluará permanentemente los mecanismos que para tal afecto adopte voluntariamente para cumplir con el principio de responsabilidad, con el objeto de medir su nivel de eficacia en cuanto al cumplimiento de la legislación nacional aplicable".

[14] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 37.

[15] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 38.1.

cipios, derechos y demás obligaciones previstas en la legislación nacional del Estado Iberoamericano que le resulte aplicable. Específicamente, con el fin de que únicamente sean objeto de tratamiento el mínimo de datos personales y se limite la accesibilidad de estos, sin la intervención del titular, a un número indeterminado de personas"[16].

b') *Oficial de protección de datos* personales. Para la RIPD, si el responsable del tratamiento está en cualquiera de las siguientes situaciones, debería designar un oficial de protección de datos personales. El responsable del tratamiento (i) es una autoridad pública; (ii) lleva a cabo "de datos personales que tengan por objeto una observación habitual y sistemática de la conducta del titular"; (iii) realiza tratamientos "donde sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, considerando, entre otros factores y de manera enunciativa mas no limitativa, las categorías de datos personales tratados, en especial cuando se trate de datos sensibles; las transferencias que se efectúen, el número de titulares, el alcance del tratamiento, las tecnologías de información utilizadas o las finalidades de estos"[17].

La RIPD precisa que, en todo caso, es voluntario que el responsable si lo estima conveniente nombre un oficial de protección en casos diferentes a los mencionados[18]. Además, recalca la importancia de que el responsable respalde[19] al oficial de cumplimiento y le suministre los recursos suficientes para cumplir, entre otras, las siguientes funciones:

"a. Asesorar al responsable respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales.

"b. Coordinar, al interior de la organización del responsable, las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.

"c. Supervisar al interior de la organización del responsable el cumplimiento de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia"[20].

[16] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 38.2

[17] Los apartes entre comillas fueron tomados de Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 39.1.

[18] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 39.2.

[19] Todas las partes entre comillas fueron tomadas de: Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 39.3.

[20] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 39.4.

c') *Evaluación de impacto a la protección de datos* personales. Esta medida también es de naturaleza preventiva porque tiene como propósito obligar al responsable a realizar, en ciertos casos, estudios para detectar riesgos graves que pueden afectar los derechos de los titulares de los datos y adoptar medidas para neutralizarlos.

En efecto, la RIPD dispone que "cuando el responsable pretenda llevar a cabo un tipo de tratamiento de datos personales que, por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, realizará, de manera previa, a la implementación del mismo una evaluación del impacto a la protección de los datos personales" [21].

d') *Otras medidas* proactivas. En adición a las anteriores, la RIPD también considera los mecanismos de autorregulación[22] como herramientas proactivas. Dentro de estos cita los códigos deontológicos, los sistemas de certificación y sellos de confianza que pueden contribuir a la correcta aplicación de las normas sobre protección de datos[23]. Lo importante es que estos mecanismos sean vinculantes y útiles en la práctica y no una mera adhesión formal sin aplicación real de los mecanismos de autorregulación.

E) *Unión Europea*

En la Unión Europea el principio de responsabilidad surgió como una medida práctica, *no teórica*, que demanda adoptar herramientas específicas para garantizar el derecho a la protección de los datos. Con esto se quiere pasar de la protección teórica de las normas a la protección real y efectiva en la gestión diaria de las organizaciones, lo cual demanda la utilización de instrumentos prácticos de protección eficaz de los datos. En este sentido, en el Dictamen 3/2010 sobre el principio de responsabilidad del Grupo de trabajo de protección de datos del artículo 29

[21] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 41.1.

[22] Sobre el particular dice lo siguiente el num. 40.1 de los Estándares: "El responsable podrá adherirse, de manera voluntaria, a esquemas de autorregulación vinculante, que tengan por objeto, entre otros, contribuir a la correcta aplicación de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia y establecer procedimientos de resolución de conflictos entre el responsable y el titular sin perjuicio de otros mecanismos que establezca la legislación nacional de la materia aplicable, teniendo en cuenta las características específicas de los tratamientos de datos personales realizados, así como el efectivo ejercicio y respeto de los derechos del titular".

[23] Cfr. Red Iberomaericana de Protección de Datos (2017). Estándares de protección de datos personales para los Estados Iberoamericanos, num. 40.2.

se recalca que "La protección de datos debe progresar «de la teoría a la práctica». Los requisitos jurídicos deben traducirse en medidas concretas de protección de datos"[24].

En suma, para logar una protección práctica y suficiente del derecho a la protección de datos en Europa se considera imprescindible que los responsables apliquen "medidas reales y eficaces de protección de datos orientadas a la buena gobernanza de protección de datos y que, al tiempo, minimicen los riesgos jurídicos, económicos y de prestigio que podrían derivarse de una práctica precaria de protección de datos"[25]. Así las cosas, es crucial el diseño y ejecución de medidas y procedimientos internos que pongan en práctica los mandatos legales sobre protección de datos y garanticen la efectiva protección del citado derecho.

a) *Dictamen 3/2010 del Grupo de Trabajo de Protección de Datos (art. 29)*

El 13 de julio de 2010 el Grupo de Trabajo de Protección de Datos del artículo 29[26] (en adelante G29) adoptó el "Dictamen 3/2010 sobre el principio de responsabilidad" (en adelante dictamen 3/2010) cuyo principal objetivo fue presentar "una propuesta concreta de introducción el [*sic*] principio de responsabilidad que reclamaría de los responsables del tratamiento de datos la aplicación de medidas apropiadas y eficaces que garantizaran la observancia de los principios y obligaciones que dispone la Directiva y la demostraran cuando se lo solicitaran las autoridades de control. Ello contribuiría a que la protección de datos progresara «de la teoría a la práctica» y ayudaría a las autoridades de protección de datos en sus funciones de supervisión y ejecución"[27]. Recalca el G29 que este principio demanda la aplicación de "medidas adecuadas y eficaces para poner en práctica los principios y obligaciones de la Directiva y demostrar este extremo cuando se les solicitara. En la práctica, ello se traduciría en programas modulables tendentes

[24] Cfr. Grupo de Trabajo de Protección de Datos del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad, pág. 3, num. 1.

[25] Cfr. Grupo de Trabajo de Protección de Datos del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad, pág. 5, num. 9.

[26] El Grupo de Trabajo de Protección de Datos del artículo 29 se creó en virtud del art. 29 de la Directiva 95/46/CE. Se trata de un organismo europeo, con carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad. El G29 está integrado por un representante de la autoridad o de las autoridades de control designadas por cada Estado miembro, por un representante de la autoridad o autoridades creadas por las instituciones y organismos comunitarios, y por un representante de la Comisión. Sus funciones se describen en el art. 30 de la Directiva 95/46/CE y en el art. 15 de la Directiva 2002/58/CE.

[27] Cfr. Grupo de Trabajo de Protección de Datos del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad, pág. 2

a ejecutar los principios de protección vigentes (a veces llamados «programas de cumplimiento»)"[28].

El dictamen pone de presente que la protección práctica y real de los titulares de los datos contribuye a "minimizar los riesgos, crear y mantener una buena reputación y ganar la confianza de ciudadanos y consumidores es algo que se ha convertido en imprescindible para los responsables del tratamiento de datos de todos los sectores". Con lo anterior se justifica la necesidad de "aplicar medidas reales y eficaces de protección de datos orientadas a la buena gobernanza de protección de datos y que, al tiempo, minimicen los riesgos jurídicos, económicos y de prestigio que podrían derivarse de una práctica precaria de protección de datos"[29].

Señala el G29 que las herramientas o procesos no son las mismas para todas las organizaciones sino que dependen de varios factores como los riesgos que representen el tratamiento y la naturaleza de los datos[30]. En suma, cada organización debe adoptar medidas *particularizadas*[31] con especial énfasis en la gestión del riesgo que involucra el tratamiento de datos personales, los anáisis de riesgos, con atención especial al riesgo del tratamiento y a los tipos de datos.

Según este enfoque, los responsables del tratamiento de datos deben ser capaces de adecuar las medidas a la realidad específica del responsable del tratamiento y a las operaciones de tratamiento de datos de que se trate (pág. 14).

Lo importante es que las organizaciones adopten "medidas concretas y prácticas, convirtiendo los principios generales de protección de datos en estrategias y procedimientos concretos definidos al nivel del responsable del tratamiento de los datos en cumplimiento de las leyes y reglamentos aplicables"[32] y que el responsable garantice "la eficacia de las medidas adoptadas y demostrar, si así se le requiere, que ha adoptado dichas acciones"[33].

El G29, enuncia como ejemplos de medidas de responsabilidad demostrada las siguientes:

• "Establecimiento de procedimientos internos previos a la creación de nuevas operaciones de tratamiento de datos personales (revisión interna, evaluación, etc.);

[28] Cfr. Grupo de Trabajo de Protección de Datos del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad, pág. 4, num. 3.

[29] Cfr. Grupo de Trabajo de Protección de Datos del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad, pág. 5, nums. 8 y 9.

[30] Cfr. Grupo de Trabajo de Protección de Datos del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad, pág. 9.

[31] Cfr. Grupo de Trabajo de Protección de Datos del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad, pág. 14.

[32] Cfr. Grupo de Trabajo de Protección de Datos del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad, pág. 9.

[33] *Ibidem*.

• Establecimiento de políticas escritas y vinculantes de protección de datos que se tengan en cuenta y se valoren en nuevas operaciones de tratamiento de datos (p. ej., cumplimiento de los criterios de calidad de datos, notificación, principios de seguridad, acceso, etc.) que deben ponerse a disposición de las personas interesadas;

• Cartografía de procedimientos que garanticen la identificación correcta de todas las operaciones de tratamiento de datos y el mantenimiento de un inventario de operaciones de tratamiento de datos;

• Nombramiento de un funcionario de protección de datos y otras personas responsables de la protección de datos;

• Oferta adecuada de protección de datos y formación a los miembros del personal; esto debe incluir a los procesadores (o responsables del proceso) de datos personales (como los directores de recursos humanos) pero también a los administradores de tecnologías de la información, conceptores y directores de unidades comerciales; deben asignarse recursos suficientes para la gestión de la privacidad, etc.;

• Establecimiento de procedimientos de gestión del acceso y de las demandas de corrección y eliminación de datos con transparencia para las personas interesadas;

• Establecimiento de un mecanismo interno de tratamiento de quejas;

• Establecimiento de procedimientos internos de gestión y notificación eficaces de fallos de seguridad;

• Realización de evaluaciones de impacto sobre la privacidad en circunstancias específicas;

• Aplicación y supervisión de procedimientos de verificación que garanticen que las medidas no sean solo nominales sino que se apliquen y funcionen en la práctica (auditorías internas o externas, etc.)”[34].

Adicionalmente, se refiere a las Normas Técnicas Internacionales adoptadas en Madrid en donde se relacionan las siguientes medidas proactivas para cumplir las regulaciones de protección de datos:

“a) La aplicación de procedimientos para impedir y localizar las filtraciones, que pueden basarse en modelos tipificados de gobernanza o gestión de seguridad de la información.

”b) El nombramiento de uno o más funcionarios de protección de datos o privacidad, con cualificaciones, recursos y competencias adecuados para ejercer adecuadamente sus funciones de supervisión.

”c) La realización periódica de programas de formación, educación y sensibilización entre los miembros de la organización dirigidos a una mejor comprensión

[34] Cfr. Grupo de Trabajo de Protección de Datos del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad, págs. 12-13.

de la legislación aplicable sobre protección de la privacidad en relación al tratamiento de datos personales así como de los procedimientos establecidos al efecto por la organización.

”d) La realización periódica de auditorías transparentes por partes cualificadas y preferentemente independientes que verifiquen el cumplimiento de la legislación aplicable sobre protección de la privacidad en relación al tratamiento de datos personales así como con los procedimientos establecidos al efecto por la organización..

”e) La adaptación de los sistemas de información o de las tecnologías de tratamiento de datos personales a la legislación aplicable sobre protección de la privacidad en relación al tratamiento de datos personales, particularmente en el momento de decidir sobre sus especificaciones técnicas y sobre su desarrollo y aplicación.

”f) La aplicación de evaluaciones de impacto sobre la privacidad previas a la implantación de nuevos sistemas de información o de tecnologías de tratamiento de datos personales y previos también a la realización de cualquier nuevo método de tratamiento de datos personales o de modificaciones sustanciales en el trat”amiento existente.

”g) La adopción de códigos de prácticas de observancia vinculante que incluyan elementos que permitan medir la eficacia en cuanto afecte al cumplimiento y al nivel de protección de los datos personales y que establezcan medidas eficaces en caso de incumplimiento.

”h) La aplicación de un plan de respuesta que establezca directrices de actuación en caso de que se verifique una infracción de la legislación sobre protección de la privacidad aplicable en relación al tratamiento de datos personales, que incluya al menos la obligación de determinar la causa y gravedad de la infracción, de describir sus efectos negativos y de adoptar las medidas adecuadas para impedir infracciones ulteriores”[35].

b) *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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. Deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE)*[36]

El Reglamento general de protección de datos señala en el numeral 2 del artículo 5 que “el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)”.

[35] Cfr. Grupo de Trabajo de Protección de Datos del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad, pág 13 (nota de pie de página num 7).

[36] El texto del Reglamento puede consultarse en: *http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679*

El apartado 1 se refiere a los siguientes principios sobre el tratamiento de datos: a) licitud, lealtad y transparencia[37]; b) limitación de la finalidad[38]; c) minimización de datos[39]; d) exactitud[40]; e) limitación del plazo de conservación[41], y f) seguridad, integridad y confidencialidad[42].

En cuanto al principio de responsabilidad, el artículo 24 del reglamento ordena al responsable utilizar medidas que le permitan demostrar que el tratamiento de datos lo ha efectuado cumpliendo lo que ordena el reglamento. Esas medidas: a) pueden ser organizacionales y técnicas pero, en todo caso, apropiadas para garantizar el cumplimiento del Reglamento; b) no son uniformes para todos los tratamientos sino que dependerán de "la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas"[43]. En otras palabras, el tipo de

[37] El lit. a) del num. 1 del at. 5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo establece lo siguiente: "*Los datos personales serán:* "a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»)".

[38] El lit. b) del num. 1 del art. 5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo establece lo siguiente: "Los datos personales serán: [...] b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»)".

[39] El lit. c) del num. 1 del art. 5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo establece: "Los datos personales serán: [...] c)adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»)".

[40] El lit. d) del num. 1 del art. 5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo establece lo siguiente: "Los datos personales serán: [...] d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»)"

[41] El lit. e) del num. 1 del art. 5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo establece lo siguiente: "Los datos personales serán: [...] e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»)".

[42] El lit. f) del num. 1 del artículo 5 de Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo establece: "Los datos personales serán: [...] f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)".

[43] Cfr. num. 1 del art. 24 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

procedimientos y mecanismos depende de los riesgos que genera el tratamiento y la naturaleza de los datos; c) deben ser revisadas y actualizadas; d) pueden ser las políticas de protección de datos[44], la adhesión a códigos de conducta o a mecanismos de certificación[45].

c) *Medidas proactivas para mejorar el cumplimiento de las normas y fortalecer el debido tratamiento de datos personales en la organización*

En adición al principio de responsabilidad, el reglamento prevé tres instituciones que, en nuestra opinión, son complementarias y necesarias para implantar dicho principio en las organizaciones, a saber: (i) protección de datos desde el diseño y por defecto; (ii) evaluación de impacto relativa a la protección de datos, y (iii) delegado de protección de datos. Estos, como veremos más adelante, también fueron incorporados en la regulación colombiana mediante el decreto 1413 de 2017[46] que establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

A continuación nos referiremos a cada una:

a') *Protección de datos desde el diseño y por defecto*. La protección de datos desde el diseño[47] implica que desde antes de iniciar el tratamiento de datos, el responsable debe aplicar medidas para evitar vulneraciones a los derechos de los titulares de los datos o afectarlos lo menos posible. Se quiere que, desde el principio y durante toda la vida del tratamiento, las organizaciones tengan en cuenta los aspectos sobre la recolección, almacenamiento, usos, circulación y acceso

[44] Cfr. num. 2 del artículo 24 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo

[45] Cfr. num. 3 del artículo 24 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo

[46] Decreto 1413 del 25 de agosto de 2017, "por el cual se adiciona el Título 17 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el Capítulo IV del Título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales".

[47] Dice lo siguiente el numeral 1 del artículo 25 del Reglamento sobre la protección de datos desde el diseño:

"1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados".

a datos que pueden verse involucrados en cualquier proceso o actividad de una organización. Como se observa, se trata de una medida netamente preventiva de indebidos tratamientos de datos y no reactiva frente a vulneraciones de los derechos de los titulares o los intereses del responsable.

Lo anterior obliga a las organizaciones a pensar desde el comienzo de cualquier proyecto en los aspectos sobre tratamiento de datos para diseñar estrategias o definir métodos o herramientas para garantizar el correcto tratamiento de los datos personales. Este principio busca que las organizaciones no actúen en este campo solo cuando enfrentan incidentes o investigaciones por infracciones del régimen jurídico. Es decir, se quiere que las empresas no actúen con carácter reactivo frente a un problema, sino preventivo para que no ocurran incidentes.

Las medidas que se adopten son de diversa naturaleza —tecnológicas, administrativas, humanas, contractuales, seudonimización y minimización de datos— y dependerán de varios factores como: (i) el estado de la técnica o de mecanismos disponibles y de riesgos existentes; (ii) los costos y recursos económicos disponibles; (iii) los fines del tratamiento; (iv) la naturaleza manual o automatizada del tratamiento; (v) la naturaleza de los datos objeto de tratamiento, *privados*, *semiprivados*, *sensibles*, *públicos*; (vi) la cantidad de datos y sus titulares; (vii) la probabilidad y la gravedad del riesgo para los derechos y libertades del titular de datos y del responsable del tratamiento, los cuales deben determinarse y ponderarse objetivamente con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos.

La protección de datos por defecto[48], por su parte, se orienta a que automáticamente solo se traten datos (i) estrictamente necesarios para alcanzar los fines puntuales del tratamiento, (ii) por el tiempo necesario para alcanzar su objetivo y que el acceso a esa información sea restringido. Enfatiza el reglamento que, por defecto, los datos personales no sean accesibles ilimitada e incontroladamente.

Para garantizar la protección de datos por defecto, el Responsable debe utilizar medidas apropiadas de diferente naturaleza, teniendo en cuenta los factores pertinentes citados para el caso de la protección de datos desde el diseño.

b') *Evaluación de impacto relativa a la protección de datos personales*. Esta evaluación es de naturaleza preventiva pues pretende que cuando el tratamiento pueda generar alto riesgo a los derechos de los titulares y antes de iniciar la re-

[48] Establece lo siguiente el num. 2 del art. 25 del Reglamento sobre la protección de datos por defecto: "2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas".

colección o uso de los datos se realice un estudio para determinar o evaluar los niveles de riesgos para así adoptar medidas para mitigarlos[49]. Según el numeral 3 del artículo 35 del reglamento dicha evaluación es necesario realizarla en caso de:

"a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

"b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1[50], o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

"c) observación sistemática a gran escala de una zona de acceso público".

El numeral 7 del artículo 35 del reglamento, por su parte, establece que la evaluación debe incluir como mínimo lo siguiente:

"a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

"b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

"c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

"d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas".

c') *Delegado de protección de datos*. El delegado de protección de datos se concibe como la persona que obrará de manera independiente para asegurar que dentro de la organización funcione correctamente todo lo referente al tratamiento de datos personales. Esto no significa que sea quien realice el trabajo directamente

[49] En efecto, el num. 1 del art. 35 del reglamento dice lo siguiente: "1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares".

[50] Este apartado se refiere a datos sensibles como los siguientes: el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

sino que será quien supervisará que esa labor se cumpla dentro de la organización. En este sentido en los considerandos del citado documento se establece lo siguiente: "Al supervisar la observancia interna del presente reglamento, el responsable o el encargado del tratamiento debe contar con la ayuda de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos [...]"[51].

Según el reglamento, "el delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento"[52]. La designación de un delegado de protección de datos es obligatoria cuando el tratamiento lo realice una autoridad u organismo público y en otros casos a los que se refiere el artículo 37 del Reglamento[53].

El delegado debe ser una persona que tenga las cualidades profesionales y conocimientos especializados en Derecho y la práctica en materia de protección de datos[54] para cumplir las siguientes funciones a que se refiere el artículo 39 del Reglamento:

[51] Cfr. Considerando núm. 97 del Reglamento.

[52] Cfr. num. 2 del art. 39 del Reglamento.

[53] Sobre la designación del delegado dice lo siguiente el Reglamento: "*Artículo 37. Designación del delegado de protección de datos.*

"1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que: a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial; b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

"2. Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

"3. Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.

"4. En casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados miembros. El delegado de protección de datos podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados".

[54] Sobre el perfil del delegado de protección de datos dice lo siguiente el considerando 97 del Reglamento: "El nivel de conocimientos especializados necesario se debe determinar, en particular, en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida

"a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

"b) supervisar el cumplimiento de lo dispuesto en el presente reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

"c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

"d) cooperar con la autoridad de control;

"e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto".

Recalca el reglamento que es necesario que el responsable o encargado respalden "al delegado de protección de datos en el desempeño de las funciones [...], facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados". Adicionalmente, deben garantizar que "el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado"[55].

F) *Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (CIAPDP)*

En 2010 la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (CIAPDP) aprobó los "Estándares internacionales sobre la protección

---

para los datos personales tratados por el responsable o el encargado. Tales delegados de protección de datos, sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente".

[55] Cfr. Art. 38 del Reglamento.

de datos personales y la privacidad"[56] conocidos como la Resolución de Madrid. En ese documento se incluyó el principio de responsabilidad de esta manera:

"11. Principio de responsabilidad. La persona responsable deberá:

"a. adoptar las medidas necesarias para cumplir con los principios y obligaciones establecidos en el presente Documento y en la legislación nacional aplicable, y

"b. dotarse de aquellos mecanismos necesarios para evidenciar dicho cumplimiento, tanto ante los interesados como ante las autoridades de supervisión en el ejercicio de sus competencias, conforme a lo establecido en el apartado 23".

Como se observa, la primera parte retoma la redacción de las directrices de la OCDE de 1980, pero la segunda hace énfasis en la necesidad de demostrar ante las autoridades y los titulares de los datos que con esas medidas se cumplen las normas sobre tratamiento de datos personales.

a) *Medidas proactivas para mejorar el cumplimiento de las normas y fortalecer el debido tratamiento de datos personales en la organización*

La Resolución de Madrid también hace referencia a las medidas proactivas que "promuevan el mejor cumplimiento de la legislación que resulte aplicable en materia de protección de datos"[57]. De dichas medidas nos referiremos a tres que nos parecen pertinentes para los efectos de esta obra, sin perjuicio que mencionemos las demás porque también son relevantes para otros propósitos relacionados con el debido tratamiento de datos personales y para tener presente a la hora de redactar un programa integral de gestión de datos personales:

a') Privacidad desde el diseño y por defecto. Aunque la Resolución de Madrid no se refiere expresamente a la privacidad desde el diseño y por defecto, en los literales a) y e) del numeral 22 existen medidas que forman parte esencial del tema como lo son:

i) El "establecimiento de procedimientos destinados a prevenir y detectar infracciones, que podrán basarse en modelos estandarizados de gobierno y/o gestión de la seguridad de la información", y

ii) La "adaptación de aquellos sistemas y/o tecnologías de información destinados al tratamiento de datos de carácter personal a la legislación que resulte aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal, en particular al decidir acerca de sus especificaciones técnicas y en su desarrollo e implementación",

b') *Oficial de privacidad o de protección de datos*. La Resolución de Madrid coincide con lo previsto por la RIPD y el Reglamento Europeo en el sentido de

[56] El texto completo de los estándares puede consultarse en: *https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Res-Madrid-estandares-sobre-prot-datos.pdf*

[57] Cfr. Num. 22 de la Resolución de Madrid.

designar una persona en la organización para que se encargue de supervisar el cumplimiento de las normas sobre tratamiento de datos. En ese sentido, considera como medida proactiva "la designación, de uno o varios oficiales de privacidad o de protección de datos, con cualificación, recursos y competencias suficientes para ejercer adecuadamente sus funciones de supervisión"[58].

c') *Estudios de impacto de privacidad*. En línea con lo mencionado respecto de los Estándares de la RIPDP, la Resolución de Madrid también es partidaria de efectuar estudios de impacto de riesgos cuando quiera que el tratamiento de datos en una situación concreta pueda afectar gravemente los derechos de los titulares de los datos.

