Mayo / 2020

SERVICIOS CIUDADANOS DIGITALES

Y LAS NUEVAS OBLIGACIONES DE PROTECCIÓN DE DATOS EN COLOMBIA

Luis Fernando Cote Peña

SERVICIOS CIUDADANOS DIGITALES Y LAS NUEVAS OBLIGACIONES DE PROTECCIÓN DE DATOS EN COLOMBIA (DECRETO 620 DE 2020)

Por Luis Fernando Cote Peña[1]

RESUMEN:

Los servicios ciudadanos digitales en Colombia han tenido un desarrollo significativo en los últimos cinco años. Ello ha conllevado la aparición de la Agencia Nacional Digital y con ella el proceso de puesta en marcha de la carpeta digital ciudadana, demandando la expedición de nuevas normativas como el Decreto 620 de 2020 que subrogó el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015 "*Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones*". En el referido Decreto 620 de 2020, se ha traído al ordenamiento normativo colombiano, en materia de protección de datos, las obligaciones de realizar Evaluaciones De Impacto De Protección de Datos Personales – EIPD, e incluir la figura del Oficial de Protección de Datos y la práctica de Protección de Datos desde el Diseño y Por Defecto, las cuales ya estaban regladas en Europa y referidas en decisiones de la Superintendencia de Industria y Comercio. De cara a tales novedades, se estimó de importancia aportar desde este ensayo a precisar, por una parte, los destinatarios de las nuevas obligaciones normativas y, por la otra, ampliar la

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

dimensión conceptual de las mismas. Para tal propósito, se expondrá un primer apartado sobre los antecedentes que dieron origen al Decreto 620 de 2020, al que le proseguirá una presentación de los destinatarios de las nuevas obligaciones incorporadas en la norma y se finalizará con la descripción de las obligaciones que se estiman novedosas en el ordenamiento jurídico colombiano.

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

I- Antecedentes

Durante el Gobierno del presidente Juan Manuel Santos se dio inicio, en relación normativa, a la articulación entre los servicios estatales y las nuevas tecnologías, con el propósito de facilitar al ciudadano el relacionamiento con las entidades públicas. Para tal efecto, en el Plan Nacional de Desarrollo 2014-2018 denominado *Todos por un nuevo país*, aprobado mediante la Ley 1753 de 2015, se le atribuyó al Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en el artículo 45, la responsabilidad de expedir las normas reglamentarias necesarias, entre otras, para "*(…) Autenticación electrónica, (…) Integración de los sistemas de información de trámites y servicios de las entidades estatales con el Portal del Estado colombiano,* [y la] *Interoperabilidad de datos (…)*"[2] y, a partir de ellas, asegurar el acceso de los ciudadanos a una carpeta electrónica.

Posteriormente, en el propósito de poner en ejecución el Plan propuesto, se expidió el Decreto 1078 de 2015, Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, a través de cuyo art. 2.2.9.1.2.1 se fijaron cuatro componentes con los cuales se buscó promover la masificación del encuentro tecnológico Estado-Ciudadano, en desarrollo de la nueva estrategia trazada, esto es: 1. TIC en los servicios, 2. TIC para el Gobierno abierto, 3. TIC para la Gestión y 4. Seguridad y privacidad de la información.

Años más tarde, en medio de la pandemia del COVID-19, este último componente, es decir, la Seguridad y Privacidad de la Información, concebido como transversal

[2] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1753 de 2015, art. 45, num. c, e y j.

a los demás y en virtud del cual se busca "*(…) proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada*"[3], se ha visto especialmente requerido, como quiera que el Plan de Desarrollo del Gobierno de Iván Duque, *Pacto Por Colombia, Pacto Por la Equidad*, acogido mediante Ley 1955 de 2019, con ocasión del "*Pacto por la transformación digital de Colombia: Gobierno, empresas y hogares conectados con la era del conocimiento*"[4], se adentró en el propósito de lograr la inclusión digital de los colombianos, ya no solo de los actores públicos, sino de estos en su interoperatividad con los privados, a través de la masificación de la banda ancha que facilita entre otras "*(…) una relación más eficiente, efectiva y transparente entre los mercados, ciudadanos y Estado*"[5].