En vista de lo anterior, la Resolución de Madrid considera que es necesario "la puesta en práctica de estudios de impacto sobre la privacidad previos a la implementación de nuevos sistemas y/o tecnologías de información destinados al tratamiento de datos de carácter personal, así como a la puesta en práctica de nuevas modalidades de tratamiento de datos de carácter personal o a la realización de modificaciones sustanciales en tratamientos ya existentes"[59].

d') *Otras medidas proactivas*. Adicionalmente, la Resolución de Madrid menciona otras medidas proactivas:

(i) Realización periódica de programas de concientización, educación y formación en protección de datos personales[60].

(ii) Implementación de auditorías independientes[61].

(iii) Adhesión a acuerdos de autorregulación[62].

(iv) Implantación de planes de contingencia[63].

[58] Cfr. Lit. b) del num. 22 de la Resolución de Madrid.

[59] Cfr. Lit. f) del num. 22 de la Resolución de Madrid.

[60] Sobre el punto, el lit. c) del num. 22 de la Resolución de Madrid dice lo siguiente "La realización periódica de programas de concienciación, educación y formación entre los miembros de la organización destinados al mejor conocimiento de la legislación que resulte aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal, así como de los procedimientos establecidos por la organización a tal efecto".

[61] Sobre el particular, el lit. d) del num. 22 de la Resolución de Madrid dispone lo siguiente: "La realización periódica de auditorías transparentes por parte de sujetos cualificados y preferentemente independientes, que verifiquen el cumplimiento de la legislación que resulte aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal, así como de los procedimientos establecidos por la organización a tal efecto".

[62] Respecto de este aspecto dice lo siguiente el lit. g) del num. 22 de la Resolución de Madrid: "La adhesión a acuerdos de autorregulación cuya observancia resulte vinculante, que contengan elementos que permitan medir sus niveles de eficacia en cuanto al cumplimiento y grado de protección de los datos de carácter personal, y establezcan medidas efectivas en caso de incumplimiento".

[63] En cuanto a este asunto señala lo que sigue a continuación el lit. h) de la Resolución de Madrid: "La implementación de planes de contingencias que establezcan unas pautas de actuación

Todas estas medidas que se pongan en práctica integral e inteligentemente en la organización, contribuirán a lograr un nivel alto de protección de los derechos de los titulares de los datos personales.

G) *Organización de Estados Americanos (OEA)*

En 2015 la OEA[64] adoptó unos principios sobre tratamiento de datos personales, dentro de los cuales se encuentra el de responsabilidad, cuyo alcance es el siguiente: "*Principio diez: responsabilidad.* Los controladores de datos adoptarán e implementarán las medidas correspondientes para el cumplimiento de estos principios".

Como se observa, el texto es muy similar al propuesto por la OECD en 1980. No obstante, en la nota explicativa de dicho principio se destaca lo siguiente:

En primer lugar, manifiesta que la protección efectiva de los derechos depende, entre otras, de (i) la *implementación efectiva* de medidas por parte de los responsables o "aquellos que tienen responsabilidad directa por la recopilación, el uso, la retención y la difusión de datos personales"; y (ii) "la capacidad de quienes recopilan, procesan y retienen datos personales para tomar decisiones responsables, éticas y disciplinadas acerca de los datos y su uso durante todo el «ciclo de vida» de los datos".

En segundo lugar, precisa respecto de los programas integrales de gestión de datos personales que estos deben tener en cuenta "la índole de los datos personales en cuestión, el tamaño y la complejidad de la organización que recopila, almacena y procesa los datos, y el riesgo de violaciones".

La OEA enfatiza la gestión de riesgos señalando que la "protección de la privacidad depende de una evaluación creíble de los riesgos que el uso de datos personales podría plantear para las personas y la mitigación responsable de esos riesgos".

Finalmente, recalca dicha entidad que los responsables del tratamiento de datos deben:

• "Cerciorarse de que los empleados que manejen datos personales estén debidamente capacitados en lo que se refiere a la finalidad de la protección de los datos y los procedimientos que se emplean para protegerlos;

en caso de que se verifique un incumplimiento de la legislación que resulte aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal, y que incluya al menos la obligación de determinar la causa y alcance de la vulneración que se haya producido, de describir sus efectos negativos y de adoptar las medidas necesarias para evitar que se reproduzca en el futuro".

[64] Cfr. Organización de Estados Americanos. Informe del Comité Jurídico Interamericano. Privacidad y protección de datos personales, 86º Período ordinario de sesiones 23-27 de marzo de 2015, Rio de Janeiro, Brasil. OEA/Ser.Q CJI/doc. 474/15 rev.2 26 marzo 2015 Original: inglés.

• ”Adoptar programas efectivos de gestión de la privacidad y realizar revisiones internas con el propósito de promover la privacidad de las personas. En muchos casos, la designación de un «responsable principal de la información y la privacidad” facilitará la consecución de esta meta».

• ”Rendir cuenta del cumplimiento de estos principios”.

En suma, los aspectos más relevantes del desarrollo regulatorio del principio de responsabilidad demostrada en los documentos de las principales organizaciones internacionales se sintetizan en la siguiente gráfica:

PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA (ACCOUNTABILITY)	RIPD 2017	UE 2016	OEA 2015	OCDE 2013	CIAPDP 2009	APEC 2004	ONU 1990
¿Está incluido expresamente en el documento?	✓	✓	✓	✓	✓	✓	X
¿Menciona expresamente que es aplicable a los sectores público y privado?	✓	✓	✓	✓	✓		
¿Ordena implantar mecanismos para demostrar el cumplimiento de normas sobre TDP?	✓	✓	✓	✓			
¿Enuncia herramientas para cumplir el principio de accountability?	✓	X	X	✓	X	X	
¿Ordena destinar recursos para la instrumentación de programas y políticas de TDP?	✓						
¿Propone implantar sistemas de administración de riesgos asociados al TDP?	✓			✓			
¿Ordena elaborar políticas y programas de TDP obligatorios y exigibles dentro de la organización del responsable?	✓			✓			
¿Incluye la necesidad de realizar programas de capacitación y actualización sobre TDP?	✓						
¿Sugiere revisar periódicamente las políticas y los programas de seguridad de datos personales para determinar las modificaciones que se requieran?	✓			✓			
¿Propone establecer un sistema de supervisión y vigilancia interna o externa, incluso auditorías, para comprobar el cumplimiento de las políticas sobre TDP?	✓						
¿Sugiere establecer procedimientos para recibir y responder dudas y quejas de los titulares?	✓			✓			
¿Ordena que se revisen y evalúen permanentemente los mecanismos incorporados para cumplir con el principio de accountability?	✓						

Tabla núm. 1. Del principio de responsabilidad sobre tratamiento de datos personales incorporados en los principales documentos internacionales.

Fuente: elaboración de Nelson Remolina Angarita©

TDP: tratamiento de datos personales.

2. Prácticas sobre "accountability" en Argentina, España, México, Perú y Uruguay

El principio de *accountability* o responsabilidad demostrada demanda que el responsable del tratamiento de datos personales o un encargado implanten los mecanismos necesarios para garantizar el cumplimiento de los principios y obligaciones encontradas en la respectiva ley de protección de datos[65]. Asimismo, el responsable debe rendir cuentas al titular de los datos y a la autoridad de control.

En los Estándares Iberoamericanos sobre Protección de Datos, por ejemplo, el artículo 20.3 consagra una lista de mecanismos que pueden utilizar los responsables para cumplir el principio de responsabilidad, entre los cuales se encuentran los siguientes: destinar recursos para la instrumentación de programas y políticas de protección de datos personales; implantar sistemas de administración de riesgos; elaborar programas y políticas de protección de datos obligatorios y exigibles; poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones; revisar periódicamente las políticas y programas de seguridad de datos personales; establecer un sistema de supervisión y vigilancia interna y externa para comprobar que las diferentes entidades cumplan con las políticas de protección de datos personales, y establecer procedimientos para recibir y responder las dudas de los titulares de los datos[66].

Los Estándares Iberoamericanos mencionados anteriormente, son directrices orientadoras para la emisión de regulación en los distintos Estados latinoamericanos. Como tales, son un referente muy importante aunque no son jurídicamente vinculantes.

Visto lo anterior, el presente acápite lo dividiremos en dos secciones, a saber: la primera se centrará en un análisis de los documentos emitidos por las autoridades de protección de datos de Argentina, Europa —concretamente España—, México, Perú y Uruguay, para establecer los asuntos que sobre *accountability* incluyen en sus regulaciones y cómo podrían ser considerados como buenas prácticas. En la segunda sección se hará un análisis de las guías de buenas prácticas en materia de *accountability* de Australia, Canadá, Colombia y Hong Kong. Adicionalmente, nos referiremos a las guías que conciernen directamente al sector público, y de existir, que traten explícitamente la protección de datos para las funciones electorales y registrales.

[65] Red Iberoamericana de Protección de Datos. "Estándares de Protección de Datos Personales para los estados Iberoamericanos", art. 20.1. Web 17 marzo. <*http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logo_RIPD.pdf*>

[66] Red Iberoamericana de Protección de Datos. "Estándares de Protección de Datos Personales para los estados Iberoamericanos", art. 20.3 Web 17 marzo.

A) *República Argentina*

La Disposición 7 de 2008 expedida por la Dirección Nacional de Protección de Datos aprueba la "Guía de Buenas Prácticas en Políticas de Privacidad para las Bases de Datos del Ámbito Público"[67], en la cual se establecen pautas de conducta sobre la protección de datos personales y particularmente en lo relacionado con la confidencialidad. Aquellas entidades públicas que adopten la Guía y se adhieran a sus términos y principios y estén además inscritas en el Registro Nacional de Bases de Datos pueden solicitar a la Dirección Nacional de Protección de Datos Personales, hoy Agencia de Acceso a la Información Pública, que se les identifique con un isologotipo que pueden utilizar en su página web, denominado "Sello Argentino de Privacidad"[68].

El objeto de la Guía es lograr optimizar los procesos de tratamiento de datos personales en las bases de datos públicos. Para ello, la Guía busca impulsar un conjunto de acciones que modifiquen hábitos para así encaminarse hacia prácticas acordes con la protección de datos personales[69]. Adicionalmente, mediante la Guía se pretende que los funcionarios públicos asuman la cultura de protección de datos personales como un elemento importante en el desempeño de sus funciones.

a') *Principios*. La Guía contiene los principios que rigen la protección de datos personales, a saber:

• Calidad. De conformidad con la citada Disposición, el principio de calidad va mucho más allá de garantizar que los datos sea exactos y que puedan actualizarse. En efecto, el principio de calidad también demanda que (i) los datos sean "adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para la que fueron recogidos"; (ii) "la recolección no pueda hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la ley"; (iii) "no puedan utilizarse los datos para finalidades distintas o incompatibles con las que motivaron su obtención"; (iv) "se almacenen de modo que el titular pueda ejercer el

[67] La Disposición 7/2008, "Guía de Buenas Prácticas en Políticas de Privacidad para las Bases de Datos del Ambito Público" y el texto modelo de "Convenio de Confidencialidad" puede consultarse en: *https://www.argentina.gob.ar/sites/default/files/disp_2008_07.pdf* o *https://www.argentina.gob.ar/aaip/datospersonales/normativa/disposiciones/gu%C3%ADasdebuenaspracticas* . En este último sitio también puede leerse otro texto sobre buenas prácticas: *Disposición 18/2015*: Guía de buenas prácticas en privacidad para el desarrollo de aplicaciones.

[68] Ministerio de Justicia y Derechos Humanos, Presidencia de la Nación. "Información Legislativa". Web Marzo 18. <*http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/143831/norma.htm*>

[69] República Argentina. Dirección Nacional de Protección de Datos Personales. Guía de Buenas Prácticas en Políticas de Privacidad para las Bases de Datos del Ámbito Público, Buenos Aires, 22/8/2008. Introducción.

derecho de acceso"; (v) "sean destruidos cuando hayan dejado de ser necesarios o pertinentes para los fines para los cuales fueron recolectados"[70].

• No automaticidad. Se refiere a que las entidades públicas no pueden "adoptar decisiones judiciales o actos administrativos que tengan como «único» fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado"[71].

• Datos sensibles. Establece la Disposición que los datos sensibles, de una parte, "solo pueden tratarse cuando medien razones de interés general autorizadas por ley o con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares" y, de otra parte, que "ninguna persona pueda ser obligada a proporcionar" este tipo de datos[72].

• Consentimiento. Señala la Disposición que por regla general las entidades públicas no requieren del consentimiento del titular del dato para tratar datos personales, siempre y cuando el tratamiento tenga como objeto el cumplimiento de las funciones legales de la entidad. Por lo tanto, el consentimiento sería excepcionalmente necesario cuando "el tratamiento de datos pretendido exceda las atribuciones específicas del órgano administrativo" [73].

De ser necesario el consentimiento, este debe "ser libre, expreso e informado y deberá realizarse por escrito o por otro medio que se le equipare"[74].

• Publicidad. La Disposición ordena que se debe comunicar al titular el derecho que tiene de solicitar el retiro o bloqueo de sus datos de la base de datos de

[70] República Argentina. Dirección Nacional de Protección de Datos Personales. Disposición 7/2008, "Guía de Buenas Prácticas en Políticas de Privacidad para las Bases de Datos del Ámbito Público" y el texto modelo de "Convenio de Confidencialidad", disponible en: *https://www.argentina.gob.ar/sites/default/files/disp_2008_07.pdf*

[71] *Ibidem.*

[72] *Ibidem.*

[73] *Ibidem.*

[74] Precisa la Disposición que "Dicho consentimiento puede ser revocado en cualquier momento, sin efectos retroactivos. Si el interesado revoca el consentimiento, el tratamiento de sus datos personales que se haga de allí en más será ilícito, por lo tanto la validez de la revocación debe considerarse al momento en que el organismo toma conocimiento de la misma y, si bien la ley 25.326 consagra expresamente la gratuidad para el ejercicio de los derechos de rectificación, actualización y supresión, la revocación del consentimiento no podría de ninguna manera estar prohibida, en tanto la facultad del consentimiento forma parte del ejercicio de un derecho humano fundamental de orden público, eje sobre el que se desarrolla la licitud del tratamiento de datos personales. En caso de que los datos personales correspondientes a la persona que revoca el consentimiento hubiesen sido cedidos a un tercero, deberá notificarse tal circunstancia al cesionario, atento que tanto este como el cedente responden solidaria y conjuntamente por la observancia de las normas de protección de datos personales ante el órgano de control y el titular de los datos".

la entidad pública y en caso de que el titular lo solicite, suministrar los datos de contacto de quien suministró a la entidad la información[75].

• Casos de no aplicabilidad de la ley de protección de datos personales. Con este principio se excluyen los casos en que no es aplicable ley argentina de protección de datos[76].

b') *Tratamientos básicos regulados*. La Guía establece que el titular de los datos tiene derecho a estar informado de manera clara y expresa acerca de los usos que le serán dados a sus datos personales. Para el efecto, se debe informar sobre la existencia del archivo o base de datos, el nombre del responsable de los datos y su domicilio, al igual que la finalidad de dichas bases de datos y sus destinatarios.

Cuando se trata de circulación o transferencia de datos personales entre las distintas dependencias de la administración pública, la Guía aclara que está permitida la cesión en forma directa y sin el consentimiento del titular de los datos, siempre y cuando sea necesario para el cumplimiento de sus respectivas competencias[77]. Por otro lado, también regula la cesión de datos personales del sector público al sector privado. Para ello, se establece que la cesión masiva de datos personales de los registros públicos solo puede ser autorizada por la ley o por la decisión del funcionario responsable de la base de datos cuando se trate de datos de acceso público y garantizando el respeto a los principios establecidos en la ley 25.326 y que con la cesión no se ocasionan perjuicios a sus titulares[78]. Sin embargo, se hace la aclaración de que no se pueden ceder los datos sensibles a no ser que haya razones de interés general, que tengan fundamento en la ley.

Adicionalmente, la Guía establece que las entidades pueden realizar transferencias internacionales de datos personales cuando se garanticen los niveles de protección en los siguientes supuestos:

[75] Dice lo siguiente la Disposición sobre el principio de publicidad: "En toda comunicación con fines de publicidad que se realice por correo, teléfono, correo electrónico, Internet u otro medio a distancia a conocer, se deberá indicar, en forma expresa y destacada, la posibilidad del titular del dato de solicitar el retiro o bloqueo, total o parcial, de sus datos personales incluidos en la base de datos. A pedido del interesado, se deberá informar el nombre del responsable o usuario del banco de datos que proveyó dicha información".

[76] Señala la Disposición respecto de dicho principio: "La ley No 25.326 no se aplica a las encuestas de opinión, mediciones y estadísticas relevadas conforme a ley 17.622, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable. Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna".

[77] Dirección Nacional de Protección de Datos Personales. Guía de Buenas Prácticas en Políticas de Privacidad para las Bases de Datos del Ámbito Público, Buenos Aires, 22/8/2008.

[78] *Ibidem*.

(i) Cuando el titular preste su consentimiento expreso o se esté ante una colaboración judicial internacional.

(ii) Cuando se esté ante el intercambio de datos de carácter médico o una investigación epidemiológica, previa disociación de los datos, siempre y cuando no se pueda identificar al titular.

(iii) Cuando se trate de transferencias bancarias o bursátiles

(iv) Cuando la transferencia de datos se acuerde en el marco de tratados internacionales en los que Argentina sea Estado parte.

(v) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia en la lucha contra el crimen organizado, el terrorismo y el narcotráfico. Vale hacer la salvedad de que no es necesario el consentimiento del titular del dato cuando la transferencia internacional se realiza desde un registro público que está legalmente constituido para facilitar información al público y que tiene consulta abierta al público en general o a cualquier persona que pueda demostrar un interés legítimo[79].

c') *Obligaciones del responsable del banco de datos.* La Guía enlista una serie de obligaciones que deben cumplir los funcionarios que tengan la titularidad de las bases de datos públicas. Por un lado, tienen la obligación de inscribir los datos de manera lícita y para ello deben estar inscritos en el Registro Nacional de Bases de Datos[80]. De otro, deben garantizar la seguridad de los datos para así garantizar la confidencialidad, íntimamente ligada con el deber de secreto que también tiene el responsable de la base de datos y cualquier persona que efectúe tratamiento de datos personales[81]. Cabe resaltar que esta obligación se mantiene incluso cuando la relación que permitió el acceso a dicho banco de datos ha finalizado. El obligado por el secreto profesional o normas de confidencialidad únicamente puede ser relevado de esa obligación mediante resolución judicial y cuando estén de por medio razones de seguridad, salud pública, y defensa nacional. Finalmente, el titular de la base de datos tiene un deber de respuesta consistente en contestar las solicitudes que se le dirija con independencia de que datos personales del afectado figuren o no.

d') *Derechos de las personas*. Dentro de la Guía, se establecen los derechos de los titulares de los datos que se encuentran en las diferentes bases de datos inscritas en el Registro. En primer lugar, está el derecho de acceso entendido como el derecho que tiene el titular de conocer la totalidad de su información existente en determinada base de datos[82]. Para ello, debe formular un reclamo directa-

[79] *Ibidem.*

[80] *Ibidem.*

[81] *Ibidem.*

[82] *Ibidem.*

mente ante el responsable del archivo o base de datos, quien debe proporcionar la información dentro de los diez días siguientes. De incumplir esta obligación, el interesado podrá promover la acción judicial de *habeas data*, y además podrá denunciar el hecho ante la Autoridad Nacional de Protección de Datos Personales.

A pesar de lo anterior, el derecho de acceso puede ser denegado si está de por medio la protección de la defensa de la Nación, el orden y la seguridad pública, al igual que los derechos e intereses de terceros. También se restringe el derecho de acceso a la información cuando su ejercicio pudiera obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias[83].

Asimismo, la Guía contiene los derechos de rectificación, actualización y supresión de datos los cuales se ejercen a solicitud del titular. Muy de la mano de lo anterior, la Guía también explica que se debe respetar el derecho de consulta del Registro Nacional de Bases de Datos, el cual se realiza de forma gratuita y su finalidad es que el titular conozca la existencia de archivos, registros o bases de datos, sus finalidades, y la identidad de los responsables del tratamiento. Este derecho no debe confundirse con el de acceso a la información, pues si bien lo facilita al informar al titular de la información encontrada en bases de datos, no es lo mismo.

e') *Temas especialmente relacionados con el Estado Nacional*. En la Guía, el Capítulo III trata temas relacionados con el Estado Nacional y para ello hace una exposición de lo consagrado en el decreto 1172 de 2003, mediante el cual se aprueba el Reglamento General de Acceso a la Información Pública para el Poder Ejecutivo Nacional.

f') *Sanciones*. En el ámbito público, los titulares de los bancos de datos no solo deben cumplir con las obligaciones establecidas en la ley y replicadas en la Guía, sino que están obligados a cumplir las normas que rigen la prestación del servicio público. En el ámbito del deber de secreto, la Guía resume las sanciones en disciplinarias, administrativas y penales, y prevé como agravante que el autor de la conducta punible sea funcionario público.

B) *Europa*

a) *Documentos sobre accountability*. En este punto debemos hacer referencia a los siguientes:

i) *Grupo de Trabajo del artículo 29*. El Grupo de Trabajo del artículo 29 (G29) recientemente ha publicado dos documentos relacionados con el nuevo Reglamento de Protección de Datos que bien vale la pena mencionar, cuando se trata de mejoras prácticas en materia de *accountability*.

[83] *Ibidem*.

El primer documento ("*Guidelines on transparency under Regulation 2016/679 17/EN WP260*)[84], trata el principio de transparencia, vinculándolo al de responsabilidad demostrada, mientras que el segundo texto ("*Guidelines on Personal data breach notification under Regulation 2016/679*)[85] se refiere a las notificaciones de brechas de seguridad en la protección de datos personales.

A continuación nos referiremos a ellos con una visión orientada a los aspectos pertinentes o conexos con el principio de responsabilidad demostrada.

• *Lineamientos en materia de transparencia*. El G29 hace énfasis en que el principio de transparencia está directamente relacionado con el de *accountability* debido a que obliga a los responsables a tener procedimientos para recolectar el consentimiento informado de los titulares e informar sobre sus derechos y las acciones que pueden tomar para hacerlos valer[86].

De igual manera, íntimamente relacionado con la transparencia, se encuentra el deber de tener reportes y registros de todo el tratamiento de datos. Para poder cumplir con el principio de responsabilidad demostrada, se propone que el registro contenga lo siguiente: 1) la petición a los titulares para tratar sus datos, 2) los métodos utilizados para verificar la identidad del titular y 3) la garantía de que el consentimiento y la información fue proveída por el titular y no por un impostor[87].

El Grupo de Trabajo afirma que aplicar el principio de *accountability* al de transparencia implica ser claro no solo en punto al proceso de recolección de datos, sino también en todo el ciclo en el que se utilizarán dichos datos. Para ello, se deben idear protocolos sobre cómo actualizar y cambiar la información de un titular. Asimismo, la entidad debe tener maneras de comunicar a los titulares de datos cualquier cambio en la política de protección y tratamiento de datos que determine realizar. Además, se requiere que todos los protocolos y políticas estén redactados en términos claros y concisos y que sean accesibles con el fin que cualquier persona que no tenga conocimiento en materia de tratamiento de datos personales pueda comprenderlas[88].

Lo anterior, a grandes rasgos, resume las mejores prácticas en materia de *accountability* que deberían tener en cuenta los responsables del tratamiento de datos personales.

[84] El texto oficial de los "Guidelines on transparency under Regulation 2016/679 17/EN WP260" puede consultarse en: *<http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227>*

[85] El texto oficial de los "Guidelines on Personal data breach notification under Regulation 2016/679" puede consultarse en: *<http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>*

[86] Article 29 Data Protection Working Party "Guidelines on transparency under Regulation 2016/679 17/EN WP260. Web 11 abril.

[87] *Ibidem*.

[88] *Ibidem*.

• *Guía de notificación de brechas de seguridad conforme al Reglamento*. En la Guía se establece como regla general que el responsable de la protección de datos debe reportar todas las brechas de seguridad, independientemente de que por regulación deba ser reportada o no. Esta obligación está directamente relacionada con el principio de responsabilidad demostrada, toda vez que el reporte de las brechas que no requieren notificación y las que sí lo requieren, facilita el cumplimiento de las obligaciones del responsable del tratamiento de los datos[89].

Si bien se hace la salvedad de que el responsable puede determinar qué método utilizar para mantener un reporte de todas las brechas, hay ciertos detalles y elementos claves que deben incluirse para asegurar que se cumple con el principio de *accountability*. Propone el G29 que se incluyan las causas de la brecha, qué sucedió y qué datos personales fueron afectados. Adicionalmente, se espera que el responsable incluya los efectos o consecuencias que tuvo la brecha, y la acción que se tomó para remediar la situación[90], con el fin de establecer protocolos aplicables cuando se enfrente una brecha similar. Es de suma importancia en este punto que el responsable pueda justificar las acciones tomadas y por qué estas no implicaban mayor riesgo para los derechos y libertades de los individuos afectados por la brecha, es decir, el porqué eran las acciones idóneas.

Por otra parte, el G29 establece que conforme al principio de responsabilidad demostrada es importante contar con un Oficial de Protección de Datos en pro de las buenas prácticas, con el fin de que en materia de brechas de seguridad, específicamente, pueda emitir un concepto a la entidad sobre las políticas de seguridad, qué hacer para dirimir los riesgos en esta materia, y cooperar con la autoridad regulatoria en adelantar todos los procedimientos necesarios para prestar la asistencia requerida a los titulares que resulten afectados. Los lineamientos hacen énfasis en que el oficial debe asistir en la prevención de las brechas de seguridad a la vez que debe monitorear el cumplimiento de la ley y las guías de gestión de privacidad dentro de la entidad[91].

ii) *Reino de España*, La Agencia Española de Protección de Datos (AEDP) publicó un artículo con el título de "El enfoque de riesgos en el Reglamento de Protección de Datos" en el cual se habla de la implantación de una política de riesgos como parte del principio de responsabilidad proactiva. Además, la AEPD emitió en 2014 la "Guía para una evaluación de impacto en la Protección de Datos Personales". Ambos documentos se examinarán en esta sección para sustraer conclusiones con respecto al principio de responsabilidad.

[89] Article 29 Working Party "Guidelines on Personal data breach notification under Regulation 2016/679 Adopted on 3 october 2017 and last revised and adopted on 6 february 2018. Web 11 abril.

[90] *Ibidem*.

[91] *Ibidem*.

a') *El enfoque de riesgos en el Reglamento de Protección de Datos*. Según la Agencia Española de Protección de Datos, el enfoque de riesgos en materia de protección de datos tiene dos vertientes: la primera está relacionada con las medidas de seguridad técnicas y organizacionales para proteger la información, y la segunda con el riesgo que corren los derechos y libertades de los titulares en el tratamiento de sus datos. Cuando la AEPD trata el tema de riesgos, el contexto en el que lo aborda tiene que ver directamente con las medidas de seguridad de la información que el responsable debe adoptar con el fin de proteger el activo (los datos). Para ello, la Agencia ha identificado un ciclo de mejora continua y unas fases de riesgo.

El ciclo de mejora continua tiene cuatro etapas, que se expondrán a continuación:

• Etapa 1. Corresponde al diseño del marco de trabajo, en la que se debe realizar un análisis de riesgos a los que pueden estar expuestos los datos que trate la entidad.

• Etapa 2. Teniendo en cuenta los riesgos identificados y el contexto específico de cada entidad, se adoptarán las medidas organizativas que se requieran para tratar los riesgos[92].

• Etapa 3. Se refiere a la gestión que se hará de los riesgos conforme a los objetivos que fueron planteados en la fase anterior. Lo que se hace es "abordar de forma objetiva y repetible el posible desfase entre los objetivos iniciales y los resultados obtenidos"[93]. En otras palabras, el responsable debe ver si en términos de análisis de riesgo, el riesgo residual es aceptable o si se debe mejorar según los objetivos planteados.

• Etapa 4. Mejorar el diseño del marco de trabajo teniendo en cuenta los resultados obtenidos en la etapa 3.

El ciclo anterior se conoce como PDCA (por sus siglas en inglés Plan, Do, Check, Act —Planificar, Hacer, Verificar, Actuar—)[94]. Dicho ciclo debería ser ejecutado por todos los responsables de tratamiento de datos personales con el fin de prever riesgos con respecto al tratamiento de datos y mejorar sus respuestas a los mismos, cumpliendo así con el principio de responsabilidad.

Por otra parte, para implantar una política de riesgos, la Agencia ha identificado varias fases, a saber:

• Fase 1. Comunicación. En ella la entidad debe identificar riesgos y probabilidades que se puedan materializar con el fin de poder establecer prioridades y

[92] Agencia Española de Protección de Datos. "El enfoque de riesgos en el Reglamento de Protección de Datos" Web. 1 abril. <*https://www.agpd.es/blog/el-enfoque-de-riesgos-en-el-reglamento-general-de-proteccion-de-datos-ides-idPhp.php*>

[93] *Ibidem*.

[94] *Ibidem*.

objetivos mientras se inculca una formación en materia de protección de datos a los encargados del tratamiento[95].

• Fase 2. Contexto. En ella se define el marco dentro del cual se desarrollará la política de análisis de riesgos[96]. Para esto, la entidad debe tener en cuenta las normas aplicables al tratamiento de datos y cuáles riesgos son aceptables.

• Fase 3. Identificación de riesgos. Su propósito es elaborar un mapa de riesgos y se deben cuantificar los posibles daños[97].

• Fase 4. Análisis y evaluación del riesgo. Se deben utilizar escalas cuantitativas y cualitativas en las que se establecerán valores objetivos para cada riesgo identificado[98].

• Fase 5. Gestión de riesgo. Durante la misma se determinan las salvaguardas que se le aplicarán a cada riesgo, teniendo en cuenta la relación costo-beneficio en cada caso[99].

• Fase 6. Seguimiento del riesgo. A lo largo de la misma se realizan auditorías e informes. Es usualmente en esta fase en donde se modifican los riesgos y las salvaguardas correspondientes[100].

Para la AEPD, el análisis de riesgos es muy importante debido a que este forma parte del principio de responsabilidad proactiva. En el Reglamento, este principio obliga a los responsables del tratamiento a demostrar la licitud de los tratamientos y adecúa cada tratamiento a circunstancias específicas para así elaborar un mapa de riesgos y salvaguardas adecuado.

b) *La Guía para una evaluación de impacto en la protección de datos personales*. Como se vio en el documento anterior, para la AEPD el análisis y la gestión de riesgos está directamente asociado con el principio de responsabilidad. Por esto, en la guía se establecen unas fases para evaluar el impacto en la protección de datos[101].

En una primera fase, se debe analizar la necesidad de llevar a cabo o no una evaluación de impacto en materia de protección de datos. En caso afirmativo, el segundo paso sería analizar las categorías de datos, los usuarios, flujos de infor-

[95] *Ibidem*.

[96] *Ibidem*.

[97] *Ibidem*.

[98] *Ibidem*.

[99] *Ibidem*.

[100] *Ibidem*.

[101] Debe entenderse "impacto" como riesgo en los términos de la Agencia Española de Protección de Datos.

mación y tecnologías utilizadas[102]. En tercer lugar, la entidad debería identificar los riesgos para la protección de datos, esto incluye una valoración de la probabilidad de que sucedan y el daño que causarían en caso de materializarse. Una vez se identifican los riesgos, el cuarto paso es determinar qué medidas se deben adoptar para eliminar, mitigar, transferir o aceptar los riesgos que fueron detectados[103]. Con esto, el quinto paso es verificar si los controles y medidas cumplen los requisitos legales en materia de protección de datos, para así proceder al sexto paso que es la realización de un informe de riesgos y recomendaciones de cómo eliminarlos y mitigarlos[104].

Una vez se realiza el informe, el séptimo paso es asignar los recursos necesarios para ejecutar las propuestas y recomendaciones y determinar quién será responsable de su ejecución. Por último, las entidades públicas responsables del tratamiento de datos, deben comprobar la efectividad de sus herramientas para mitigar el riesgo y verificar si hay nuevos riesgos que hayan pasado desapercibidos[105]. Todas estas fases ayudan a que una entidad pueda poner en práctica herramientas para mitigar los riesgos relacionados con el tratamiento de información y así poder llevar a cabo las obligaciones relacionadas con el cumplimiento del principio de responsabilidad.

C) *Estados Unidos Mexicanos*

En México no existe una guía de buenas prácticas en materia de *accountability* ni una guía de buenas prácticas en protección de datos en general[106]. Por ello, esta sección dará cuenta de lo que se ha encontrado en dos documentos. Por una parte, en el "Estudio para la elaboración de una guía con la metodología y procesos de gestión para el cumplimiento de las obligaciones en materia de protección de datos personales"[107] realizado por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). La guía metodológica realizada por el INAI pretende dar respuesta a tres preguntas: (1) ¿qué obligaciones tengo que cumplir como responsable/encargado del tratamiento?; (2) ¿cómo puedo cumplir las obligaciones que tengo?, y (3) ¿cómo sé si cumplo o no?[108]. Por otra

[102] Agencia Española de Protección de Datos. "Guía para una evaluación de impacto en la Protección de Datos Personales" Web. 8 abril <*http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf*>

[103] *Ibidem*.

[104] *Ibidem*.

[105] *Ibidem*.

[106] Tal es la situación a 2 de mayo de 2018. Es factible que posteriormente se emitan guías sobre el tema.

[107] *Ibidem*.

[108] *Ibidem*.

parte, México también cuenta con un documento titulado: "Principios y deberes en materia de Protección de Datos Personales".

A continuación nos referiremos a los citados instrumentos.

a) *Estudio para la elaboración de una guía con la metodología y procesos de gestión para el cumplimiento de las obligaciones en materia de protección de datos personales*. Esta guía metodológica busca ser un instrumento útil para que los responsables o encargados del tratamiento de datos personales puedan autoevaluar su nivel de cumplimiento de la normativa sobre protección de datos personales.

Para el tratamiento de datos personales de manera lícita y leal, los responsables no solo deben cumplir los principios y deberes establecidos en la ley sino respetar los derechos de los titulares. Para ello, la guía lista los siguientes principios: responsabilidad, licitud y lealtad, información, consentimiento, finalidad, calidad y proporcionalidad[109]. Asimismo, expone dos deberes, a saber: (i) implantar las medidas de seguridad suficientes para proteger los datos y (ii) mantener la confidencialidad de dicha información. Por último, explica que en todo momento los titulares de los datos cuentan con los Derechos ARCO —*Acceso, Rectificación, Cancelación y Oposición*—. Pone de presente la guía que en todas las fases del tratamiento de datos personales hay lugar a revocar el consentimiento.

La guía propuesta por el INAI, pretende ser de fácil comprensión y aplicación en la práctica para que los responsables del tratamiento de datos no requieran tener conocimientos jurídicos y tecnológicos previos y aun así puedan cumplir con las disposiciones legales en materia de tratamiento de datos personales. Además, la Guía procura concientizar y desarrollar una cultura de protección de datos personales en México[110].

b) *Principios y deberes en materia de protección de datos personales*. Este documento, también desarrollado por el INAI, define el principio de responsabilidad como "*las medidas que pudieran adoptarse o preverse para garantizar la observancia en materia de protección de datos*"[111]. Luego determina su importancia basándose en que varios principios de protección de datos personales dependen del principio de responsabilidad. Por ello, se requiere que los responsables actúen en calidad de "buen custodio" de aquellos datos que les han sido confiados[112].

Más allá de lo anterior, el documento hace hincapié en que la protección de la privacidad, y el buen cumplimiento del principio de responsabilidad, depende

[109] *Ibidem*.

[110] *Ibidem*.

[111] INAI. "Principios y deberes en materia de protección de Datos Personales". Web. 6 Abril. <*http://metabase.uaem.mx/bitstream/handle/123456789/2525/3%20Principios%20y%20deberes%20en%20materia%20de%20Protección%20de%20Datos%20Personales.pdf?sequence=1*>

[112] *Ibidem*.

ampliamente de la realización de una evaluación creíble de los riesgos a que dichos datos se encuentran sometidos para que el responsable pueda así mitigarlos y establecer procedimientos y protocolos para evitar vulnerar los derechos de los titulares.

El INAI declara que la Ley de Protección de Datos Personales de México indica que el principio de *accountability* "debe entenderse en el sentido de que corresponderá a la entidad o persona responsable el deber de velar por el cumplimiento de los principios y rendir cuentas al titular en caso de incumplimiento"[113]. Siendo así que dicho principio se vuelve la verdadera garantía que tiene el titular de los datos al depositar su confianza en el responsable, porque sabe que este debe tomar todas las previsiones necesarias con el fin de que los datos puedan ser tratados conforme a la voluntad del titular y según las medidas de seguridad proveídas.

Finalmente, el documento contiene medidas para que se cumpla el principio de *accountability*. Para ello, lista las encontradas en el artículo 48 de la Ley Federal de Protección de Datos en Posesión de Particulares, a saber:

"1. Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización del responsable;

"2. Poner en práctica un programa de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales;

"3. Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad;

"4. Destinar recursos para la instrumentación de los programas y políticas de privacidad;

"5. Instrumentar un procedimiento de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos;

"6. Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran;

"7. Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales;

"8. Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento;

"9. Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permiten garantizar al responsable el cumplimiento de los principios y obligaciones que establece la ley y el presente reglamento, o

[113] *Ibidem*.

”10. Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a [*sic*] los datos personales durante su tratamiento”[114]

D) *Perú*

La autoridad peruana de protección de datos, elaboró una Directiva de Seguridad, en la cual existe un capítulo sobre el principio responsabilidad.

En la Directiva se establece que el responsable del banco de datos, debe otorgar y mantener un nivel suficiente de protección de dicha información y también debe determinar qué finalidad tienen dichos datos y asegurarse de que no sean utilizados con un propósito diferente[115]. Adicionalmente, debe garantizar el cumplimiento de los derechos del titular que son los consagrados en la ley 29.733.

La Directiva procede a listar medidas de seguridad para el tratamiento de datos personales. Aclara que las medidas de seguridad dependerán de la categoría a la que pertenezca la entidad, por lo que es importante estudiar las diferentes categorías. Se entiende que la categoría básica es la de menor nivel, por lo que los bancos de datos no contienen información de más de cincuenta personas y el número de datos personales no es mayor a cinco, por lo cual además no incluye datos sensibles y los titulares son personas naturales[116].

La segunda categoría es la simple, que contiene información de no más de cien personas, y como la anterior no incluye datos sensibles, y el tiempo del tratamiento es inferior a un año[117]. A diferencia de la anterior, el titular puede ser una persona natural o una persona jurídica.

La tercera categoría de la clasificación es la intermedia. En esta se encuentran los bancos de datos personales que contienen información de hasta mil personas, su tratamiento puede ser por un tiempo indeterminado o superior a un año. A diferencia de las anteriores puede incluir datos sensibles[118] y tiene como titular a una persona natural o jurídica.

La cuarta categoría es la compleja y en ella se encuentran los bancos de datos personales cuyo tratamiento se cumple en un período indeterminado o superior a

[114] *Ibidem*.

[115] Ministerio de Justicia y Derechos Humanos. “Directiva de Seguridad de la Autoridad Nacional de Protección de Datos Personales”. Web 8 abril. <*https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-de-Directiva-de-Seguridad.pdf*>

[116] Ministerio de Justicia y Derechos Humanos. “Directiva de Seguridad de la Autoridad Nacional de Protección de Datos Personales”. Web 8 abril. Capítulo VI Medidas de Seguridad, Sección 1.1.1. (a)

[117] *Ibidem*, Sección 1.1.1 (b)

[118] *Ibidem*, Sección 1.1.1 (c)

un año y cuyo tratamiento se realiza en múltiples oficinas o dependencias, por lo que además incluye datos sensibles. Esta categoría es la que nos interesa, toda vez que tiene como titular a una persona jurídica o entidad pública[119].

Finalmente, se encuentra la categoría crítica que evidentemente es la de mayor nivel debido a que incluye bancos de datos personales cuya finalidad está respaldada por la ley, y cuyo plazo es indeterminado o superior a un año. Adicionalmente, sirve para tratar datos personales en múltiples oficinas o dependencias, por lo que además incluye datos sensibles[120].

La razón por la cual se clasifican las bases de datos en diferentes categorías es porque existen diversas estrategias para que el responsable del tratamiento de los datos garantice el cumplimiento del principio de responsabilidad. Es muy diferente contener los datos personales de veinte personas a manejar datos personales de ciudades enteras, por lo que los mecanismos, procesos, y herramientas serán distintos. Por ello, para los niveles complejos y críticos la siguiente tabla expone los requisitos para el tratamiento de datos.

Criterio	Categoría compleja	Categoría crítica
Política de protección de datos personales	Debe ser una declaración formal de compromiso y debe ser clara y comprensible; ser apropiada para los objetivos de la organización; proporcionar lineamientos de alto nivel organizativo; incluir un compromiso de cumplimiento de requisitos de seguridad; incluir un compromiso de respeto a los principios de la ley 29.73; un compromiso de mejora continua y de comunicarse oportuna y claramente al interior de la organización.	Debe ser una declaración formal de compromiso y debe ser clara y comprensible; ser apropiada para los objetivos de la organización; proporcionar exigentes criterios de organización; incluir un compromiso de cumplimiento de requisitos de seguridad, un compromiso de respeto a los principios de la ley 29.733, un compromiso de mejora continua y de comunicarse oportuna y claramente al interior de la organización.

[119] *Ibidem*., Sección 1.1.1 (d)

[120] *Ibidem*., Sección 1.1.1 (e)

[121] Ministerio de Justicia y Derechos Humanos. "Directiva de Seguridad de la Autoridad Nacional de Protección de Datos Personales". Web 8 abril. Capítulo VI Medidas de Seguridad, Sección 1.4.1.

[122] *Ibidem.*

Gobernabilidad	El responsable debe conocer los procesos y procedimientos relacionados con el tratamiento de datos personales y debe tener control de las decisiones sobre los procesos involucrados en el tratamiento, sean tercerizados o no[123].	El responsable debe conocer los procesos y procedimientos relacionados con el tratamiento de datos personales y debe tener control de las decisiones sobre los procesos involucrados en el tratamiento, sean tercerizados o no[124].
Implantación de medidas de seguridad	El responsable debe implantar controles adecuados de un sistema de gestión de seguridad de la información. Para ello, debe designar un "responsable de seguridad del banco de datos personales" con el fin de que coordine la aplicación de la Directiva. Adicionalmente, debe limitar la información encontrada en los bancos de datos a lo estrictamente necesario para desarrollar la finalidad para la cual fueron recolectados. Cada entidad debe evaluar la posibilidad de implantar mecanismos de anonimización o disociación[125].	El responsable debe implantar controles adecuados de un sistema de gestión de seguridad de la información. Para ello, debe designar un "responsable de seguridad del banco de datos personales" con el fin de que coordine la aplicación de la Directiva. Debe limitar la información encontrada en los bancos de datos a lo estrictamente necesario para desarrollar la finalidad para la cual fueron recolectados. Finalmente, cada entidad debe evaluar la posibilidad de implantar mecanismos de anonimización o disociación[126].
Documentar los procedimientos	El Responsable debe implantar y documentar los siguientes procedimientos: a. Control de documentos y registro b. Registros de acceso c. Registros de auditorías d. Registro de incidentes y problemas e. Documento de compromiso de confidencialidad[127].	El responsable debe implantar y documentar los siguientes procedimientos: a. Control de documentos y registro b. Registros de acceso c. Registros de auditorías d. Registro de incidentes y problemas e. Documento de compromiso de confidencialidad[128].

[123] Ministerio de Justicia y Derechos Humanos. "Directiva de Seguridad de la Autoridad Nacional de Protección de Datos Personales". Web 8 abril. Capítulo VI Medidas de Seguridad, Sección 1.3.1.2.

[124] *Ibidem.*

[125] Ministerio de Justicia y Derechos Humanos. "Directiva de Seguridad de la Autoridad Nacional de Protección de Datos Personales". Web 8 abril. Capítulo VI Medidas de Seguridad, Sección 2.

[126] *Ibidem.*

[127] Ministerio de Justicia y Derechos Humanos. "Directiva de Seguridad de la Autoridad Nacional de Protección de Datos Personales". Web 8 abril. Capítulo VI Medidas de Seguridad, Sección 1.4.3.

[128] *Ibidem.*

Documento maestro de seguridad de la información	Requerido[129]	Requerido[130]
Revisión de las medidas de seguridad adoptadas	El responsable debe realizar periódicamente una revisión de la efectividad de todas las medidas de seguridad instauradas y registrar la verificación en un documento[131].	El responsable debe realizar periódicamente una revisión de la efectividad de todas las medidas de seguridad instauradas y registrar la verificación en un documento[132].
Creación de conciencia y entrenamiento en protección de datos personales	Es obligación del responsable desarrollar un programa en el cual se cree conciencia y se entrene a los funcionarios que tratarán los datos con respecto a la protección que dichos datos deben tener[133].	Es obligación del responsable desarrollar un programa en el cual se cree conciencia y se entrene a los funcionarios que tratarán los datos con respecto a la protección que dichos datos deben tener[134].

Tabla núm. 2. Requisitos para el tratamiento de datos por parte de las entidades públicas. (Datos de categoría compleja y crítica)

Con relación al principio de *accountability*, todos los criterios listados en la tabla anterior, ayudarán a que las entidades lo cumplan y a que, por consiguiente, se tenga un adecuado tratamiento de los datos personales. Cabe resaltar que en Perú, la Directiva es de obligatorio cumplimiento, por lo que la realización y cumplimiento de lo mencionado anteriormente no es potestativo de las entidades públicas.

[129] Ministerio de Justicia y Derechos Humanos. "Directiva de Seguridad de la Autoridad Nacional de Protección de Datos Personales". Web 8 abril. Capítulo VI Medidas de Seguridad, Sección 1.3.1.7.

[130] *Ibidem*.