De hecho, en el mismo Plan de Desarrollo *Pacto Por Colombia, Pacto Por la Equidad*, al definirse los principios por los cuales se regirán los proyectos estratégicos de transformación digital, se advirtió que se daría "*(…) Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales; (…) Plena interoperabilidad entre los sistemas de información públicos que garantice el suministro e intercambio de la información de manera ágil y eficiente a través de una plataforma de interoperabilidad. Se habilita de forma plena, permanente y en tiempo real cuando se requiera, el intercambio de información de forma electrónica en los estándares definidos por el Ministerio TIC, entre entidades públicas. Dando cumplimiento a la protección de datos personales y salvaguarda de la información*" [6] (subrayado fuera de texto original); al igual que la "*(…) Inclusión y actualización permanente de políticas de seguridad y confianza digital*"[7] (subrayado fuera de texto original).

La razón de la relevancia que implicaba el componente de *seguridad de la información* para los propósitos del Gobierno Duque, estaba determinada, entre otras, por el marco normativo que desde el año 1991 se había incorporado en el artículo 15 de la naciente Constitución Política de Colombia, logrando su

[3] PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. Decreto 1078 de 2015, art. 2.2.9.1.2.1, num. 4.
[4] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1955 de 2019, art. 3, num. 7.
[5] Ibidem, art. 4.
[6] Ibidem, art. 147, num. 2 y 3.
[7] Ibidem, num. 11.

desarrollo posterior en la Ley 1266 de 2008 en lo que a Hábeas Data Financiero se trataba y, tardíamente, de manera posterior, en la Ley 1581 de 2012, ambas reglamentadas por el Decreto 1074 de 2015, los cuales se constituyen como las bases normativas de la protección de datos personales en el país.

Fueron estos los motivos por los cuales el Gobierno Nacional, al expedir el Decreto 620 de 2020 dirigido a seguir construyendo las líneas regulatorias del Sector de Tecnologías de la Información y las Comunicaciones, dedicó el capítulo 5 denominado *TRATAMIENTO DE DATOS PERSONALES, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN*, a la incorporación de las innovaciones trascendentes que adelante se presentan y que, siendo de carácter obligatorio, suman a la normativa existente ajustes al instituto jurídico del hábeas data, aún en fase de consolidación.

II- Obligados en el Ecosistema de Servicios Ciudadanos Digitales

Las disposiciones contenidas en el Decreto 620 del 2020 en materia de protección de datos, no son generales para todos los sujetos que tratan datos personales en los términos de la Ley 1581 de 2012. Su universo está determinado, fundamentalmente, por los denominados servicios ciudadanos digitales.

El universo de los obligados está constituido, en principio, por las entidades y organismos que conforman las ramas del Poder Público, los órganos autónomos e independientes del Estado y los particulares en cumplimiento de funciones administrativas o públicas, siempre que ejecuten actividades de aquellas que se enmarcan dentro de los denominados servicios ciudadanos digitales que están a cargo de la Agencia Nacional de Gobierno Digital - AND[8], entidad creada el 29 de diciembre de 2017 mediante documento privado, como una corporación sin ánimo de lucro, con carácter de asociación civil, de participación pública y naturaleza privada, adscrita al Ministerio de las Tecnologías y las Comunicaciones.

La misión que se le ha asignado a la AND, se describe en su sitio web como "*Promover, administrar y articular los procesos asociados a la prestación de Servicios Ciudadanos Digitales para la interacción entre los ciudadanos, empresas y entidades a través de medios electrónicos para mejorar la calidad de vida de los colombianos, y desarrollar las actividades de ciencia, tecnología e innovación*

[8] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Decreto 2106 de 2019, art. 9; en concordancia con PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. Decreto 1078 de 2015, art. 2.2.17.1.2.

asociadas a la creación de un ecosistema de información pública que brinde soluciones a las diferentes instituciones del Estado"[9].

Cabe destacarse que los servicios ciudadanos digitales se definen como "*(…) el conjunto de herramientas y procesos (Interoperabilidad, Carpeta Ciudadana y Autenticación Digital) que le permiten al ciudadano acceder de manera eficiente a los servicios y trámites del Estado a través de medios electrónicos*"[10].

Efectuadas las anteriores precisiones y conforme al Decreto 1413 del 25 de agosto de 2017 en concordancia con el Decreto 620 de 2020, resulta de importancia señalar que los actores del sistema de *servicios ciudadanos digitales* son los siguientes:

1. **Usuario:** "*Es la persona natural, nacional o extranjera titular de cédula de extranjería, o la persona jurídica, de naturaleza pública o privada, que haga uso de los servicios ciudadanos digitales*"[11].

2. **Articulador:** Agencia Nacional Digital. Es la "*(…) encargada de proveer y gestionar de manera integral los servicios ciudadanos digitales, además de apoyar técnica y operativamente al Ministerio de Tecnologías de la Información y las Comunicaciones para garantizar el pleno funcionamiento de tales servicios*"[12].