[131] Ministerio de Justicia y Derechos Humanos. "Directiva de Seguridad de la Autoridad Nacional de Protección de Datos Personales". Web 8 abril. Capítulo VI Medidas de Seguridad, Sección 2.1.4.

[132] *Ibidem*.

[133] Ministerio de Justicia y Derechos Humanos. "Directiva de Seguridad de la Autoridad Nacional de Protección de Datos Personales". Web 8 abril. Capítulo VI Medidas de Seguridad, Sección 2.1.8.

[134] *Ibidem*.

E*) República Oriental del Uruguay*

La Unidad Reguladora y de Control de Datos Personales, emitió una guía sobre manejo de Datos Personales en la Administración Pública[135]. La Guía tiene como punto central la siguiente pregunta: "¿cuándo pueden los organismos públicos recabar, comunicar e intercambiar los datos de los ciudadanos?". Para dar respuesta al interrogante, la Guía explica cómo el intercambio de información por medios electrónicos es importante y cómo es necesaria la cooperación e integración entre los diferentes organismos del Estado para simplificar los procesos administrativos y poder brindar gran variedad de servicios de manera conjunta. La Guía está dividida en tres secciones: el consentimiento para el tratamiento de datos personales, casos en los que no se requiere el consentimiento expreso, y políticas de difusión de datos públicos por Internet.

En materia de protección de datos personales, la primera aclaración que hace la guía consiste en que se necesita del previo consentimiento informado de los titulares de los datos y para esto se requieren medios sencillos, claros y gratuitos. La prueba de dicho consentimiento, positivo o negativo, debe ser guardada. Cuando transcurridos diez días el titular de los datos no se ha manifestado, se entenderá que el silencio equivale a negativa.

La Guía establece los criterios en materia de comunicación de datos personales a una persona distinta del titular. Para ello, comienza por establecer que se requiere el consentimiento del titular para poder realizar dicho cometido. Sin embargo, no se requerirá el consentimiento cuando la comunicación de los datos esté autorizada por la ley. De igual manera, si los datos provienen de una fuente accesible al público, como los son los medios masivos de comunicación, no es necesario contar con el consentimiento del titular. Además, si lo que se comunican son listados que contengan únicamente los datos que listamos a continuación, tampoco se requerirá de autorización: "nombres y apellidos; documento de identidad, nacionalidad, domicilio y fecha de nacimiento de las personas físicas. En el caso de personas jurídicas, la razón social, nombre de fantasía, RUT, domicilio, teléfono e identidad de las personas a cargo de la misma"[136]. Asimismo, si los datos se derivan de una relación contractual, científica o profesional y son necesarios para el desarrollo o cumplimiento de dicho contrato, no se requerirá del consentimiento del titular para comunicar los datos a un tercero. Por otra parte, tampoco se requerirá de dicho consentimiento cuando median razones de salud o

[135] Unidad Reguladora y de Control de Datos Personales. " Guía 4 Manejo de Datos Personales en la Administración Pública" Web 4 abril. *<http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_bp_ur_g_4.pdf>*

[136] *Ibidem*.

higiene pública o cuando la información se requiere para realizar estudios epidemiológicos. En ambos casos es importante que se preserve la identidad mediante mecanismos de disociación para estar exentos del consentimiento. Finamente, el último supuesto que exime a la entidad pública de requerir el consentimiento expreso del titular es cuando se hayan aplicado procedimientos de disociación en cualquier intercambio de datos a un tercero.

En materia de difusión de información pública, cuando la misma contiene datos personales que requieran el previo consentimiento de sus titulares por no estar contemplados en las salvedades previamente mencionadas, tienen carácter de confidenciales y, por tanto, deben ser clasificados.

Hay otros casos en los que para garantizar la transparencia del Estado es necesario difundir cierta información como sucede en los concursos públicos. Para ello es suficiente la divulgación de nombres y apellidos y las puntuaciones obtenidas en cada etapa del concurso. Vale aclarar que si se va a difundir la hoja de vida de un funcionario, la Guía aclara que es suficiente publicar la información relativa a la función o al cargo y la que permita evaluar la idoneidad técnica de quien lo ocupa. De esta manera, la información relacionada con el estado civil, edad, domicilio, teléfono particular y correo personal no pueden ser divulgadas.

Capítulo IV

GUÍAS DE RESPONSABILIDAD DEMOSTRADA (*ACCOUNTABILITY*) Y PROGRAMAS INTEGRALES DE GESTIÓN DE DATOS PERSONALES

Pocos países han desarrollado guías de buenas prácticas en materia de responsabilidad demostrada[1], razón por la cual a continuación nos referiremos a las guías existentes en Australia, Canadá, Colombia y Hong Kong. Adicionalmente, nos referiremos a la Guía GECTI sobre *accountability* en las transferencias internacionales de datos.

1. Australia

En Australia existe una guía que se ocupa de la publicidad y transparencia en el manejo de datos, y que contiene el principio de *accountability* de manera transversal. Dicha guía se titula "Chapter 1: Australian Privacy Principle 1 – Open and transparent management of personal information"[2] y fue expedida en febrero de 2014 por la Oficina del Comisionado de Información de Australia. El objetivo de la guía es crear unos lineamientos que deben tener en cuenta las entidades que traten datos personales para que lo hagan de manera abierta y transparente[3].

En términos generales la guía se estructura de la siguiente manera:

[1] No obstante, desde la academia se ha emitido guías especializadas de accountability respecto de aspecto puntuales sobre tratamiento de datos como lo es, por ejemplo, la circulación transfronteriza de datos. En dicho sentido, véase: Nelson Remolina Angarita, Luisa Fernanda Álvarez Zuluaga, *Guía GECTI para la implementación del principio de responsabilidad demostrada —accountability— en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos*, Bogotá, Universidad de los Andes, Facultad de Derecho, GECTI, 2018, 1-58. Disponible en: *https://gecti.uniandes.edu.co/index.php/accountability*

[2] El texto de la guía puede consultarse en: <*https://www.oaic.gov.au/resources/agencies-and-organisations/app-guidelines/APP_guidelines_complete_version_2_March_2018.pdf*>

[3] Australia. Office of the Australian Information Commissioner. "Australian Privacy Principles Guidelines" Privacy Act 1988. Web 17 abril.

Principio de Privacidad australiano 1 (What does APP 1 say?)	• Obligación 1: Tomar las medidas razonables para implantar prácticas, procedimientos y sistemas que garanticen que la entidad cumpla con los principios de privacidad australianos. • Obligación 2: Tener una política de privacidad sobre el tratamiento de datos personales. • Obligación 3: Tomar las medidas razonables para que el programa de privacidad esté disponible de manera gratuita y adecuada para garantizar su acceso.
Prácticas, sistemas y procedimientos para garantizar el cumplimiento del principio (implementing practices, procedures and systems to ensure APP compliance)	Para implantar las prácticas, sistemas y procedimientos se requiere hacer un estudio que determine: 1. La naturaleza de la información tratada. 2. Las posibles consecuencias adversas hacia un titular si sus datos personales son tratados de manera inadecuada. 3. La naturaleza de la entidad que desarrolla el programa.
Desarrollo de una política de privacidad (Developing an APP Privacy Policy)	Elementos que debería contener la política de privacidad: 1. Clasificación de información recolectada. 2. Descripción de la recolección y tratamiento de los datos. 3. Propósitos de la recolección, uso y divulgación de los datos personales. 4. Acceso y corrección de los datos personales para el titular. 5. Quejas y reclamos sobre brechas a la privacidad. 6. Transferencia internacional de datos.
Publicidad de la política de privacidad (Making an APP Privacy Policy publicly available)	1. Desarrollar una política de privacidad que esté disponible de forma gratuita y apropiada. 2. Desarrollar un formulario mediante el cual se pueda solicitar la política de privacidad de la entidad.

Tabla núm. 1. Estructura de la guía australiana de principios de privacidad.

La Ley de Privacidad de Australia fue reformada en marzo de 2014 época en que se incluyeron trece principios conocidos como *Australian Privacy Principles*

(APP)[4]. El primer principio es el de manejo abierto y transparente de los datos personales (en adelante APP 1). Por consiguiente, la Guía regula la publicidad y transparencia ("Australian Privacy Principle 1-Open and transparent management of personal information") y en ella se encuentra desarrollado el principio de *accountability* de manera transversal. El APP 1 refiere todos los requerimientos que las entidades deben cumplir para manejar los datos de manera transparente. Para ello hay una serie de prácticas, procedimientos, y sistemas que asegurarán el cumplimiento de dicho principio.

En términos generales el objetivo del APP 1 es asegurar que las entidades sometidas a la Ley de Protección de Datos traten dichos datos de manera abierta y transparente[5]. Para esto, ese primer principio le impone a la entidad tres obligaciones distintas. La primera es la de adoptar las medidas necesarias para implantar prácticas, procedimientos y sistemas que garanticen que la entidad cumpla con los APP y con cualquier código que haya registrado para el tratamiento de datos. La segunda obligación es tener un Programa de privacidad actualizado que indique cómo trata la entidad los datos personales. Finalmente, se impone la obligación de tomar medidas conducentes para que su programa de privacidad esté disponible de manera gratuita, en un medio general, y en un medio particular a petición del titular[6].

A continuación nos referiremos a estos tres aspectos:

A) *Implantación de prácticas, procedimientos, y sistemas*

La primera obligación impuesta por el APP 1 es la de implantar prácticas, procedimientos y sistemas para garantizar el cumplimiento de dicho principio. Los pasos razonables que debe tomar cada entidad para materializar en la práctica el cumplimiento de esta obligación depende de la naturaleza de los datos personales que son tratados. Así, por ejemplo, si los datos son de naturaleza sensible, las medidas deben ser más estrictas.

Adicionalmente, las entidades deben hacer un análisis de riesgos, entre más adversas sean las consecuencias en caso de un mal uso de los datos, más rigurosos deben ser los pasos para evitar que tal ocurra[7]. También es relevante a la hora de realizar un programa, que se revise la naturaleza de la entidad, debido a que, según sea su tamaño, sus recursos y su modelo de negocios, hay ciertos elementos que deben adoptar.

[4] *Ibidem.*

[5] *Ibidem.*

[6] *Ibidem.*

[7] *Ibidem.*

Tras este breve análisis, la guía enuncia un número de prácticas, procedimientos y sistemas que las entidades deben implantar. Por un lado, deben clasificar los procedimientos según la etapa en la que se realizará la recolección, divulgación, almacenamiento o destrucción de los datos. Adicionalmente, tienen que implantar sistemas de seguridad, físicos y virtuales con el fin de evitar interferencias y pérdidas en los datos. Por otra parte, deben realizar procedimientos para identificar y responder a las brechas de privacidad, evitando así que se generen perjuicios al titular.

De otra parte, se recomienda que las organizaciones cuenten con mecanismos de gobernanza como la designación de oficiales de protección de datos. Adicionalmente, se exhorta a las entidades para que realicen capacitaciones a los empleados y tengan boletines de información.

Lo anterior debe ir acompañado de herramientas de supervisión apropiadas con los empleados para hacer un análisis de cómo están manejando los datos. Finalmente, la entidad debe crear mecanismos que garanticen que los agentes y contratistas que actúan a nombre de o para la entidad, cumplan las políticas de privacidad.

B) *Programa de privacidad*

La segunda obligación requiere que las entidades tengan un programa de privacidad de datos (APP Privacy Policy) actualizado para garantizar el correcto tratamiento de datos personales. Este programa debe ser fácil de entender, por lo que debe tener en cuenta el público al que está dirigido y no debería ser una mera réplica de la ley.

Es importante que el programa solo incluya la información relevante de manejo de datos para la entidad y que ésta se encuentre en la página Web de la misma. Igualmente, el programa debe ser objeto de permanente actualizaciones para que siempre refleje el manejo de datos que se está dando. Como mínimo, en la guía se propone que se revise cada año y es necesario que se indique cuándo fue actualizado por última vez y que reciba comentarios sobre la experiencia que se ha tenido con el manejo de los datos, con el fin de que se utilice esa retroalimentación para mejorar el programa.

Hay cierta información que debería ser incluida en un programa de privacidad según las sugerencias de la autoridad australiana en materia de protección de datos. Esta, por ejemplo, sugiere tener un resumen de las clases de datos personales que se recolectan, señalando la forma en que se recolecta y almacena la información junto con los propósitos para los que se realizó. Vale aclarar que es cardinal tener procedimientos para que los titulares accedan a su información, hagan correcciones,

y presenten quejas y reclamos. Finalmente, la entidad debería aclarar si realiza transferencias internacionales de datos y a quién.

A pesar de que los elementos que hemos listado son los más significativos, la guía también puede incluir otros. Entre ellos, la autoridad australiana propone incorporar una lista de quiénes, además de los titulares, tienen acceso a los datos. De igual manera, propone explicar cómo realizará cambios en su política de protección de datos y cómo esas modificaciones serán informadas a los titulares. Por otra parte, de poder comunicarse el titular con la organización mediante pseudónimos, la entidad debe aclarar en qué supuestos puede realizar estas comunicaciones y cuándo requiere identificarse plenamente. Finalmente, es trascendental explicar las prácticas de retención y destrucción de la información para que los titulares conozcan con claridad y transparencia estos aspectos sobre el tratamiento d sus datos.

C) *Disponibilidad del programa de privacidad*

La última obligación impuesta por el APP 1 es la de garantizar que el programa de privacidad del responsable del tratamiento de datos esté disponible, con el fin de cumplir cabalmente con el principio de transparencia y acceso a la información. Para esto, se propone que el programa esté publicado en la página web de la organización y pueda ser descargado fácilmente (i. e. que no requiera un programa especial para visualizarse). En caso de no poderse publicar de manera virtual, el programa debe encontrarse en la sede de la entidad y debe suministrarse una copia al titular en caso de que así lo requiera. Si el titular se contacta telefónicamente se le debe explicar cómo pueden acceder al programa de privacidad de la organización.

2. Canadá

La guía canadiense de *accountability* se titula “Getting Accountability Right with a Privacy Management Program”[8] y fue expedida en 2012 por la Oficina del Comisionado de Privacidad de Canadá. Su objetivo es proveer sobre lo que significa ser una organización responsable (*accountable organization*). Vale aclarar que la guía va dirigida a las empresas del sector privado que se espera tengan un programa de gestión de datos (*Privacy Management Program*).

En términos generales la guía se estructura de la siguiente manera:

[8] El texto de la guía puede consultarse en: <*https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf*>

Compromisos organizacionales	**1. Desde la Alta Gerencia** • Nombrar un oficial de protección de datos (Privacy Officer). • Aprobar los controles del programa . • Aprobar y monitorear el programa integral de gestión de datos personales (PIGDP). • Informar periódicamente sobre la ejecución del PIGDP a la Junta Directiva. **2. Oficial de Protección de Datos** • Debe establecer e implantar controles del programa. • Coordinar el tratamiento de datos en la organización. • Revisar y evaluar el PIGDP. **3. Mecanismos de reporte** • Auditorías internas. • Tests de cumplimiento. • Reportes de cumplimiento.
Controles del programa	1. Inventario de bases de datos. 2. Diseñar políticas para recolección, uso, acceso, corrección, retención, desecho de datos personales. 3. Diseñar controles físicos y tecnológicos de seguridad. 4. Implantar herramientas de evaluación y riesgo del tratamiento de datos en la organización. 5. Formación y educación del equipo de colaboradores para generar una cultura de tratamiento de datos personales . 6. Tener previsto protocolos de respuesta a incidentes de seguridad. 7. Gestionar adecuadamente los procesos que impliquen recurrir a encargados de tratamiento o transmisiones y transferencias de datos. 8. Comunicación externa de sus políticas para conocimiento del público y los titulares de los datos.
Evaluación y revisión permanente	Efectuar evaluaciones independientes respecto de las medidas que se han adoptado para garantizar un debido tratamiento de los datos personales.
Demostración de cumplimiento	Implantar mecanismos que permitan probar el cumplimiento de los deberes de la RNEC sobre tratamiento de datos personales.

Tabla núm. 2. Estructura de la guía canadiense de *accountability*.

Como se mencionó, la guía fue elaborada por la Oficina del Comisionado de Privacidad para Canadá[9]. Se establecen criterios para cumplir con el principio de responsabilidad demostrada en las organizaciones sujetas a las reglas de protección de datos para el sector privado. En esta guía, se entiende que la responsabilidad demostrada con relación a la privacidad se materializa en políticas y procedimientos pertinentes que promuevan las buenas prácticas en esta materia. Por ello, la guía considera que la mejor manera de cumplir el principio de *accountability* es elaborando un programa integral de gestión de datos (*Privacy Management Program*).

El documento elaborado por la autoridad canadiense tiene dos partes. La primera contiene un esquema de los fundamentos básicos que cada organización necesita, que son esenciales para el cumplimiento del principio de *accountability*. La segunda se refiere a la manera de mantener y mejorar el programa integral de gestión de datos debido a que este nunca será un producto terminado, sino que requiere constante evaluación y revisión.

A) *Fundamentos básicos del principio de responsabilidad*

Cuando se habla del principio de responsabilidad, hay varios requisitos que se deben tener en cuenta para garantizar su cumplimiento. Por un lado, las organizaciones están obligadas a designar a alguien que vigile el desarrollo, la implantación y el mantenimiento del programa de protección de datos de la empresa. En segundo lugar, se deben establecer políticas y procedimientos, dentro de los cuales es importante tener capacitaciones para empleados.

Asimismo, se requiere que las organizaciones dispongan de sólidas cláusulas contractuales en materia de transferencia de información a terceros para garantizar que dicha información esté protegida, como lo haría la misma organización. Finalmente, se espera que tengan sistemas para responder a los requerimientos que hagan los individuos que quieran acceder o corregir su información o que quieran presentar queja, denuncia o reclamo sobre la manera en la que sus datos están siendo protegidos[10].

Con el fin de cumplir todos los requisitos, el primer fundamento básico consiste en que la organización se comprometa con el correcto tratamiento de datos personales. Para ello es necesario desarrollar una estructura interna de gobernanza que promueva una cultura de respeto hacia la privacidad y protección de datos. Para el efecto, es de suma importancia el apoyo de la alta gerencia en el desarrollo de la política de privacidad, lo cual se refleja, entre otras, con la designación del

[9] Canadá. Office of the Privacy Commissioner of Canada. “Getting Accountability Right with a Privacy Management Program”. Web 15 abril.

[10] *Ibidem*.

oficial de protección de datos, el aval de controles del programa y el monitoreo del programa para llevar el reporte a los accionistas[11].

Vale aclarar que para organizaciones más grandes se recomienda que además del oficial de protección de datos, se cree una oficina o dirección de protección de datos que tenga responsabilidades delegadas sobre monitoreo del programa de gestión de datos. Finalmente, dentro del compromiso de la organización debe estar la creación de mecanismos de reporte mediante los cuales se garantice que todos los trabajadores conozcan la estructura del programa de privacidad y si esta funciona adecuadamente.

Otro fundamento básico de un buen programa de gestión de datos para garantizar el principio de *accountability* es tener controles. Dichos controles se encuentran de varias maneras. Por un lado, se deben realizar inventarios para saber qué datos personales se tienen, qué información es sensible, cuál es pública y para qué propósitos fue recolectado cada dato con el fin de que la organización pueda supervisar que los datos solo se utilizan para lo que se le dijo al titular que se iban a utilizar[12]. Por otra parte, se deben desarrollar políticas de uso de información, requerimientos del consentimiento, notificaciones a los titulares de los datos, acceso y corrección de la información personal, retención y destrucción de la misma.

Además, es necesario que dentro de las políticas que se pongan en práctica, estén las relacionadas con controles administrativos, físicos y tecnológicos de seguridad. Junto a lo anterior deben crearse herramientas para que los titulares de los datos puedan presentar quejas y reclamos cuando sientan que su información está siendo utilizada indebidamente y contar con mecanismos o procesos para evaluar los riesgos de seguridad a los que se somete esa información.

La educación y capacitación son otro aspecto relevante para lograr el debido tratamiento de la información[13]. Por esto, se recomienda que todos los empleados tengan una educación general en materia de tratamiento de datos, y aquellos que están expuestos directamente al uso de dichos datos, tengan un entrenamiento más específico conforme a la función que cumplen en la compañía.

De otra parte, la organización responsable del tratamiento debe tener protocolos para manejar brechas de seguridad y cualquier otro incidente que pueda presentarse. Para ello, se recomienda tener una persona especializada que se encargue de brechas de seguridad para que pueda manejar la situación. La autoridad canadiense aclara que en compañías grandes se requerirá de varios empleados para reportar la brecha y activar controles de mitigación de daños[14]. Finalmente, dentro de los controles es

[11] *Ibidem.*

[12] *Ibidem.*

[13] *Ibidem.*

[14] *Ibidem.*

importante que se tenga en cuenta cómo se va a manejar la transferencia de datos a terceros y a proveedores y cómo se conducirán las comunicaciones externas con respecto a todo lo relacionado con el tratamiento de datos personales.

B) *Evaluación y revisión continua*

Habiendo establecido los fundamentos básicos para construir un programa de gestión de datos (*privacy management program*) para cumplir con el principio de *accountability*, la segunda parte de la guía se ocupa de la evaluación y revisión continua del programa de gestión de datos[15].

En esta parte se recomienda a las empresas que desarrollen un plan de monitoreo y revisión (*review and revise policies*) para garantizar que el programa de protección de datos esté actualizado y sin fallas, el cual usualmente lo desarrolla el oficial de protección de datos de la compañía. Una vez se ha desarrollado dicho plan, es necesario evaluar y revisar los controles que se establecieron en el programa de gestión de datos para mirar si hay riesgos nuevos y si el programa se ha mejorado para incluir hallazgos nuevos y aprendizajes de brechas pasadas. Para ello, es necesario monitorear y actualizar el inventario de datos personales, revisar las políticas de la empresa, modificar la capacitación a los empleados en los puntos pertinentes, y adaptar los protocolos de respuesta a las brechas de seguridad cuando dé lugar para que reflejen las buenas prácticas en la materia.

3. Colombia

Como es sabido, el artículo 15 de la Constitución de la República de Colombia no solo consagra el derecho de cualquier persona de conocer, actualizar y rectificar los datos personales que existan sobre ella en bancos de datos o archivos de entidades públicas o privadas, sino que ordena a quienes tienen datos personales de terceros, a respetar los derechos y garantías previstos en la Constitución cuando se recolecta, trata y circula esa clase de información.

La ley estatutaria 1581 de 17 de octubre de 2012, por su parte, establece las condiciones mínimas para realizar el tratamiento legítimo de la información de cualquier persona natural. Tanto los literales k) del artículo 17 como f) del artículo 18 de dicha ley obliga a los responsables y encargados del tratamiento de datos personales a "adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos".

[15] *Ibidem.*

El artículo 25 de la ley, establece que las políticas de tratamiento de datos son de obligatorio cumplimiento y que su desconocimiento acarreará sanciones. Dichas políticas no pueden garantizar un nivel de tratamiento inferior al establecido en la ley 1581 de 2012.

El capítulo III del decreto 1377 de 2013 (incorporado en el decreto 1074 de 2015*)* reglamenta algunos aspectos relacionados con el principio de responsabilidad demostrada y la Superintendencia de Industria y Comercio con miras a dar orientaciones sobre la materia y la construcción de los programas integrales de gestión de datos expidió el 28 de mayo de 2015 la "guía para implementación del principio de responsabilidad demostrada (*accountability*)" con miras a que los obligados a cumplir la ley 1581 de 2012 deben hacer lo que se refiere a continuación en los siguientes frentes: (véase tabla de la página siguiente).

Como se observa, el principio de responsabilidad demostrada (*accountability*) exige implantar acciones concretas en cada organización para garantizar el debido cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales.

En la Guía, la Superintendencia de Industria y Comercio (SIC) establece que el ordenamiento jurídico colombiano trae exigencias precisas para que los sujetos obligados adopten políticas internas efectivas que no se limiten a reproducir los textos legales ni que sean una declaración básica de principios. Es por esto por lo que se les recomienda a las entidades desarrollar un Programa Integral de Gestión de Datos Personales (PIGD) para garantizar mayor protección de los individuos. Un programa efectivo debería contener políticas que, por un lado, sirvan como respuesta a los ciclos internos de gestión de datos y que, por otro, generen unos resultados que se puedan medir con el fin de que la entidad pruebe la diligencia especial[16]. Adicionalmente, los sujetos obligados deben garantizar la existencia de una estructura administrativa para adoptar y poner en práctica la ley de protección de datos; la adopción de mecanismos internos para ejecutar el PIGD, y la adopción de procesos para la atención y respuestas a consultas y peticiones[17].

Entrando en materia, la SIC establece unos elementos esenciales que deben ser incorporados por la organización con el fin de desarrollar e implantar el PIGD. En primer lugar, el programa debe tener un componente de compromiso de la organización. Dentro de este, están los compromisos adoptados por la alta dirección de la organización, los cuales incluyen el nombrar un oficial de protección de datos, aprobar y monitorear el PIGD, e informar a los directivos sobre su ejecución[18].

[16] Colombia. Superintendencia de Industria y Comercio. "Guía para la implementación del principio de responsabilidad demostrada (*accountability*). Web 10 abril.

[17] *Ibidem.*

[18] *Ibidem.*

Compromiso de la organización	1. Desde la alta gerencia • Designar persona o área responsable del cumplimiento de las normas sobre tratamiento de datos personales. • Aprobar y monitorear el programa integral de gestión de datos personales (PIGDP). • Informar periódicamente sobre la ejecución del PIGDP. • Destinar recursos necesarios para el cumplimiento de la normativa sobre tratamiento de dato personales. 2. Presentación de informes a directivos: • Seguimiento y ejecución del PIGDP • Auditorías internas sobre tratamiento de datos personales.
Controles del programa	1. Diseñar e implantar procesos para cumplir las normas sobre tratamiento de datos personales. 2. Realizar un inventario de bases de datos. 3. Definir la política de tratamiento de datos personales y otras conexas como, entre otras, las de seguridad. 4. Implantar herramientas de evaluación y riesgo del tratamiento de datos en la organización. 5. Formación y educación del equipo de colaboradores con miras a generar una cultura de tratamiento de datos personales y asegurar que respetarán las normas en el ejercicio de sus funciones. 6. Tener previsto protocolos de respuesta a incidentes de seguridad. 7. Gestionar adecuadamente los procesos que impliquen recurrir a encargados de tratamiento o transmisiones y transferencias de datos. 8. Comunicación externa de sus políticas para conocimiento del público y los titulares de los datos.
Evaluación y revisión continua	Efectuar evaluaciones independientes respecto de las medidas que se han adoptado para garantizar un debido tratamiento de los datos personales.
Demostración del cumplimiento	Implantar mecanismos probatorios del cumplimiento de los deberes de la RNEC sobre tratamiento de datos personales.

Tabla núm. 3. Estructura de la guía colombiana de *accountability*.

Con respecto al oficial de protección de datos, este debe diseñar e implantar el programa, por lo cual debe ser un enlace entre todas las áreas de la organización y debe impulsar una cultura de protección de datos. Es importante resaltar que esta es la persona encargada de registrar ante la SIC las bases de datos de la organización. En lo que respecta a la presentación de informes de los directivos, se sugiere implantar planes de auditoría interna para verificar el cumplimento de políticas de protección de datos.

El segundo elemento establecido por la SIC es el de instaurar controles al Programa[19]. Para esto, se propone establecer procedimientos operacionales, y además realizar un inventario de las bases de datos que contengan información personal para poder identificar la información sensible y asegurarse de poder implantar las medidas adecuadas para su protección reforzada. En tercer lugar, es necesario que se generen políticas internas sobre recolección, almacenamiento y uso de datos. Por otra parte, también se deben desarrollar políticas con respecto al acceso y corrección de dichos datos, como sobre su conservación y eliminación. También es necesario que la organización tenga un sistema de administración de riesgos en el que se identifiquen, midan, controlen y monitoreen los diversos riesgos asociados al tratamiento de datos personales. En este punto del programa es necesario considerar la formación y educación de aquellos que tratan los datos y los protocolos de manejo de violaciones e incidentes para tener una política clara en materia de comunicación externa. Por último, la guía recomienda designar a alguien que se encargue de las transferencias internacionales de datos con el fin de realizar auditorías, entablar acuerdos y exigir la adherencia a las políticas de tratamiento utilizadas[20].

Un último elemento que establece la guía es el de revisión y evaluación continua del Programa con el fin de que siempre esté actualizado[21]. Para ello se recomienda que las organizaciones desarrollen planes de supervisión y revisión donde se mida el desempeño y se revisen las políticas y controles del programa. Por otra parte, se deben evaluar y revisar los controles del programa para asegurarse de que incluyan las últimas amenazas y riesgos a los que está expuesta la protección de datos.

A) *De los lineamientos del decreto 1413 de 2017 para la prestación de servicios ciudadanos digitales*

En adición a la guía de responsabilidad demostrada de la SIC, nos parece relevante referirnos a varias instituciones incorporadas a la regulación colombiana mediante el decreto 1413 de 2017[22]. Buena parte de ellos reproducen las medidas proactivas a que nos referimos cuando estudiamos los documentos de la Unión Europea, la Red Iberoamericana de Protección de Datos y la Conferencia Internacional de Autoridades sobre privacidad y protección de datos.

[19] *Ibidem*.

[20] *Ibidem*.

[21] *Ibidem*.

[22] Decr. 1413 de 2017, "por el cual se adiciona el Título 17 a la Parte 2 del Libro 2 del decreto único reglamentario del sector de tecnologías de la información y las comunicaciones, decr. 1078 de 2015, que reglamenta parcialmente el Capítulo IV del Título III de la ley 1437 de 2011 y el art. 45 de la ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales".

Estas instituciones cobran especial relevancia para las entidades públicas y otras que tienen que ver con la aplicación del decreto cuyo objeto es establecer "los lineamientos que se deben cumplir para la prestación de servicios ciudadanos digitales, y para permitir a los usuarios el acceso a la administración pública a través de medios electrónicos"[23].

Los servicios ciudadanos digitales se dividen en básicos y especiales. Los primeros son los siguientes:

- Autenticación biométrica[24].
- Autenticación con cédula[25] digital[26].
- Autenticación electrónica[27].
- Carpeta ciudadana[28].
- Interoperabilidad[29].

[23] Cfr. Decr. 1413 de 2017, art. 2.2.17.1.1.

[24] Cfr. El servicio de autenticación biométrica lo describe de la siguiente manera el num. 1.1. del art. 2.2.17.2.1.1. del decr. 1413 de 2017: "Es aquel que permite verificar y validar la identidad de un ciudadano colombiano por medio de huellas dactilares contra la base de datos biométrica y biográfica de la Registraduría Nacional del Estado Civil, dando pleno cumplimiento a la resolución 5633 de 2016 emitida por la Registraduría Nacional del Estado Civil o cualquier otra norma que la adicione, modifique, aclare, sustituye o derogue".

[25] La *cédula de ciudadanía digital* es definida como el "el equivalente funcional de la cédula de ciudadanía, expedida por la Registraduría Nacional del Estado Civil" (decr. 1413 de 2017, art. 2.2.17.1.3. num. 5).

[26] Cfr. El servicio de autenticación con cédula digital es descrito de la siguiente manera en el num. 1.2. del art. 2.2.17.2.1.1. del decr. 1413 de 2017: "Es aquel que permite la validación de la identidad de los ciudadanos colombianos por medios electrónicos, a través de la cédula de ciudadanía digital que para tal efecto expida la Registraduría Nacional del Estado Civil".

[27] Cfr. El servicio de autenticación electrónica es descrito de la siguiente manera en el num. 1.3. del art. 2.2.17.2.1.1. del decr. 1413 de 2017: "Es aquel que permite validar a los usuarios por medios electrónicos, en relación con un mensaje de datos y provee los mecanismos necesarios para firmarlos electrónicamente, en los términos de la ley 527 de 1999 y sus normas reglamentarias sin perjuicio de la autenticación notarial".

[28] Cfr. El servicio de carpeta ciudadana se describe en el num. 1.4. del art. 2.2.17.2.1.1. del decr. 1413 de 2017 como sigue: "Es aquel que permite el almacenamiento y conservación electrónica de mensajes de datos en la nube para las personas naturales o jurídicas, en donde estas pueden recibir, custodiar y compartir de manera segura y confiable la información generada en su relación con el Estado a nivel de [*sic*] trámites y servicios. En ningún caso la carpeta ciudadana hará las veces de sistema de gestión de documentos electrónicos de archivo".

[29] Se define el servicio de interoperabilidad (num. 1.5. del ar. 2.2.17.2.1.1. del decr. 1413 de 2017) como "aquel que brinda las capacidades necesarias para garantizar el adecuado flujo de información y de interacción entre los sistemas de información de las entidades del Estado, permitiendo el intercambio, la integración y la compartición de la información, con el propósito de facilitar el ejercicio de sus funciones constitucionales y legales, acorde con los lineamientos del marco de interoperabilidad".

Según el citado decreto, la RNEC tiene directa incidencia en los servicios de autenticación biométrica y con cédula digital.

Los servicios ciudadanos digitales especiales, por su parte, son aquellos adicionales a los servicios básicos "tales como el desarrollo de aplicaciones o soluciones informáticas que puedan ser de interés para la administración o cualquier interesado en el marco de la prestación de los servicios ciudadanos digitales básicos"[30],

El decreto 1413 obliga a las entidades que integran la administración pública en los términos del artículo 39[31] de la ley 489 de 1998 y a los particulares que cumplen funciones públicas[32]. Respecto de las otras entidades que forman parte del Estado colombiano, la norma precisa que "*la implementación de los servicios ciudadanos digitales en las ramas legislativa y judicial, en los órganos de control, los órganos autónomos e independientes, y demás organismos del Estado no contemplados en este artículo, se realizará bajo un esquema de coordinación y colaboración armónica en aplicación de los principios señalados en el artículo 209 de la Constitución Política*"[33].

La privacidad y la circulación restringida de la información son piedras angulares de la prestación de los servicios ciudadanos digitales. En ese sentido, el numeral 7 del artículo 2.2.17.1.5. consagra el principio de seguridad, privacidad y circulación restringida de la información, que ordena lo siguiente: "Toda la

[30] Cfr. decr. 1413 de 2017, art. 2.2.17.2.1.1. num. 2.

[31] Ley 489 de 1998, art. 39 " *Integración de la administración pública*. La administración pública se integra por los organismos que conforman la rama ejecutiva del poder público y por todos los demás organismos y entidades de naturaleza pública que de manera permanente tienen a su cargo el ejercicio de las actividades y funciones administrativas o la prestación de servicios públicos del Estado colombiano.

"La Presidencia de la República, los ministerios y los departamentos administrativos, en lo nacional, son los organismos principales de la administración.

"Así mismo, los ministerios, los departamentos administrativos y las superintendencias constituyen el sector central de la administración pública nacional. Los organismos y entidades adscritos o vinculados a un ministerio o un departamento administrativo que gocen de personería jurídica, autonomía administrativa y patrimonio propio o capital independiente conforman el sector descentralizado de la administración pública nacional y cumplen sus funciones en los términos que señale la ley.

"Las gobernaciones, las alcaldías, las secretarías de despacho y los departamentos administrativos son los organismos principales de la administración en el correspondiente nivel territorial. Los demás les están adscritos o vinculados, cumplen sus funciones bajo su orientación, coordinación y control en los términos que señalen la ley, las ordenanzas y los acuerdos, según el caso.

"Las asambleas departamentales y los concejos distritales y municipales son corporaciones administrativas de elección popular que cumplen las funciones que les señalan la Constitución Política y la ley".

[32] Cfr. Decr. 1413 de 2017, art. 2.2.17.1.2.

[33] Cfr. Decr. 1413 de 2017, art. 2.2.17.1.2. parg.

información de los usuarios que se genere, almacene o transmita en el marco de los servicios ciudadanos digitales, debe ser protegida y custodiada bajo los más estrictos esquemas de seguridad y privacidad con miras a garantizar la confidencialidad, el acceso y circulación restringida de la información, de conformidad con lo estipulado en el componente de seguridad y privacidad de la estrategia de gobierno en línea".

Visto lo anterior, a continuación nos referiremos a destacar los aspectos más relevantes que el decreto en mención prevé sobre (i) la responsabilidad demostrada y el programa integral de datos; (ii) la privacidad por diseño y por defecto; (iii) el delegado de protección de datos y (iv) la evaluación del impacto del tratamiento de datos personales en determinados proyectos o actividades que generan graves riesgos a los derechos de los titulares de dicha información.

a) *Responsabilidad demostrada y programa integral de gestión de datos*. La norma se refiere expresamente a la responsabilidad y los programas integrales de gestión de datos de la siguiente manera.

En primer lugar, obliga a los "operadores de servicios ciudadanos digitales"[34] a adoptar "*medidas apropiadas, efectivas y verificables que le permitan demostrar el correcto cumplimiento de las normas sobre tratamiento de datos personales*"[35]. En segundo lugar, obliga a los operadores a "crear e implementar un Programa Integral de Gestión de Datos (PIGD), como mecanismo operativo para garantizar el debido tratamiento de los datos personales"[36].

Finalmente, se ordena que el PIGD cumpla con "*las instrucciones de la Superintendencia de Industria y Comercio, en particular, la guía para la implementación del principio de responsabilidad demostrada (accountability) de dicha entidad*" [37].

b) *Privacidad por diseño y por defecto*. El decreto no solo define la privacidad por diseño "como la protección de la información que exige la incorporación en las especificaciones de diseño de tecnologías, procesos, prácticas de negocio e infraestructuras físicas que aseguren la protección de la privacidad de la información"[38], sino que la considera un principio cuyo alcance es el siguiente: "desde antes que se recolecte información y durante todo el ciclo de vida de la misma, se deben adoptar medidas preventivas de diversa naturaleza (tecnológica, organizacional, humana, procedimental) para evitar vulneraciones al derecho a la privacidad o a la confidencialidad de la información, así como fallas de seguridad o indebidos

[34] Los operadores pueden ser personas jurídicas de naturaleza pública o privada

[35] Cfr. Decr. 1413 de 2017, art. 2.2.17.6.3.

[36] *Ibidem*.

[37] *Ibidem*.

[38] Cfr. Decr. 1413 de 2017, art. 2.2.17.1.3 num. 17..

tratamientos de datos personales. La privacidad y la seguridad deben hacer parte del diseño, arquitectura y configuración predeterminada del proceso de gestión de información y de las infraestructuras que lo soportan"[39].

El decreto obliga a los operadores a aplicar las buenas prácticas y principios desarrollados internacionalmente sobre los "*Privacy by design (PbD*)" y "*Privacy Impact Assessment (PIA)*", y prescribe que "la protección de la privacidad y de los datos no puede ser asegurada únicamente a través del cumplimiento de la normativa, sino que debe ser un modo de operar de las organizaciones, y aplicarlo a los sistemas de información, modelos, prácticas de negocio, diseño físico, infraestructura e interoperabilidad, que permita garantizar la privacidad al ciudadano y a las empresas en relación con la recolección, uso, almacenamiento, divulgación y disposición de los mensajes de datos para los servicios ciudadanos digitales gestionados por el operador"[40].

Para lograr lo anterior, los operadores deben tener presente los siguientes lineamientos:

"1. Realizar y actualizar las evaluaciones del impacto de tratamiento de los datos personales y el Programa Integral de Gestión de Datos Personales ante cambios que generen riesgos de privacidad.

"2. Incorporar prácticas y procesos de desarrollo necesarios destinados a salvaguardar la información personal de los individuos a lo largo del ciclo de vida de un sistema, programa o servicio.

"3. Mantener las prácticas y procesos de gestión adecuados durante el ciclo de vida de los datos que son diseñados para asegurar qué sistemas de información cumplen con los requisitos, políticas y preferencias de privacidad de los ciudadanos.

"4. Uso de los máximos medios posibles necesarios para garantizar la seguridad, confidencialidad e integridad de información personal durante el ciclo de vida de los datos, desde su recolección original, a través de su uso, almacenamiento, difusión y segura destrucción al final del ciclo de vida.

"5. Asegurar la infraestructura, sistemas TI, y prácticas de negocios que interactúan o implican el uso de cualquier información o dato personal siendo sujeta a verificación independiente por parte de todas las partes interesadas, incluyendo clientes, usuarios y organizaciones afiliadas"[41].

En adición a nuestros comentarios sobre este principio, queremos destacar que la privacidad por diseño (PbD por sus siglas en inglés) fue definida y desarrollada desde la década de los noventa por Ann Cavoukian, quien considera que

[39] Cfr. Decr. 1413 de 2017, art. 2.2.17.1.5. num. 6.

[40] Cfr. Decr. 1413 de 2017, art. 2.2.17.6.5.

[41] *Ibidem*.

"el aseguramiento de la privacidad debe convertirse en el modo de operación predeterminado de una organización"[42]. Para el efecto, propone los siguientes siete principios que nos permitimos mencionar, pues son muy importantes para lograr los objetivos del citado principio:

• *Proactivo, no reactivo. Preventivo no correctivo*. Según este principio, se deben adoptar medidas proactivas y no reactivas para proteger los datos personales. Según Cavoukian, la PbD "no espera a que los riesgos se materialicen, ni ofrece remedios para resolver infracciones de privacidad una vez que ya ocurrieron, su finalidad es prevenir que ocurran. En resumen, la Privacidad por Diseño llega antes del suceso, no después"[43].

• *Privacidad como la configuración predeterminada*. Este principio parte de que "Lo predeterminado es lo que manda"[44], por eso se quiere que la protección de datos haga parte de lo predeterminado. Por lo tanto, se debe asegurar que "los datos personales estén protegidos automáticamente en cualquier sistema de IT dado o en cualquier práctica de negocios"[45].

• *Privacidad Incrustada en el diseño*. En línea con lo anterior, la privacidad y el debido tratamiento del dato debe formar parte del diseño y arquitectura del software, los dispositivos tecnológicos y la operatividad de las empresas y las organizaciones. Con esto se quiere que "la privacidad se convierte en un componente esencial de la funcionalidad central que está siendo entregada. La privacidad es parte integral del sistema, sin disminuir su funcionalidad"[46].

• *Funcionalidad total. "Todos ganan", no: "Si alguien gana, otro pierde"*. Con este principio se quiere recalcar que los negocios o las actividades de las organizaciones no son incompatibles y no deben plantearse unas en contra de otras, sino buscar un punto de equilibrio. Según Cavoukian, "Privacidad por Diseño busca acomodar todos los intereses y objetivos legítimos de una forma «ganar-ganar», no a través de un método anticuado de «si alguien gana, otro pierde», donde se realizan concesiones innecesarias"[47].

• Seguridad extremo-a-extremo. Protección del ciclo de vida completo. Si la seguridad se incorpora en los procesos desde el inicio, ello contribuye a garantizarla durante todo el ciclo de tratamiento de los datos personales.

[42] Cfr. Ann Cavoukian (2011), *Privacy by Design. Los 7 Principios Fundamentales.* Disponible en*: https://www.acc.com/chapters/euro/upload/7foundationalprinciples-spanish.pdf*

[43] *Ibidem*.

[44] *Ibidem*.

[45] *Ibidem*.

[46] *Ibidem*.

[47] *Ibidem*.

• *Visibilidad y transparencia. Mantenerlo abierto*. Se quiere que las promesas que se hagan a las personas sobre privacidad y tratamiento de datos se cumplan en la práctica y que se pueda verificar.

• *Respeto por la privacidad de los usuarios. Mantener un enfoque centrado en el usuario*. "Por encima de todo, la Privacidad por Diseño requiere que los arquitectos y operadores mantengan en una posición superior los intereses de las personas, ofreciendo medidas tales como predefinidos de privacidad robustos, notificación apropiada, y facultando opciones amigables para el usuario. Hay que mantener al usuario en el centro de las prioridades"[48].

c) *Del delegado de protección de datos*. El decreto exige a cada operador que designe "un encargado de protección de datos que acredite conocimientos especializados en la materia, que actuará de manera autónoma, imparcial e independiente[49]. Dicho delegado o encargado de protección de datos debe cumplir, entre otras, las siguientes funciones:

"1. Velar por el respeto de los derechos de los titulares de los datos personales respecto del tratamiento de datos que realice el operador.

"2. Informar y asesorar al operador en relación con las obligaciones que les competen en virtud de la regulación colombiana sobre privacidad y tratamiento de datos personales.

"3. Supervisar el cumplimiento de lo dispuesto en la citada regulación y en las políticas de tratamiento de información del operador y del principio de responsabilidad demostrada.

"4. Prestar el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos.

"5. Atender los lineamientos y requerimientos que le haga la Delegatura de Protección de Datos Personales de la Superintendencia de Industria y Comercio o quien haga sus veces"[50].

d) *Evaluación del impacto de tratamiento de datos personales*. Como lo mencionamos al referirnos al Reglamento europeo, la norma ordena a los operadores de servicios ciudadanos digitales que antes de iniciar la prestación de sus servicios, realicen un estudio que les permita evaluar el impacto de sus operaciones en el tratamiento de datos personales[51].

Dicha evaluación debe contener, por lo menos, lo siguiente:

[48] *Ibidem*.

[49] Cfr. Decr. 1314 de 2017, art. 2.2.17.6.4.

[50] *Ibidem*.

[51] Cfr. Decr. 1314 de 2017, art. 2.2.17.6.2.

"1. Una descripción detallada de las operaciones de tratamiento de datos personales que involucra la prestación de los servicios ciudadanos digitales y de los fines del tratamiento.

"2. Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.

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

"4. Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad, diseño de software, tecnologías y mecanismos que garanticen la protección de datos personales, teniendo en cuenta los derechos e intereses legítimos de los titulares de los datos y de otras personas eventualmente afectadas"[52].

4. Hong Kong

La guía de Hong Kong sobre *accountability* se titula "Implementing and Demonstrating Accountability"[53] y fue expedida el 11 de febrero de 2014 por la Oficina del Comisionado de Privacidad para Datos Personales de Hong Kong con la cooperación de Nymity. El objetivo de la guía es que las organizaciones puedan demostrar el cumplimiento del principio de *accountability* utilizando los criterios y lineamientos establecidos en la misma.

En términos generales la guía se estructura de la siguiente manera: (véase tabla de la página siguiente).

En la guía de *accountability*[54] se subrayan tres elementos principales. El primero es el de responsabilidad, debido a que solo una empresa responsable tiene un programa de gestión de datos (*Privacy Management Program*) para garantizar el cumplimiento del principio de *accountability*. El segundo elemento es el de manejo y monitoreo de los datos, debido a que debe haber un responsable que haga seguimiento al tratamiento de los datos personales para garantizar el cumplimiento del PIGD y, de fallar algo, será esa persona la responsable. Finalmente, el tercer componente está relacionado con tener soportes y evidencias de cómo se manejan los datos, qué se hace con estos y qué protocolos existen.

[52] *Ibidem*.