3. **Operador o Prestador de servicios ciudadanos digitales:** "*Es la persona jurídica que presta los servicios ciudadanos digitales en el marco de la ley y del presente título*"[13], esto es, las "*Entidades pertenecientes al sector público o privado, quienes, mediante un esquema coordinado y administrado por el Articulador, pueden proveer los servicios ciudadanos digitales a ciudadanos y empresas, siempre bajo los lineamientos, políticas,*

[9] AGENCIA NACIONAL DIGITAL. Nosotros. Rescatado de: https://and.gov.co/nosotros-3/
[10] Ibidem. Servicios ciudadanos digitales. Rescatado de: https://and.gov.co/servicios-ciudadanos-digitales/
[11] PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. Decreto 1078 de 2015, art. 2.2.17.1.4, num. 14.
[12] Ibidem, num. 2.
[13] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 1413 del 2017, art. 1.

guías, que expida el Ministerio de Tecnologías de la Información y las Comunicaciones"[14].

4. **Organismos y entidades establecidos en el artículo 2.2.17.1.2 del Decreto 620 de 2020:** Son los "*(…) sujetos obligados a la aplicación del presente título, todos los organismos y entidades que conforman las ramas del Poder Público en sus distintos órdenes, sectores y niveles, los órganos autónomos e independientes del Estado, y los particulares, cuando cumplan funciones administrativas o públicas*"[15].

5. **Autoridades del Sistema de Servicios Ciudadanos:** Son "*Las autoridades que tienen a su cargo las funciones de política, regulación, vigilancia y control sobre las actividades que involucran la prestación de los servicios ciudadanos digitales*"[16].

6. **Autoridad de Identificación:** Lo será la Registraduría Nacional del Estado Civil, como autoridad constitucionalmente facultada para la identificación de las personas.

7. **Aliado tecnológico**: "*Es la persona jurídica que apoya a la entidad pública, al particular con funciones públicas o particulares autorizados por la ley en todos los aspectos relacionados con las tecnologías de la información para el proceso de autenticación biométrica*"[17].

No obstante la advertencia anterior, se hace la anotación de que la falta de una disciplina en el ejercicio de la expedición normativa por parte de los generadores de aquellas, suscita confusiones terminológicas al buscar la coherencia conceptual en los elementos de definición como ocurre, por ejemplo, con los términos usados en el Decreto 620 de 2020 y el Decreto 1413 de 2017. Ilustra el comentario lo que ocurre con las expresiones operador, prestador de servicios y organismos y entidades establecidos en el artículo 2.2.17.1.2 del Decreto 620 de 2020, lo cual

[14] PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. Decreto 1078 de 2015, art. 2.2.17.1.4, num. 11.
[15] Ibidem, art. 2.2.17.1.2.
[16] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 1413 del 2017, art. 1.
[17] Idem.

se pone de manifiesto, entre otras, en divulgaciones institucionales como la que se pone de presente en el portal oficial de estrategia.gobierno.gov.co