[53] El texto de la guía puede consultarse en: <*https://www.pcpd.org.hk/privacyconference 2014/files/9_booklet_guide.pdf*>

[54] Office of the Privacy Commissioner for Personal Data, Hong Kong. "Implementing and Demonstrating Accountability. Featuring the Nymity Privacy Accountability Management Framework and the Data Privacy Accountability Scorecard". Prepared for the International Conference on Privacy Protection in Corporate Governance. 11 February 2014. Web 13 abril.

Elementos para invertir en un programa de privacidad (Drivers for investing in a privacy program)	• Obligación legal y regulatoria. • Brecha de seguridad. • Cultura de protección de datos. • Ventajas competitivas.
Elementos de accountability en materia de privacidad de datos (Elements of Data Privacy Accountability)	• Responsabilidad. • Propiedad (*Ownership*). • Evidencia.
Responsabilidad demostrada en la práctica (Accountability in practice)	• Actividades de gestión de datos (Privacy Management Activities). • Actividades de gestión de datos en el contexto de *accountability* (Privacy Management Activities in the Context of Accountability).
Demonstrando la responsabilidad utilizando una lista de chequeo (Demonstrating Accountability Using a Scorecard)	• Ejemplo. Lista de chequeo de Nymity.
Acreditando el cumplimiento (Attesting Compliance)	• Utilizar la siguiente fórmula: % accountability = cantidad de actividades fundamentales evidenciadas / cantidad de actividades fundamentales

Tabla núm. 4. Estructura de la guía de Hong Kong sobre *accountability*.

Establecidos estos tres elementos, la guía procede a listar las actividades que se pueden realizar en el marco de gestión de datos para demostrar el cumplimiento del principio de *accountability*. Como primer elemento es importante que la organización tenga un programa efectivo de gestión de datos (*Effective Management Privacy Program*) donde haya dos tipos de actividades: las fundamentales para el manejo de los datos y las electivas, que son las recomendadas mas no requeridas[55]. A manera de ejemplo, la Guía establece que en el sector público una actividad fundamental es la de registrar las bases de datos con la autoridad de protección

[55] *Ibidem.*

de datos, mientras que una actividad electiva es la de integrar la privacidad a las prácticas en los medios de comunicación social[56].

La guía señala que en el programa de gestión de datos deben encontrarse dos clases de actividades: las periódicas, que se ejercen con cierta frecuencia, y las continuas, que están incorporadas en el día a día de la organización[57]. Adicionalmente, la guía establece dos clases de monitoreo de los datos: uno centralizado y otro descentralizado. En el centralizado, un equipo o una persona es responsable de todo lo relacionado con el tratamiento de datos, mientras que en el descentralizado, las decisiones y el monitoreo se delega en diferentes niveles de la organización[58].

Con el fin de que toda la gestión de los datos se haga de manera adecuada para cumplir con el principio de *accountability*, la Guía recomienda hacer un *scorecard* o un *checklist*. En este se deben identificar las actividades, los responsables de realizarlas, y los controles y procedimientos. Todo esto se debe hacer preferiblemente mediante pregunta cerrada cuya respuesta sea "si" o "no" para recolectar toda la evidencia o estadística necesaria en caso de que las autoridades quieran verificar el cumplimiento de la ley de protección de datos[59]. Este c*hecklist* sirve para calcular el puntaje de cumplimiento del principio de accountability de la empresa. La fórmula es la siguiente: % accountability = número de actividades fundamentales evidenciadas / número de actividades fundamentales[60]. Si el porcentaje es 100, significa que todo se ha cumplido a cabalidad. Así, las empresas pueden tener un registro del cumplimiento de su programa para ver en qué pueden mejorar y qué están haciendo bien.

5. Guía GECTI sobre implementación del principio de accountability en las transferencias internacionales de datos

El GECTI[61] de la Universidad de los Andes publicó una guía de accountability especializada en las transferencias internacionales de datos[62]. La misma no replica

[56] *Ibidem.*

[57] *Ibidem* .

[58] *Ibidem.*

[59] *Ibidem.*

[60] *Ibidem.*

[61] El Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática (GECTI) fue creado el 5 de octubre del 2001 en la Facultad de Derecho de la Universidad de los Andes (Bogotá, Colombia) con el fin de fomentar el trabajo multidisciplinario y establecer un puente entre la Universidad y la sociedad para procurar reflexiones y acciones en materia de la internet, la sociedad de la información y temas convergentes. La misión del GECTI consiste en hacer un aporte académico independiente sobre diferentes aspectos del ciberespacio, la economía digital y la realidad socio-tecnológica contemporánea, así como realizar investigaciones, consultorías, publicaciones y programas académicos de alto nivel especializados en derecho y tecnología. Página web: *https://gecti.uniandes.edu.co/*

[62] Cfr. Remolina Angarita, Álvarez Zuluaga, *Guía GECTI para la implementación del principio de responsabilidad demostrada -accountability- en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos*, *op. cit.*, págs. 1-58.

lo dicho en las guías precitadas para el tratamiento de datos en general sino que se centra en desarrollar orientaciones para materializar la responsabilidad demostrada cuando una organización envíe datos a otros países o, por ejemplo, utilice servicios de computación en la nube que normalmente involucran el flujo transfronterizo de información en la medida que los centros de datos (data centers) de los proveedores de dichos servicios se encuentran ubicados en muchas partes del mundo.

En la guía se hace referencia al tratamiento de datos personales como un asunto global y una actividad cotidiana en el ciberespacio, destacando que en la práctica las organizaciones están transfiriendo o transmitiendo datos personales permanentemente. Adicionalmente, destaca la importancia del buen gobierno de datos personales, la responsabilidad digital empresarial y responsabilidad jurídica de los directivos de una organización.

De otra parte, la guía GECTI advierte de la existencia de "Paraísos informáticos" que no solo son países sino empresas u organizaciones ubicadas en otros territorios que no tiene protección de datos o la que garantizan es muy baja. en el tratamiento de datos personales e "internet de las empresas" *–Internet of Corporations-*.

Luego se refiere a las transferencias y las transmisiones internacionales de datos personales recalcando los riesgos que generan esas actividades las empresas, organizaciones, entidades públicas así como a las personas (titulares de los datos) y la protección de sus derechos humanos.

En la guía se advierte que la SIC exige que para realizar transferencias internacionales de datos es imperativo adoptar medidas de accountability. En efecto, se recalca que para el caso de la República de Colombia mediante la Circular Externa 5 del 10 de agosto del 2017 de la Superintendencia de Industria y Comercio (SIC) —autoridad colombiana de protección de datos personales— ordenó lo siguiente en el parágrafo primero del numeral 3.2:

"Sin perjuicio de que las transferencias de datos personales se realicen a países que tienen un nivel adecuado de protección, *los responsables del tratamiento, en virtud del principio de responsabilidad demostrada, debe ser capaces de demostrar que han implementado medidas apropiadas y efectivas para garantizar el adecuado tratamiento de los datos personales que transfieren a otro país y para otorgar seguridad a los registros al momento de efectuar dicha transferencia*.

Como se observa, señala la guía "para transferir datos a otros países no es suficiente que el país de destino esté catalogado por la SIC como un país con nivel adecuado de protección, sino que además es necesario que el responsable del tratamiento pueda demostrar que ha tomado medidas adecuadas, útiles y prácticas para logra estos dos objetivos:

"1) Garantizar el adecuado tratamiento de los datos personales que transfieren a otro país.

”2) Conferir seguridad a «los registros al momento de efectuar dicha transferencia»”[63].

En concreto, para las transferencias internacionales de datos, la guía GECTI enuncia y desarrolla las siguientes recomendaciones:

• Verificar que está facultado para transferir o transmitir los datos personales a otro país.

• Determinar el mecanismo adecuado que utilizará para transferir o transmitir internacionalmente los datos personales.

• Establecer cómo se probarán las medidas de accountability para transferir los datos personales.

• Tener en cuenta los objetivos que se deben cumplir según la regulación de su país para transferir datos internacionalmente.

• Asegurar el cumplimiento de las finalidades que se deben alcanzar con las medidas de accountability.

• Crear estrategias para proteger los intereses de su organización.

• Adoptar medidas para no defraudar la confianza de sus clientes o de los titulares de los datos.

• Prever las transferencias ulteriores de datos personales.

• Incrustar la privacidad desde el diseño y por defecto en las transferencias internacionales de datos personales.

• Replicar medidas proactivas del tratamiento de datos personales a las transferencias internacionales de dicha información.

• Articular las herramientas de accountability en un contrato ajustado a las particularidades de cada transferencia.

• No olvidar que estas estas recomendaciones deben articularse con la guía de accountability de la autoridad de protección de datos.

De las anteriores recomendaciones nos parece importante que las entidades utilicen, entre otros, los contratos o convenios como mecanismo para acordar aspectos fundamentales de las transferencias y transmisiones internacionales de datos. En la guía GECTI, por ejemplo, se recomienda lo siguiente:

“Los contratos representan una alternativa jurídica para demostrar la implementación de medidas de accountability en las transferencias internacionales de datos. Aunque existen modelos de contratos[64] en esta materia, es crucial que el

[63] Cfr. Cfr. Remolina Angarita, Álvarez Zuluaga, *Guía GECTI para la implementación del principio de responsabilidad demostrada -accountability- en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos*, *op. cit.*, págs. 33-34.

[64] La Comisión de las Comunidades Europeas, por ejemplo, adoptó las decisiones 2001/497/CE, 2004/915/CE y 2010/78/CE mediante las que avala ciertas cláusulas contractuales tipo para la transferencia de datos personales. Las decisiones 2001/497/CE y 2004/915/CE sugieren modelos

contrato sea consistente con las peculiaridades y necesidades de cada organización. Así mismo, es relevante que el exportador de los datos trate de establecer si el receptor de los datos en otro país es una empresa u organización seria (no un paraíso informático) que cumplirá las obligaciones contractuales."

Para la redacción del contrato, tenga presente varios aspectos:

• La naturaleza jurídica de los datos que se exportarán a otro país. Según sea aquella (sensible, de menores de edad, privada, semiprivada, pública), pacte medidas especiales de protección. Recuerde, por ejemplo, que para el tratamiento de datos sensibles se exige una responsabilidad reforzada, es decir, mayores medidas de seguridad, mayores restricciones de acceso, uso y circulación.

• Las medidas de seguridad que debe cumplir el destinatario (importador) de los datos exportados a otro país.

• La cantidad de datos que se exportarán.

• ¿Cuáles son los derechos que el destinatario de la información o importador debe garantizar al titular del dato?

• ¿Cuáles son los principios del tratamiento de datos personales que el importador o destinatario de los datos debe observar o garantizar?

• ¿Quiénes podrán tener acceso a la información exportada?

• Los mecanismos para que el titular del dato pueda ejercer sus derechos de manera sencilla y expedita ante el destinatario de los datos exportados.

• Las finalidades para las cuales se transfiere los datos. Es muy importante dejar claro qué puede y qué no puede hacer el destinatario de los datos transferidos.

• ¿Cuál será el límite de tiempo durante el cual el destinatario de los datos transferidos podrá tratarlos?

• La ley de protección de datos que regirá el contrato. Será la ley del país del exportador de los datos o la del importador de estos. Si se quiere garantizar el principio de "continuidad de protección de datos" a que nos referimos en este documento, lo recomendable es que el contrato se rija por la ley de protección de datos del país desde donde se exportarán.

• La posibilidad o no de realizar transferencias ulteriores a otros países. Deje claro si los datos inicialmente transferidos a un país (A) pueden ser transferidos luego desde ese país (A) a otro país (B). En caso positivo, establezca las condiciones que se deben observar para dicho efecto.

---

de contratos cuando la administración de los datos personales pasa de un operador a otro que se encuentra en un país diferente, mientras que la Decisión 2010/78/CE comprende un esquema de contrato para aquellos casos en que la administración de la información está bajo responsabilidad de un operador que acude a un tercero ubicado en otro país para que se encargue del tratamiento de ellos.

• ¿Qué hacer para recuperar los datos transferidos y garantizar los derechos de los titulares de ellos cuando el destinatario de la exportación incumpla el contrato?

• ¿Quién o quiénes responderán ante la autoridad de protección de datos o los titulares de los datos por un eventual indebido tratamiento de la información exportada y por los daños y perjuicios causados?

• Cuál será la responsabilidad (conjunta o solidaria) del exportador y del importador de los datos frente al titular de estos por las eventuales vulneraciones de sus derechos o los daños y perjuicios causados?

• ¿Qué se hará con los datos una vez termine el contrato?" [65]

6. Programa Integral de Gestion de Datos Personales (PIGDP)

El Programa Integral de Gestión de Datos Personales (PIGDP) es el mecanismo operativo para realizar todo lo necesario con miras a garantizar el debido tratamiento de los datos personales. Como tal, es el principal instrumento para definir los mecanismos para poner en ejecución el principio de responsabilidad demostrada en las organizaciones.

El PIGDP consiste en un instrumento para lograr el buen gobierno corporativo en el tratamiento de datos personales, que redunde en beneficio de los titulares de los datos y de las entidades que los administran, porque les permite maximizar el uso de la información para cumplir sus cometidos constitucionales y legales en un escenario respetuoso de los derechos de las personas.

El PIGDP debe contener las políticas y los procedimientos que el responsable del tratamiento de los datos debe adoptar con el fin de promover buenas prácticas en materia de responsabilidad demostrada. Así, la existencia de un PIGDP le permite a las entidades demostrar que cumplen debidamente las regulaciones pertinentes sobre tratamiento de datos personales. Una entidad que cumple con su PIGDP no solo fortalece la confianza con sus clientes, empleados o ciudadanos sino que consolida una buena reputación empresarial o institucional. Adicionalmente, permite que las organizaciones exploten inteligentemente el uso de la información garantizando los derechos de las personas y, a la vez, generando condiciones para ser más competitivos en el mercado o en la sociedad.

Con el fin de elaborar un programa lo más completo posible, a continuación destacaremos los aspectos más importantes que se incluyen en los PIGDP de otras organizaciones con miras a determinar los aspectos nucleares que debe incluir el PMP. Para el efecto, nos referiremos a los PIGDP de estas organizaciones:

[65] Cfr. Remolina Angarita, Álvarez Zuluaga, *Guía GECTI para la implementación del principio de responsabilidad demostrada -accountability- en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos*, *op. cit.*, págs. 46-48.

- El Ombudsman de Manitoba (Canadá)
- The International Association of Privacy Professionals (IAPP)
- Nymity

Manitoba es una región en Canadá cuya oficina del ombudsman fue creada mediante el *Ombudsman Act* de 1970, que establece que es competencia del ombudsman investigar las quejas y reclamos que tengan las entidades gubernamentales con respecto a la administración. Adicionalmente, en el Freedom of Information and Protection of Privacy Act se le otorgó al ombudsman potestad para investigar las quejas de los titulares de los datos con respecto a cualquier decisión, acción o inacción, en el tratamiento de sus datos, de cualquier entidad pública[66]. Su PIGDP[67] se expidió el 13 de julio de 2017 y tiene como objetivo proveer una guía, paso a paso, para las entidades públicas sobre cómo implantar los programas integrales de gestión de datos con el fin de cumplir con el principio de responsabilidad demostrada con respecto a la protección de datos personales.

En términos generales, el PIGDP se estructura de la siguiente manera:

Compromisos Organizacionales (Organizational Commitment)	• Demostrar el cumplimiento de la alta gerencia. • Designación y empoderamiento de un oficial de privacidad. • Establecimiento de los mecanismos de reporte.
Controles del programa (Program controls)	• Inventario de bases de datos. • Políticas. • Respuestas a brechas de seguridad. • Capacitación. • Herramientas de evaluación de riesgos de privacidad y seguridad. • Transferencias de datos. • Comunicación transparente con titulares.
Evaluación y revisión continua (Ongoing Assessment and Revision)	• Plan de supervisión y revisión. • Revisar y evaluar los controles del programa.

Tabla núm. 5. Estructura del PIGDP de Manitoba (Canadá).

The International Association of Privacy Professionals (IAPP), por su parte, es una red de profesionales que se dedican a manejar riesgos y proteger datos

[66] Manitoba Ombudsman "About the Office". Web 2 mayo. <*https://www.ombudsman.mb.ca/info/about-the-office.html*>

[67] El texto del PIGDP de Manitoba puede consultarse en: <*https://www.ombudsman.mb.ca/uploads/document/files/privacy-management-program-guidelines-en.pdf*>

personales, y se ha convertido en la comunidad en materia de protección de datos más grande y completa, lo que los ha llevado a afirmar que son la única red en la que personas, herramientas e información global convergen para presentar las prácticas que requieren las organizaciones en materia de protección de datos para ser exitosas[68]. Su PIGDP[69] se elaboró en 2013, y tiene como propósito brindar todas las herramientas para la construcción de un PIGDP en todo tipo de entidades.

Grosso modo, el PIGDP se organiza de la siguiente manera:

Gerencia Estratégica (Strategic Management)	• Visión y misión de privacidad de la organización. • Desarrollar una estrategia de privacidad. • Estructura del equipo de privacidad.
Desarrollo e implementación de un marco de protección de datos (Develop and Implement a Framework)	• Marcos de referencia. • Desarrollar políticas de privacidad organizacionales, estándares o guías.
Evaluar (Assess)	• Modelo de evaluación. • Elementos fundamentales de evaluación (datos, sistemas y procesos).
Proteger (Protect)	• Manejo de los ciclos de datos. • Prácticas de seguridad de la información. • Diseño de privacidad (físico y tecnológico). • Análisis y evaluaciones.
Sustentar (Sustain)	• Monitorear. • Auditar. • Comunicar.
Respuesta (Respond)	• Requerimientos de información. • Cumplimiento legal. • Planeación de incidentes. • Manejo de incidentes.

Tabla núm. 6. Estructura del PIGDP de la IAPP.

Nymity es una compañía privada que se especializa en la elaboración de metodologías, *frameworks*, análisis y tecnologías de transferencia de información.

[68] International Association of Privacy Professionals (IAPP). "Your comprehensive global information privacy community and resource". Web 2 mayo. <*https://iapp.org/about/*>

[69] El texto del PIGDP de la IAPP puede consultarse en: < *https://books.google.com.co/books/about/Privacy_Program_Management.html?id=GI8zkwEACAAJ&redir_esc=y*>

Para esto, cuenta con un grupo de profesionales en materia de privacidad con el fin de ayudar a organizaciones (públicas y privadas) a cumplir con la legislación vigente en materia de protección de datos[70]. Su PIGDP[71] se actualizó en febrero de 2018 y tiene como propósito servir de guía para las actividades de manejo de datos con medidas técnicas y organizacionales, para cumplir con el principio de *accountability*.

A grandes rasgos, el PIGDP se organiza de la siguiente manera:

Estructura de Gobernanza (Maintain Governance Structure)	• Oficial de privacidad. • Asignación de responsabilidades en materia de privacidad de los datos en la organización. • Reportes internos sobre el manejo de privacidad. • Mantener una estrategia de privacidad. • Implantar una misión de privacidad.
Inventario de Datos Personales y mecanismos de transferencia (Maintain Personal Data Inventory and Data Transfer Mechanisms)	• Inventario de datos personales. • Registro de bases de datos ante la autoridad competente. • Documentación de transferencias de datos (internacionales o no).
Política interna de privacidad de datos (internal data privacy policy)	• Documentar las bases legales para procesar los datos personales. • Integrar la ética en el procesamiento de datos (Códigos de Conducta).
Integrar la privacidad de datos en las operaciones (Embed Data Privacy into Operations)	• Procedimientos para la recolección y el uso de datos. • Procedimientos para garantizar la calidad de la información. • Procedimientos para obtener consentimiento válido. • Procedimientos para la destrucción segura de los datos personales.
Programas de capacitación y concientización (Training and Awareness Program)	• Capacitaciones específicas para cada labor desempeñada. • Conducir entrenamientos regulares. • Incorporar la protección de datos en los entrenamientos operacionales . • Boletín interno de privacidad.

[70] Nymity. “About Nymyty: Empowering Privacy Officers Around the World”. Web 2 mayo. <*https://www.nymity.com/about/*>

[71] El texto del PIGDP de Nymity puede consultarse en: <*https://www.nymity.com/wp-content/uploads/Nymity-Privacy-Management-Accountability-Framework.pdf*>

Manejar riesgos de seguridad de la información (Manage Information Security Risk)	• Medidas técnicas de seguridad. • Medidas para encriptar datos personales. • Medidas para mantener el uso aceptable de la información. • Estrategias de prevención en caso de pérdida o destrucción involuntaria de datos personales.
Manejar riesgos provenientes de terceros (Manage Third-Party Risk)	• Revisar contratos con terceros que involucren transferencia de datos. • Mantener políticas para el uso de la nube. • Realizar debida diligencia alrededor de manejo de datos antes de firmar contratos con proveedores.
Notificaciones (Maintain Notices)	• Notificaciones sobre recolección de datos. • Notificaciones en contratos y términos. • Tener libretos para que los empleados utilicen al explicar al titular el tratamiento de sus datos.
Responder a peticiones y reclamos de individuos (respond to Requests and Complaints from Individuals)	• Procedimientos para responder a quejas y denuncias. • Mecanismos para cambio y corrección de datos personales.
Monitorear nuevas prácticas operacionales (Monitor for New Operational Practices)	• Integrar la privacidad por diseño (Privacy by Design) en las operaciones de tratamiento de datos.
Mantener programa de manejo de brechas de privacidad (Maintain Data Privacy Breach Management Program)	• Monitorear y reportar brechas a la privacidad. • Conducir pruebas para encontrar brechas e incidentes a la privacidad de los datos.
Monitorear prácticas de tratamiento de datos (Monitor Data Handling Practices)	• Auto evaluación de gestión de datos. • Auditorías internas. • Contratar un tercero neutral para conducir las auditorías.
Rastrear los criterios externos (Track External Criteria)	• Identificar requerimientos de cumplimiento en materia de tratamiento de datos. • Participar en conferencias sobre el tema. • Tener un reporte sobre leyes y regulaciones nuevas en materia de tratamiento de datos personales.

Tabla núm. 7. Estructura del PIGDP de Nymity.

En términos generales se observa que los PIGD son un reflejo de lo establecido en las guías de *accountability*[72] que mencionamos en la sección anterior. A continuación, realizaremos un análisis comparado de esos PIGDP y posteriormente presentaremos una lista de control (*checklist*) de los elementos básicos de un PIGD.

7. Análisis comparado de programas de gestión de datos

De la revisión comparativa de los PIGDP de Manitoba[73], The International Association of Privacy Professionals (IAPP) y Nymity se pueden extraer los siguientes componentes: (véase tabla de la página siguiente).

A continuación nos referiremos sucintamente a los siguientes aspectos: (i) compromiso de la organización dentro de una estructura de gobernanza en datos personales; (ii) controles del programa integral de gestión de datos personales; (iii) evaluación y revisión continua, y (iv) demostrar el cumplimiento de la ley.

A) *Compromisos organizacionales*

Dentro de estos compromisos se pueden citar los siguientes que agrupamos en estos términos: (i) apoyo de la alta gerencia o directivos de la organización; (ii) designación y empoderamiento de un oficial de privacidad o de tratamiento de datos personales; (iii) creación de una oficina de privacidad o de tratamiento de datos, y (iv) uso de mecanismos de reporte de cumplimiento.

En las siguientes líneas no referiremos brevemente a los mismos:

a) *Apoyo de la alta gerencia o directivos de la organización*. Es muy importante que la alta gerencia o los funcionarios jerárquicamente superiores, abierta y sinceramente se comprometan con el cumplimiento del PIGDP. Para esto, hay diversas maneras en las que pueden mostrar su apoyo. Por ejemplo, los directivos de la organización pueden:

[72] A las guías mencionadas se suma la siguiente que se refiere a los aspectos de *accountability* cuando se realice circulación transfronteriza de datos. Este texto fue referente y usado para efectos de la realización de algunas tablas de esta obra y la parte teórica sobre el principio de accountability: Remolina Angarita, Álvarez Zuluaga, *Guía GECTI para la implementación del principio de responsabilidad demostrada -accountability- en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos, op. cit.*, págs. 1-58. Disponible en: *https://gecti.uniandes.edu.co/index.php/accountability*

[73] El Ombudsman de Manitoba, región en Canadá, realizó una guía de PMP para accountability en el sector público de Manitoba, por lo cual al tratar específicamente el sector público consideramos ponerla como ejemplo. Vale aclarar que esta guía es una réplica de los programas realizados en conjunto por el Comisionado de Privacidad de Canadá y las Oficinas de Información y Privacidad del Comisionado para Alberta, la Columbia Británica, y Nova Scotia. Por lo que debe dar una orientación de lo que son los requisitos de gestión de datos en Canadá.

		Manitoba	IAPP	Nymity
COMPROMISO ORGANIZACIONAL	Compromiso y apoyo de la Alta Gerencia	✓	✓	✓
	Designación y empoderamiento de un Oficial de protección de datos	✓	✓	✓
	Oficina de protección de datos	**X**	✓	✓
	Establecer mecanismos de reporte de cumplimiento	✓	✓	✓[74]
	Carta de declaratoria de la misión de privacidad	X	X	✓
CONTROLES DEL PROGRAMA	Inventario de datos personales	✓	✓	✓
	Políticas	✓	✓	✓
	Procedimientos de respuesta en caso de violación a la seguridad y privacidad	✓	✓	✓
	Capacitación de funcionarios	✓	✓	✓
	Herramientas para evaluar el riesgo de privacidad y seguridad	✓	✓	✓
	Gestión de proveedores de servicios, gestor de información y acuerdos de investigación	✓	✓	✓
	Comunicación externa	✓	✓	✓
EVALUACIÓN Y REVISIÓ CONTINUA	Desarrollar un plan de supervisión y revisión	✓	✓	✓
	Evaluar y revisar los controles del programa según sea necesario	✓	✓	✓
	Mantenerse informado sobre tratamiento de datos personales	X	X	✓
DEMOSTRAR EL CUMPLIMIENTO	Acreditar cumplimiento de la ley	X	X	X

Tabla núm. 8. Comparación de PIGDP de Manitoba, IAPP y Nymity.

[74] Proponen que los mecanismos sean a internos, externos y a accionistas.

• Nombrar un oficial de privacidad y apoyarlo en el desarrollo de su labor.

• Proveer los recursos necesarios para que el programa de gestión de datos pueda operar.

• Monitorear el PIGDP[75].

• Exigir a los funcionarios de la organización el cumplimiento del PIGDP.

• Liderar y promover una cultura de privacidad y debido tratamiento de datos personales en la entidad[76].

b) *Designación y empoderamiento de un oficial de privacidad o de tratamiento de datos personales*. El oficial de privacidad es la persona encargada de estructurar, diseñar y manejar el PIGDP, que comprende todo lo relacionado con procedimientos, capacitaciones, monitoreo, documentaciones, supervisión y evaluaciones del programa[77].

El oficial de privacidad debe poder establecer, implantar y monitorear los programas de control de privacidad, a la vez que debe garantizar la protección de los datos personales en todas las funciones que realiza dicha entidad[78].

Es relevante que las entidades asignen al oficial de privacidad la responsabilidad de cumplir el PIGDP, y que se le empodere de autoridad para que pueda cumplir su función y dar órdenes a los funcionarios dentro de la organización para todo lo relacionado con el tratamiento de datos personales.

c) *Creación de una oficina de privacidad o de tratamiento de datos*. En algunos casos, la designación del oficial de privacidad no es suficiente porque la organización o entidad es muy grande y maneja un número exorbitante de datos personales. En esas situaciones es recomendable que haya una oficina de privacidad, que dirija el oficial de privacidad, donde haya funciones y recursos asignados, claros y concretos.

Esa oficina debe tener una estructura organizacional que permita monitorear el cumplimiento del programa de gestión de datos y fomentar una cultura de protección de datos en la organización. Es crucial que mediante esa oficina se articule todo lo necesario para garantizar que la protección de datos se encuentre regulada y protocolizada en cada función de la entidad donde se traten datos personales[79].

d) *Uso de mecanismos de reporte de cumplimiento*. Deben establecerse ciertos mecanismos que permitan que la alta gerencia o el funcionario con mayor jerarquía y el oficial de privacidad puedan estar informados del cumplimiento de lo

[75] Ombudsman Manitoba "Guidelines for Implementing a Privacy Management Program for Privacy Accountability in Manitoba's Public Sector". Web 8 abril.

[76] *Ibidem*.

[77] *Ibidem*.

[78] *Ibidem*.

[79] *Ibidem*.

establecido en el PIGDP con miras a que puedan saber cómo está funcionando el programa para identificar sus fallas y proceder a su inmediata corrección.

Los mecanismos de reporte deben ser claros con el fin de que los empleados que manejan o trabajan con los datos personales sepan cómo proceder cuando ocurre un grave incumplimiento del PIGD y ante quién comunicarlo. Es recomendable incluir una serie de tests y reportes sobre los resultados que arrojan los reportes de cumplimiento, para así tener la estadística del progreso de la entidad en dicha materia[80]. Igualmente, deben instaurarse mecanismos para que los que tratan datos personales sepan en qué formato tomar las quejas de los individuos titulares de los datos cuando estos consideren que se les han vulnerado sus derechos[81].

e) Carta de declaratoria de la misión de privacidad. Esta carta es una especie de hoja de ruta mediante la cual las entidades establecen la misión de su gestión relacionada con los datos para que el equipo humano de la organización se sintonice y enfoque a cumplirla[82].

Aunque pueda pensarse que se trata de algo simbólico, este tipo de manifestaciones busca lograr mayor compromiso de todo el equipo de la organización y, a la vez, generar mayor confianza a los titulares de los datos porque muestra la transparencia de la entidad respecto del tratamiento de los datos personales.

B) *Controles del programa*

Dentro de los controles del PIGDP es usual que se recurra a los siguientes: (i) realización de un inventario de bases de datos personales; (ii) definición de políticas de tratamiento de datos personales; (iii) establecimiento de procedimientos de respuesta en caso de violación a la seguridad y privacidad; (iv) capacitación de funcionarios; (v) herramientas para evaluar el riesgo de privacidad y seguridad; (vi) reglas para el suministro de información a terceros; (vii) transparencia y comunicación externa.

a) *Realización de un inventario de bases de datos personales*. La entidad u organización debe crear un inventario de bases datos personales en el que establezca qué clase de datos tiene bajo su custodia o control. De igual manera, debe determinar si tiene bajo su responsabilidad datos sensibles y dónde y con qué controles de seguridad se encuentra almacenada dicha información[83]. Finalmente, es de gran relevancia que la entidad considere delimitar los propósitos para los que fueron recolectados y utilizados los datos, con el fin de establecer si se le da un uso adecuado a dicha información.

[80] *Ibidem*.

[81] *Ibidem*.

[82] Nymity. "Privacy Management Accountability Framework". Web 9 abril.

[83] Ombudsman Manitoba "Guidelines for Implementing a Privacy Management Program for Privacy Accountability in Manitoba's Public Sector". Web 8 abril.

El inventario debe ser actualizado permanentemente de manera que la entidad pueda saber en todo momento cuál es la información que trata bajo su responsabilidad y conocer quiénes dentro de la organización, acuden y usan los datos personales. Sin un inventario de bases de datos el Responsable se expone a que reine la anarquía en la organización en materia de manejo de los datos personales.

b) *Definición de políticas de tratamiento de datos personales*. Las entidades deben instaurar políticas para abordar ciertos problemas a los que se pueden enfrentar en el tratamiento de datos personales. Por un lado, deberían listar los requerimientos para la notificación de la recolección del dato al titular, estableciendo el propósito del uso de los datos y facilitándole un formato de consentimiento.

A título enunciativo, las políticas deberían establecer procedimientos claros y concretos para:

• Garantizar la calidad de la información.

• Poner en práctica la actualización, supresión o modificación de los datos personales.

• Fijar plazos de retención (almacenamiento) y destrucción de los datos.

• Garantizar la seguridad de los datos.

• Evitar el uso indebido de los datos personales.

• Atender debida y oportunamente las consultas y reclamos de los titulares de los datos.

• Reaccionar oportuna, inteligente y eficientemente frente a incidentes de seguridad mediante el establecimiento de planes de respuesta en caso que sucedan esas situaciones.

c) *Establecimiento de procedimientos de respuesta en caso de violación a la seguridad y privacidad*. Todas las organizaciones (públicas o privadas) deben establecer procedimientos en caso de que haya una violación a la seguridad y privacidad de los datos. Para ello, deben demarcar los medios y procesos para el manejo de dicha violación y a la vez identificar la persona encargada dentro de la entidad de manejar todo el proceso relacionado con la violación a la privacidad y seguridad del tratamiento de datos.

Es relevante que se tenga absoluta claridad sobre la persona responsable de reportar las violaciones, bajo qué formato, y cómo se buscará proteger los demás datos cuando ocurre una brecha de seguridad. En este orden de ideas deben fijarse con antelación los planes para dar respuesta a los incidentes de seguridad.

d) *Capacitación de funcionarios*. Se recomienda que las entidades capaciten a sus funcionarios en materia de tratamiento y protección de datos. Estas capacitaciones no deben ser ocasionales sino permanentes y oportunas (antes y durante el tratamiento de los datos personales).

La capacitación debería ser aún más especializada para aquellos funcionarios que directamente manipulan o trabajan con dicha información. Para ello, se les debe explicarl las políticas, herramientas y procedimientos previstos por la organización, de manera apropiada y efectiva, de tal modo que sin tener un conocimiento legal sobre el tema puedan entender cuál es su función.

Es crucial y estratégica la concientización del equipo humano de la organización respecto de su responsabilidad y las consecuencias por el debido o indebido tratamiento de datos personales.

e) *Herramientas para evaluar el riesgo de privacidad y seguridad*. También es fundamental que la entidad tenga herramientas que le ayuden a establecer el nivel de riesgo (alto, medio o bajo) que involucra el tratamiento de datos personales y la seguridad de los datos personales cada que haya un nuevo proyecto, traslado de datos, uso de datos, y nuevas plataformas tecnológicas, con el fin de tener siempre un perfil de riesgos actualizado[84].

f) *Reglas para el suministro de información a terceros*. Es necesario que el PIGDP prevea un capítulo sobre los procedimientos para la transferencia de información a un proveedor o a otra entidad en desarrollo de sus funciones, para garantizar que no haya uso indebido de la información recibida de los titulares[85].

g) *Transparencia y comunicación externa*. Es relevante, en especial cuando se trata de una entidad pública, que haya comunicación transparente con los titulares de los datos. En este sentido, se les debe informar sus derechos y cómo pueden ejercerlos. De igual manera, se les debe explicar las prácticas de recolección de datos de la entidad y una vez cuenten con toda la información se les debe pedir su consentimiento, en los casos que sea necesaria, para que dichos datos puedan ser tratados por la organización.

Para lograr lo anterior es recomendable que se informe o comunique a los titulares de los datos y a la sociedad en general las políticas de privacidad y tratamiento de datos de la entidad.

C) *Evaluación y revisión continua*

Dentro de este ítem normalmente se involucran estos aspectos: (i) desarrollar un plan de supervisión y revisión; (ii) evaluar y revisar los controles del programa según sea necesario, y (iii) mantenerse informado sobre la regulación respecto del tratamiento de datos personales.

[84] Nymity. “Privacy Management Accountability Framework”. Web 9 abril.

[85] Ombudsman Manitoba “Guidelines for Implementing a Privacy Management Program for Privacy Accountability in Manitoba’s Public Sector”. Web 8 abril.

a) *Desarrollar un plan de supervisión y revisión*. Quien sea nombrado oficial de privacidad al interior de la entidad, debe desarrollar y vigilar el plan de monitoreo y evaluación de la efectividad del programa de privacidad cubriendo todas sus herramientas y procedimientos.

Dicho plan debe ser actualizado periódicamente (semestral o anualmente) para que siempre refleje el estado actual de las políticas en materia de privacidad y protección de datos.

b) *Evaluar y revisar los controles del programa según sea necesario*. Esta tarea también le corresponde al oficial de privacidad, y está relacionada con verificar, por un lado, que la información personal de los titulares esté actualizada y que los nuevos datos recolectados cumplan con todo lo establecido en la ley y en el programa de gestión de datos. Por otra parte, el oficial debe revisar las políticas que se tienen y mirar si hay nuevas guías o mejores prácticas internacionales que valga la pena implantar al interior de la entidad.

Cuando sea requerido, debe actualizar los procedimientos en caso de brechas en la seguridad de la información, teniendo en cuenta lo aprendido en experiencias anteriores.

c) *Mantenerse informado sobre la regulación respecto del tratamiento de datos personales*. Un aspecto importante sobre el cumplimiento del principio de *accountability* es mantenerse informado sobre las regulaciones recientes en materia de tratamiento de datos personales. Para ello hay varias opciones. Por un lado, contratar servicios legales que envíen reportes semanales o mensuales de cualquier novedad que haya con respecto a tratamiento de datos personales[86]. Por otro, participar en conferencias y foros que traten los temas relacionados con el tratamiento de los datos, para así estar a la vanguardia en lo que concierne a tan delicado tema.

D) *Demostrar el cumplimiento de la ley*

No basta realizar actividades para cumplir debidamente las leyes sobre tratamiento de datos; también es necesario probar todo lo que se hizo. Por lo tanto es relevante pensar no solo en hacer las cosas, sino establecer cómo probar todo lo que se ha hecho.

En suma, es cardinal pensar en los requerimientos probatorios de las regulaciones para acreditar la debida diligencia y el cumplimiento del correcto tratamiento de los datos.

[86] Nymity. “Privacy Management Accountability Framework”. Web 9 abril.

8. Resumen de los principales elementos de un programa de gestión integral de datos

Visto todo lo anterior, a continuación sintetizamos los aspectos medulares que deben tenerse presente para la definición del PIGDP:

A) *Compromiso de la organización dentro de una estructura de gobernanza en datos personales*

- *Compromiso de los superiores jerárquicos dentro de la entidad*
  - Crear, de ser pertinente, una Oficina de protección de datos personales
  - Nombrar un oficial de datos personales
  - Distribuir recursos del presupuesto para llevar a cabo las labores relacionadas con la protección de datos personales
  - Mantener canales abiertos de comunicación entre el oficial de datos personales y los superiores jerárquicos
  - Crear una Carta dentro de la entidad que contenga la misión y visión en materia de protección de datos dentro de la organización para que sirva de hoja de ruta.
  - Exigir reportes de cumplimiento del programa de privacidad
- *Designación de un oficial de protección de datos*
  - Delimitar las labores del oficial para que se incluyan las de realizar procedimientos, capacitaciones, monitoreo y evaluaciones del programa de protección de datos.
  - El oficial debe servir de enlace y coordinador con las demás áreas de la organización para garantizar la aplicación transversal del programa de gestión de datos.
  - Realizar capacitación general para los demás empleados de la organización.
- *Mecanismos de reporte de cumplimiento*
  - Definir la estructura de los reportes.
  - ¿Qué empleado es responsable de estos?
  - ¿Cómo se realizan?
  - ¿Cuánto tiempo tiene para realizarlos?
  - Documentar el proceso de generación de portes.
  - Guardarlos.
  - Sacar reportes con conclusiones sobre lo recolectado en los diversos reportes de cumplimiento.
  - Informar sobre el estado del programa de gestión de datos.

B) *Controles del programa de gestión de datos*

- *Inventario de datos personales*
  - Establecer cuántas bases de datos hay en la organización.
  - Clasificar la información de esa base de datos:
  - Información sensible.
  - Información pública.
  - Información confidencial.
  - Determinar qué controles de seguridad hay para los diferentes datos almacenados.
  - Registrar las bases de datos en la SIC en caso de aplicarse.
  - Mantener documentación sobre el flujo de datos de una base de datos a otra.
  - Mantener todos los documentos donde se otorga consentimiento para el uso de los datos y organizarlos en un archivo.
  - Crear y organizar un archivo donde estén todos los datos que puedan ser manipulados en pro del interés general sin necesidad de consentimiento expreso.
  - Mantener un archivo con el uso para el que se pidieron los datos con el fin de monitorear que sí se les esté dando el uso adecuado.
- *Políticas*
  - Establecer un formato con los requerimientos para la notificación de la recolección del dato al titular donde se liste el propósito del uso de sus datos.
  - Establecer un formato de consentimiento para el titular de los datos personales.
  - Procedimiento sobre cambio y actualización de los datos personales, con sus respectivos formatos.
  - Manual de retención y destrucción de datos personales en el que se listen los procedimientos.
  - Políticas de salvaguarda de datos:
  - Administrativas.
  - Técnicas.
  - Físicas.
  - Procedimiento para recibir las quejas, denuncias y reclamos de los titulares de datos con respecto a su uso.

- Implantar cláusulas vinculantes sobre mecanismos de transferencia de información y confidencialidad en todos los medios contractuales de la organización.

➢ *Procedimientos de respuesta en caso de ocurrir brechas de seguridad y privacidad*

- Identificar un responsable del manejo e identificar incidentes y vulneraciones de los sistemas de información.
- Mantener mecanismos para comunicarle a los Titulares afectados el incidente, sus consecuencias, y proporcionar herramientas para mitigar el daño.
- Instaurar un plan de respuesta ante una brecha o incidente de seguridad.

➢ *Capacitación de funcionarios*

- Tener una capacitación generalizada para todos los funcionarios de la entidad.
- Realizar una capacitación más específica para aquellos funcionarios que vayan a manipular directamente los datos.
- Realizar periódicamente un entrenamiento para actualizar a los funcionarios en la política de protección de datos.
- Asegurarse de que en la comunicación interna haya una sección de privacidad y protección de datos donde se vaya publicando información para refrescarle a los empleados sus obligaciones en materia de tratamiento de datos.

➢ *Herramientas para evaluar el riesgo de privacidad y seguridad*

- Implantar un sistema de administración de riesgos con las siguientes etapas:
- Identificación del riesgo en cada proceso en el que se utilizan los datos personales en la entidad.
- Medir el riesgo identificando la posibilidad de que estos ocurran y cuál sería su impacto en caso de suceder.
- Tomar acciones para controlar y mitigar el riesgo, analizando si dichas acciones o controles serían suficientes, efectivos y oportunos. Para ello se propone clasificar los controles de la siguiente manera: manual, automático, discrecional, obligatorio, preventivo o correctivo[87].

[87] Esta clasificación sigue la propuesta por la Superintendencia de Industria y Comercio en su Guía de Accountability en materia de tratamiento de datos personales. Web 10 abril. <*http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf*>

- Monitorear los controles establecidos para verificar su eficacia.
- Cuando se hagan estudios de riesgos de seguridad dentro de la entidad, incluir los riesgos relacionados con el mal tratamiento de datos personales.
- Instalar mecanismos técnicos de seguridad como la encriptación de los datos personales.
- Conducir exámenes regulares para verificar que todos los controles de seguridad estén funcionando adecuadamente.

➢ *Gestión de proveedores de servicios, gestor de información y acuerdos de investigación*

- Tener un protocolo de manejo de datos personales que deban cumplir las entidades que intercambien información con la RNEC.
- Mantener procedimientos mediante los cuales se pueda atender casos de uso incorrecto de datos por parte de terceros con la información proveída por la entidad.
- Revisar los acuerdos de intercambio o cesión de datos personales para verificar que incluya todo lo necesario para garantizar una correcta gestión de datos personales.

➢ *Comunicación externa*

- Tener un procedimiento claro para informarle a los titulares de los datos cuáles son sus derechos y cómo pueden ejercerlos.
- Tener un modelo de carta en el que se le explique a los titulares las prácticas de recolección de datos de la entidad y se les solicite dar su consentimiento.
- Tener un manual de procedimientos internos para quejas, denuncias, y reclamos que tengan los titulares de los datos.

C) *Evaluación y revisión continua*

➢ *Plan de supervisión y revisión*

- Realizar un plan en el que se delimiten qué procedimientos se utilizarán para supervisar y revisar que se estén cumpliendo las disposiciones en materia de protección de datos.

➢ *Evaluación de los controles del programa de gestión de datos*

- Conducir evaluaciones de las bases de datos de la entidad para ver si cumplen con todos los requisitos.
- Conducir auditorías internas del programa de gestión de privacidad.
- Conducir análisis de las quejas, reclamos y denuncias con el fin de compilar en un reporte las conclusiones y el paso que se debe seguir para mejorar el tratamiento de datos personales.

- *Monitoreo de nuevas prácticas*
  - Conducir búsquedas de nuevas prácticas en materia de protección de datos para actualizar la política de gestión de datos de la entidad.
  - Actualizar los programas, protocolos, y herramientas según los cambios legales o los nuevos riesgos encontrados.

D*) Demostrar el cumplimiento*

- Acreditar el cumplimiento de la ley
  - Llevar una bitácora en la que la entidad pueda demostrarle a cualquier autoridad o a los titulares de los datos que está cumpliendo con lo establecido en la ley de protección de datos.

CONCLUSIONES

1. La democracia en nuestro Estado social y de derecho, implica, en cuanto hace a las instituciones políticas, una serie de engranajes en las facultades de los actores institucionales que integran el país, para lograr su efectivo ejercicio, una dinámica que se desenvuelve a través de la visualización de la realidad social, lo que significa unas garantías mínimas de respecto de un sistema jurídico, político y social.

2. La división de poderes y la función de gobernar mediante la división clásica entre el poder ejecutivo, poder legislativo y poder judicial, que en la Constitución Política de Colombia de 1991 se positiviza a partir de la idea de un solo poder público, contemplado en tres ramas que a su vez son órganos independientes unos de otros, que ejercen control recíproco y que al mismo tiempo colaboran entre ellos.

3. La Registraduría Nacional del Estado Civil es un organismo de rango constitucional autónomo, conforme a los artículos 113 y 120 de la Carta Política de la República de Colombia, que forma parte de la organización electoral. Su objeto es garantizar la transparencia y confiabilidad del proceso electoral y lo relativo a la identidad de las personas, contribuyendo así de forma directa con la realización del principio constitucional democrático, siendo neutral y objetiva.

4. La RNEC promueve la participación social de los ciudadanos colombianos, tiene como facultad la promoción y garantía de cada evento en la vida de los seres humanos que deba registrarse respecto de la situación civil de las personas en Colombia, lo que debe certificarse por medio de los instrumentos que garanticen su confiabilidad y seguridad plena en la identidad de las personas y, por ende, en sus datos personales.

5. Actualmente la RNEC es una de las instituciones más sólidas y no se puede concebir la vida democrática, desde el punto de vista electoral y registral de este país, sin los grandes aportes institucionales que durante más de 70 años ha producido esta institución para Colombia.

6. Todas las personas, independientemente de su origen, sexo, raza etc, son titulares del derecho a la intimidad, el cual hace referencia al ámbito personal de cada individuo como sujeto de derechos y obligaciones o de la familia como

núcleo esencial de la sociedad, es decir, que está compuesto por aquellos fenómenos, comportamientos, datos y situaciones que normalmente no son puestos en conocimiento de extraños. Lo íntimo, lo realmente privado y personal de los seres humanos es un derecho fundamental que lo faculta a no promulgar, publicar o dar a conocer a terceros, a no ser que por voluntad del titular trasciendan al dominio de la opinión pública.

7. El Estado tiene una doble carga: la primera nos indica que tiene un deber de respeto por el ejercicio del derecho, y, adicionalmente, la segunda indica que así como debe respetarlo también debe velar por que los demás respeten el ejercicio del derecho y brinden garantías para su pleno y efectivo ejercicio.

8. El núcleo esencial del derecho de *habeas data* consiste en garantizar que el titular de la información pueda conocerla, actualizarla o rectificarla.

9. La RNEC es uno de los principales administradores de datos del país, pues es quien administra los datos de las personas de nacionalidad colombiana y de los residentes en nuestro país, desde su origen, es decir el nacimiento (registro civil de nacimiento) hasta su final (registro civil de defunción), pero a su vez actúa como órgano constitucional autónomo dotado de *imperium*, con facultades que tienen que fundamentar su actuar desde el punto de vista constitucional de forma total.

10. La RNEC es una entidad de orden constitucional, autónoma e independiente de los órganos de las ramas del poder público, conforme al principio de legalidad, el cual plantea el cumplimiento de la Constitución Política, las leyes o tratados internacionales, sean normas nacionales o internacionales, convenios, acuerdos y reglamentos, cualquiera que sea su rango.

11. La seguridad y certeza jurídica, que se traduce en el principio de legalidad en el sentido de definir mediante la fundamentación de los actos de autoridad que gozan de *imperium*, que traducen las facultades de la RNEC en el ámbito misional y la definición en el ejercicio de los derechos plasmados en la Constitución, hacen de todo sistema la piedra de toque del sistema democrático.

12. La democracia se puede definir tanto por la adecuada división de los poderes y del actuar de los órganos constitucionales autónomos, que se traduce en las facultades que acatan los que gobiernan, como en el ejercicio de derechos de los gobernados.

13. Internacionalmente se ha identificado un grupo de postulados generales contentivos de las directrices centrales que inspiran el debido tratamiento de los datos personales. Estos principios son una serie de reglas concebidas para procurar que la recolección y uso de la información personal no afecte o lesione los

derechos de las personas. Su observancia o inobservancia permiten establecer si un tratamiento de datos se realiza debida o indebidamente.

14. Los principios sobre el tratamiento de datos personales son herramientas muy valiosas para garantizar, en la práctica, la efectiva protección de los derechos de los titulares de los datos personales frente al tratamiento de su información. Adicionalmente, dichos postulados se constituyen en un límite al tratamiento indebido de los datos personales y en instrumento hermenéutico para la correcta interpretación y aplicación de las leyes sobre tratamiento de datos personales.

15. Del estudio comparado de la normativa de Argentina, Costa Rica, Colombia, España, México, Perú y Uruguay se concluye lo siguiente: en primer lugar, las autoridades de protección de datos no han emitido instrucciones específicas sobre el tratamiento de datos para cumplir la función electoral y registral. No obstante, en el caso de España su regulación prevé normas particulares para dichas funciones. Lo mismo sucede en el caso de México, pero únicamente respecto de la función electoral y en un reglamento interno. En segundo lugar, solo en España y Colombia se ha emitido instrucciones para implantar el principio de responsabilidad demostrada. Finalmente, únicamente México cuenta con una norma especial para el tratamiento de datos personales en el sector público.

16. Garantizar la aplicación efectiva y práctica de lo que ordenan las normas sobre protección de datos es un reto permanente de cualquier organización. Aunque es importante, no es suficiente la expedición de una norma porque ellas no tienen efectos mágicos. Por eso, se deben concentrar esfuerzos para que los objetivos de las leyes sobre tratamiento de datos no sean formales sino reales y concretos de manera que las personas realmente se beneficien de ellas.

17. El principio de responsabilidad demostrada (accountability) cobra cardinal importancia para lograr ese propósito. Exige que los responsables y encargados del tratamiento implanten medidas apropiadas, efectivas y verificables que le permitan probar el correcto cumplimiento de las normas sobre tratamiento de datos personales. Dichas medidas deben ser objeto de revisión y evaluación permanente para establecer su eficacia en cuanto al cumplimiento y el grado de protección de los datos personales. Para el efecto, el Programa Integral de Gestión de Datos Personales (PIGDP) se constituye en un mecanismo operativo para materializar el debido tratamiento de los datos personales.

18. Los PIGDP son una herramienta para lograr buen gobierno corporativo en el tratamiento de datos personales, que redunde en beneficio de los titulares de los datos y de las entidades porque les permite maximizar el uso de la información para cumplir sus cometidos constitucionales y legales en un escenario respetuoso de los derechos humanos.

19. El principio de responsabilidad demostrada demanda menos retórica y más acción en el cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. Exige implantar acciones concretas por parte de las organizaciones, para garantizar el debido tratamiento de los datos personales.

20. El éxito en esta materia dependerá del compromiso real de todos los miembros de una organización pero, especialmente, de los directivos de las organizaciones ya que sin su apoyo franco y decidido todo esfuerzo será insuficiente para diseñar, implantar, revisar, actualizar y evaluar los programas de gestión de datos. Es necesario destinar recursos (económicos y humanos) para esta labor y que las dependencias de la organización trabajen armónicamente, ya que esto no es solo un asunto jurídico sino, ante todo, una cuestión de gestión gerencial y estratégica de gobierno corporativo.

21. El reto de las organizaciones frente al principio de responsabilidad (accountability) va mucho más allá de la mera expedición de documentos, porque en la práctica exige que se demuestre el cumplimiento real y efectivo cuando realizan sus funciones. Con este principio se quiere que los mandamientos constitucionales y legales sobre tratamiento de datos personales sean una realidad verificable y que redunden en beneficio de la protección de los derechos de las personas.

22. Particular importancia debe darse a las acciones preventivas en materia de tratamiento de datos, razón por la cual son cruciales las medidas tendientes a: (i) inculcar y consolidar en el equipo humano de una organización una cultura de debido tratamiento de datos personales. Poco se logra si los servidores públicos no son conscientes de la importancia del derecho de la protección de datos, ni saben que si tratan indebidamente los datos personales afectan los derechos humanos de las personas; (ii) promover el diseño de procesos y desarrollo de tecnologías que desde el principio tengan presente el debido tratamiento de datos como un factor relevante. En suma, se trata de implantar la "protección de datos desde el diseño y por defecto" con miras a que antes que se recolecte información y durante todo el ciclo vital de la misma, se adopten procedimientos y medidas preventivas de diversa naturaleza (tecnológica, organizacional, humana) para evitar vulneraciones al derecho a la protección de datos personales, así como fallas de seguridad o indebidos tratamientos de datos personales.

23. El principio de responsabilidad demostrada (*accountability*) ha sido incorporado en los principales documentos sobre tratamiento de datos personales de las siguientes entidades: la Organización para la Cooperación y el Desarrollo Económico (OCDE), el Foro de Cooperación Asia Pacífico (APEC), la Red Iberoamericana de Protección de Datos Personales (RIPDP), la Unión Europea, la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (CIAPDP) y la Organización de Estados Americanos (OEA).

24. De los documentos de dichas organizaciones que se analizaron, se observa que los primeros fueron emitidos en la década de los ochenta y posteriormente algunos fueron modificados para ampliar su contenido e incluir la obligación de estar en capacidad de probar que los mecanismos para cumplir las reglas sobre tratamiento de datos personales son útiles, adecuados y eficientes.

25. La RIPDP y la OCDE se destacan por describir aspectos concretos de lo que se debe hacer para materializar la aplicación de dicho principio en la práctica cotidiana de las organizaciones. La RIPDP sugiere mecanismos como los siguientes que el responsable debería adoptar para cumplir con el principio de responsabilidad: a) destinar recursos para la instrumentación de programas y políticas de protección de datos personales; b) implantar sistemas de administración de riesgos asociados al tratamiento de datos personales; c) elaborar políticas y programas de protección de datos personales obligatorios y exigibles en la organización del responsable; d) poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales; e) revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran; f) establecer un sistema de supervisión y vigilancia interna y externa, con auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales; g) crear procedimientos para recibir y responder dudas y quejas de los titulares; h) efectuar revisiones y evaluaciones de los mecanismos utilizados con miras a establecer su grado de eficacia y cumplir sus deberes sobre tratamiento de datos personales.

26. En el ámbito internacional se ha recomendado producir y utilizar medidas proactivas de protección de datos con miras a mejorar el cumplimiento de las normas sobre protección de datos, así como consolidar y fortalecer el debido tratamiento de datos personales en las organizaciones. Son instrumentos de este tipo, los siguientes: (i) privacidad desde el diseño y por defecto; (ii) designación de un oficial de privacidad o delegado de protección de datos; (iii) evaluación de impacto de privacidad o de protección de datos; (iv) realización periódica de programas de concientización, educación y formación en protección de datos personales; (v) poner en práctica auditorías independientes; (vi) adhesión a acuerdos de autorregulación; (vii) implantar planes de contingencia.

27. Las medidas proactivas de protección de datos son consistentes con el principio de responsabilidad demostrada y se constituyen en buenas prácticas para asegurar el debido tratamiento de datos personales. Como tales, deben formar parte de los programas integrales de protección de datos personales (PIGDP).

28. Del análisis de buenas prácticas en materia de responsabilidad demostrada en Argentina, Colombia, España, Perú, México y Uruguay se concluye que dicho

principio cobra enorme importancia para llevar la protección de datos personales al campo práctico y abandonar el escenario teórico. Sin embargo, falta mucho por recorrer en la mayoría de estos Estados, por lo cual no hay claros y completos desarrollos del principio de responsabilidad demostrada, y menos para el tratamiento de datos personales en el sector público.

29. Del estudio de Programas Integrales de Gestión de Datos, se establece, entre otras cosas, que la mayoría son reflejos y, en diversas ocasiones, copias de las guías de *accountability* creadas en Australia, Canadá, Colombia y Hong Kong, por lo que en la práctica no hay una verdadera diferencia entre una Guía de Responsabilidad Demostrada y un Programa Integral de Gestión de Datos.

30. No existe una fórmula única y estándar para implantar el principio de responsabilidad demostrada en las organizaciones. Este debe estar acompañado de medidas particularizadas según la realidad específica de cada organización y teniendo en cuenta, entre otros, el nivel de riesgos que involucra el tratamiento de datos personales.

31. Las organizaciones deben poner en práctica el PIGDP, teniendo en cuenta la disponibilidad de recursos, la naturaleza de los datos que trata en sus sistemas de información y los riesgos que el tratamiento de información personal implica para el titular y para los responsables. Por eso es necesario priorizar los aspectos en que se enfocarán las actividades que es preciso realizar: (i) consolidar internamente una cultura de debido tratamiento de datos personales enfocada en la formación y concientización permanente de su equipo humano respecto de las responsabilidades y riesgos que supone el tratamiento de datos personales; (ii) dar prioridad a los tratamientos de datos personales que impliquen mayores niveles de riesgo sistémico con la potencialidad de afectar de manera grave los derechos de los titulares de los datos o los objetivos de los responsables; (iii) fortalecer las medidas de seguridad de los datos personales especialmente aquellos que sean sensibles, privados y semiprivados; (iv) reforzar estrategias probatorias que demuestren las gestiones realizadas para garantizar el debido tratamiento de los datos personales; (v) garantizar la confidencialidad de los datos personales sensibles, privados y semiprivados.

32. Es muy importante garantizar un buen gobierno corporativo de tratamiento de datos y para ello designar un delegado de protección de datos que actúe de manera autónoma, imparcial e independiente. Dentro de sus principales funciones se encuentran las siguientes: (i) velar por el respeto de los derechos de los titulares de los datos personales en cuanto al tratamiento de datos y por la aplicación efectiva del PIGDP; (ii) servir de enlace y coordinador, con todas las áreas de la or-

ganización, para asegurar la aplicación transversal del PIGDP; (iii) coordinar la elaboración de un sistema de administración de riesgos asociados al tratamiento, monitorearlo y evaluarlo; (iv) presentar recomendaciones a las directivas de la organización para materializar la aplicación permanente del PIGDP en todas las actividades que impliquen tratamiento de datos personales; (v) crear un sistema único de información sobre las bases de datos y archivos de la organización, que permita tener control sobre ellas y contar con datos oportunos, fiables y de alta calidad; vi) eliminar la "anarquía" de administración de sistemas de información al interior de cada organización.

33. La correcta aplicación del principio de responsabilidad demostrada y el diseño y puesta en marcha de los programas integrales de gestión de datos, no solo redundará en beneficio de la protección de los derechos de los titulares de datos personales sino que beneficiará positivamente a las organizaciones porque les permitirá maximizar el uso inteligente de la información y consolidar su buena reputación empresarial o institucional.

34. Es crucial que los directivos de las organizaciones sean proactivos respecto del tratamiento de la información, de manera que por iniciativa propia se anticipen a eventuales problemas y adopten medidas estratégicas capaces de neutralizarlos o que les permitan a la organización explotar la información en un escenario competitivo, innovador y respetuoso de los derechos humanos.

BIBLIOGRAFÍA

García González, Aristeo: "La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado", en *Boletín Mexicano de Derecho Comparado*, num. (120), Ciudad de México, Universidad Nacional Autónoma de México, 2007.

Habermas, Jürgen (1989): *Identidades nacionales y postnacionales*, Madrid, Tecnos, 1989.

Remolina Angarita, Nelson: *Tratamiento de datos personales: aproximación internacional y comentarios a la ley 1581 de 2012*, Bogotá, Legis Editores, 2013.

— "Recolección internacional de datos: un reto del mundo postinternet", en *BOE – Boletín Oficial del Estado*, Madrid, 2015.

— "Accountability y compromiso gerencial en el tratamiento de datos personales, 24-III-2015", en *https://habeasdatacolombia.uniandes.edu.co/?p=1886*, (2).

— El principio de «accountability» en el gobierno Obama y en el contexto Iberoamericano 03-II-2015", en *https://habeasdatacolombia.uniandes.edu.co/?p=1804*.

Remolina Angarita, Nelson y Álvarez Zuluaga Luisa Fernanda: *Guía GECTI para la implementación del principio de responsabilidad demostrada -accountability- en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos*, Bogotá, Universidad de los Andes, Facultad de Derecho, GECTI, 2018, págs. 1-58. Disponible en: *https://gecti.uniandes.edu.co/index.php/accountability*

Tenorio, Adame Manuel: *De la relación entre las facultades registrales y los derechos, a través de la supremacía constitucional*, Bogotá, 2018.

— "*La protección de datos personales desde el derecho al acceso a la información y como derecho fundamental autónomo. El caso mexicano*, Bogotá, Universidad de los Andes, Facultad de Derecho, núm. 1, julio-diciembre de 2012.

- MinTIC: *Seguridad y privacidad de la información: controles de seguridad y privacidad de la información (Guía núm. 8)*. Versión 3.0.1 de 16 de marzo de 2016, en *https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf*
- Norma NTC: ISO/IEC 27001: 2013
- *Gestión de riesgo en la seguridad informática: facilitando el manejo seguro de la información en organizaciones sociales*, en *https://protejete.wordpress.com/gdr_principal/definicion_si/*
- Ministerio del Interior (2014): *Políticas de seguridad de la información: control de acceso.*
- Ministerio de Justicia y Derechos Humanos Perú: "Directiva de Seguridad de la Autoridad Nacional de Protección de Datos Personales".

- Office of the Australian Information Commissioner: "Australian Privacy Principles Guidelines". Privacy Act 1988.
- Office of the Privacy Commissioner for Personal Data, Hong Kong: "Implementing and Demonstrating Accountability. Featuring the Nymity Privacy Accountability Management Framework and the data Privacy Accountability Scorecard". Prepared for the International Conference on Privacy Protection in Corporate Governance. 11 febrero 2014.
- Office of the Privacy Commissioner of Canada: "Getting Accountability Right with a Privacy Management Program".
- Nymity: "Privacy Management Accountability Framework".
- Ombudsman Manitoba: "Guidelines for implementing a Privacy Management Program for Privacy Accountability in Manitoba's Public Sector".
- Superintendencia de Industria y Comercio: "Guía para la implementación del principio de Responsabilidad Demostrada (Accountability)".
- The International Association of Privacy Professionals: "Getting Accountability Right with a Privacy Management Program".

Argentina

Dirección Nacional de Protección de Datos Personales: Guía de Buenas Prácticas en Políticas de Privacidad para las Bases de Datos del Ámbito Público, Buenos Aires, 2008.

Ministerio de Justicia y Derechos Humanos, Presidencia de la Nación: "Información Legislativa", Web 18 mar.*http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/143831/norma.htm*.

España

Agencia Española de Protección de Datos: "El enfoque de riesgos en el Reglamento de Protección de Datos". Web. 1 abril. *https://www.agpd.es/blog/el-enfoque-de-riesgos-en-el-reglamento-general-de-proteccion-de-datos-ides-idPhp.php*.

Agencia Española de Protección de Datos: "Guía para una evaluación de impacto en la Protección de Datos Personales". Web. 8 abril *http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf.*

México

INAI: "Estudio para la elaboración de una guía con la metodología y procesos de gestión para el cumplimiento de las obligaciones en materia de protección de datos personales". Web. 5 abril. <*http://inicio.ifai.org.mx/DocumentosdeInteres/E1-Elab.pdf*>

INAI: "Principios y deberes en materia de protección de Datos Personales". Web. 6 abril. <*http://metabase.uaem.mx/bitstream/handle/123456789/2525/3%20Principios%20y%20deberes%20en%20materia%20de%20Protección%20de%20Datos%20Personales.pdf?sequence=1*>

Perú

Ministerio de Justicia y Derechos Humanos: "Directiva de Seguridad de la Autoridad Nacional de Protección de Datos Personales". Web 8 abril. <*https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-de-Directiva-de-Seguridad.pdf*>

Uruguay

Unidad Reguladora y de Control de Datos Personales: "Guía 4 Manejo de Datos Personales en la Administración Pública". Web 4 abril. <*http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_bp_ur_g_4.pdf*>

Guías de Accountability

Office of the Australian Information Commissioner: "Australian Privacy Principles Guidelines". Privacy Act 1988. Web 17 abril <*https://www.oaic.gov.au/resources/agencies-and-organisations/app-guidelines/APP_guidelines_complete_version_2_March_2018.pdf*>

Office of the Privacy Commissioner for Personal Data, Hong Kong:"Implementing and Demonstrating Accountability. Featuring the Nymity Privacy Accountability Management Framework and the Data Privacy Accountability Scorecard". Prepared for the International Conference on Privacy Protection in Corporate Governance. 11 February 2014. Web 13 abril. <*https://www.pcpd.org.hk/privacyconference2014/files/9_booklet_guide.pdf*>

Office of the Privacy Commissioner of Canada: "Getting Accountability Right with a Privacy Management Program". Web 15 abril. <*https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf*>

Superintendencia de Industria y Comercio: "Guía para la implementación del principio de Responsabilidad Demostrada (Accountability)". Web 10 abril. <*http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf*>

Programas de gestión de datos

Nymity: "Privacy Management Accountability Framework". Web 9 abril. <https://www.nymity.com/wp-content/uploads/Nymity-Privacy-Management-Accountability-Framework.pdf>

Ombudsman Manitoba: "Guidelines for Implementing a Privacy Management Program for Privacy Accountability in Manitoba's Public Sector". Web 8 abril. <*https://www.ombudsman.mb.ca/uploads/document/files/privacy-management-program-guidelines-en.pdf*>

The International Association of Privacy Professionals. "Getting Accountability Right with a Privacy Management Program". Web. 8 abril. <*https://iapp.org/media/pdf/knowledge_center/Canada-Getting_Accountability_Right(Apr2012).pdf*>

ORGANIZACIONES Y DOCUMENTOS INTERNACIONALES

Red Iberoamericana de Protección de Datos

- Estándares de protección de datos personales para los Estados Iberoamericanos (2017).

Unión Europea

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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).
- Protocolo adicional al convenio 108 del Consejo para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal y relativo a la transferencia de datos (2001 y 2018).
- Carta de los derechos fundamentales de la Unión Europea (2000) ;
- Convenio 108 del Consejo para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal (1981).

Organización de Estados Americanos

- Principios de la OEA sobre la privacidad y la protección de datos personales con anotaciones (2015).

Organización para la Cooperación y el Desarrollo Económico

- Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales (2013, 1980).

Conferencia Internacional de Autoridades de Protección de Datos y Privacidad

- Estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal —Resolución de Madrid— (2009).

Foro de Cooperación Económica Asia Pacífico

- Marco de privacidad APEC (2004).

Organización de las Naciones Unidas

- Principios rectores para la reglamentación de los ficheros computadorizados de datos personales (1990), adoptados por la Asamblea General de la ONU en su resolución 45/95, de 14 de diciembre de 1990.

EQUIPO CONSULTOR

Este libro fue fruto del trabajo de un equipo conformado por las siguientes personas cuya síntesis de su formación académica nos permitimos presentar a continuación:

Nelson Remolina Angarita. Doctor (Ph.D.) *Summa Cum Laude* en Ciencias Jurídicas de la Pontificia Universidad Javeriana (Bogotá, Colombia). Master of Laws, The London School of Economics and Political Sciences, Londres - Inglaterra. Especialista en Derecho Comercial y Abogado de la Universidad de los Andes. Director del GECTI –*Grupo de Estudios en internet, Comercio Electrónico, Telecomunicaciones e Informatica*— de la Universidad de los Andes y del Observatorio Ciro Angarita Barón sobre protección de datos personales. Ganador del Premio Protección de Datos Personales de Investigación 2014, conferido por la Agencia Española de Protección de Datos (AEPD) sobre trabajos originales e inéditos que traten acerca del derecho a la protección de datos en países iberoamericanos. Profesor Asociado y Director de la Especialización en Derecho Comercial de la Universidad de los Andes.

Manuel Tenorio Adame. Doctor (Ph.D) en Estudios Superiores de Derecho Constitucional de la Universidad Complutense de Madrid. Especialista en Derechos Humanos de la Universidad Complutense de Madrid. Especialista en Ciencia Política y Derecho Constitucional por el Centro de Estudios Políticos y Constitucionales en Madrid España. Diploma de Estudios Avanzados de la Facultad de Derecho de la Universidad Complutense de Madrid. Diplomado en Derecho Norteamericano por Georgetown University, Diplomado en Derechos Humanos por el Instituto Internacional de Derechos Humanos Estrasburgo, Francia. Abogado por la Universidad Anahuac del Norte de México. Director de la Especialización en Derecho Constitucional de la Universidad Sergio Arboleda. Miembro del GECTI.

Gustavo Quintero Navas. Doctor (Ph.D.) y Master (D.E.A.) en Derecho Público, Universidad de Nantes - Francia. Especialista en Derecho Administrativo, Universidad Externado de Colombia. Abogado, Universidad Santo Tomás de Bogotá. Profesor Asociado de la Universidad de los Andes. Miembro del GECTI.

María Mónica Pérez López. Especialista en Derecho Constitucional de la Universidad Sergio Arboleda (Sede Bogotá). Abogada de la Universidad Libre (Sede Bogotá).

Luisa Fernanda Álvarez Zuluaga. Abogada de la Universidad de los Andes. Miembro del GECTI.

Este libro se terminó de imprimir en los Talleres de Editorial Nomos, el día veintinueve de junio de dos mil dieciocho, aniversario del nacimiento de PIETRO BONFANTE (n. 29, VI, 1864 y m. 22, XI, 1932).

LABORE ET CONSTANTIA

EDITORIAL TEMIS
OBRAS JURÍDICAS

ISBN 978-958-35-1183-7

REGISTRADURÍA NACIONAL DEL ESTADO CIVIL

cedae Centro de Estudios en Democracia y Asuntos Electorales

REMOLINA ANGARITA CONSULTORES