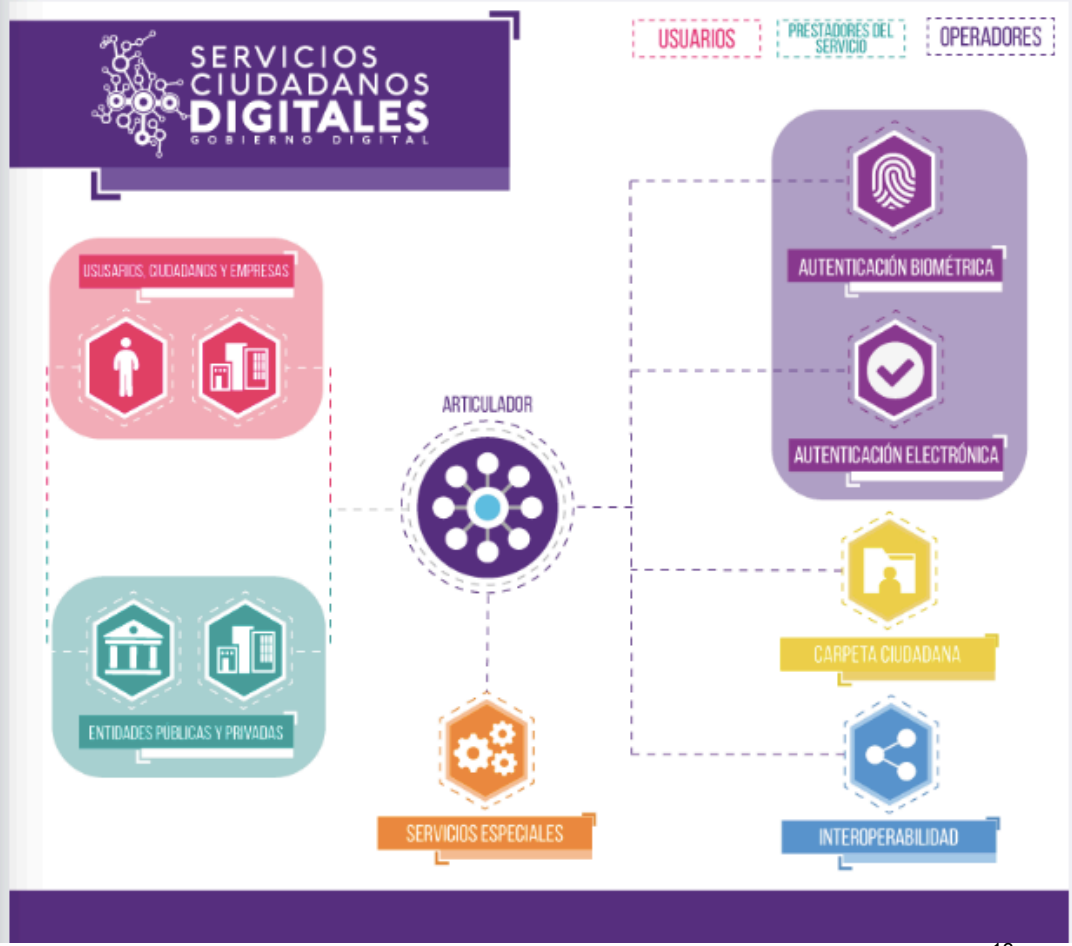

Ilustración 1. Gráfica de Servicios Ciudadanos Digitales[18].

[18] Ibidem. Gobierno digital. Rescatado de: https://estrategia.gobiernoenlinea.gov.co/623/w3-article-18756.html

III- Nuevas Obligaciones En Protección de Datos Personales

Se han incorporado nuevas obligaciones en materia de protección de datos en el Decreto 620 de 2020 que, aun cuando surge en el marco temporal del Estado de Emergencia Social, Sanitaria y Ambiental decretado por el Gobierno del presidente Duque con ocasión de la pandemia por COVID-19, no fue expedido con ocasión de las facultades derivadas del decreto de declaratoria de la misma. Se destacan en ella entonces, como innovación en el universo jurídico colombiano de hábeas data, las siguientes obligaciones:

- Deber de realizar Evaluación de Impacto de Tratamiento de Datos Personales - EIPD (art. 2.2.17.5.2).

- Deber de designar Oficial de Protección de Datos (art. 2.2.17.5.4.).

- Deber de realizar Privacidad por Diseño y Por Defecto (art. 2.2.17.5.5.).

Debe señalarse que a las referidas innovaciones se sumó la reafirmación del deber de los Responsables y Encargados de dar cumplimiento a los Principios de Seguridad de la Información (art. 2.2.17.5.6), Circulación restringida y Finalidad (art. 2.2.17.5.7), y de *Accountability* o Responsabilidad Demostrada y del Programa Integral de Gestión de Datos Personales (art. 2.2.17.5.3.)**,** que ya se habían establecido en normas vigentes antes del Decreto 620 de 2020.

Por encima de las aclaraciones y/o precisiones que seguramente habrán de darse por parte de las entidades responsables del marco normativo sobre los actores del sistema de servicios ciudadanos digitales (cuyas dificultades quedaron advertidas), esto es, Ministerio de las TIC, la AND o incluso la SIC como autoridad del tema de hábeas data, para los efectos de este ensayo, resulta de interés aportar luces sobre el alcance de las nuevas obligaciones y con ello contribuir en la definición de quienes podrían llegar a tener la calidad de Responsables o Encargados en los términos de la Ley 1581 de 2012, a efectos de que dentro de los 18 meses siguientes a la expedición del Decreto 620 del 2020[19] (plazo dado por la norma para la implementación) logren cumplir, para bien tanto de los Titulares de los datos tratados como de las organizaciones obligadas. En tal sentido, se ponen sobre la mesa los siguientes conceptos que se esperan aportar en el propósito advertido, así:

1. Evaluación De Impacto De Protección de Datos Personales

La nueva obligación consistente en realizar la Evaluación de Impacto de Protección de Datos, esto es, la identificación proactiva de los riesgos que el tratamiento de datos personales genera en los sistemas, procesos, infraestructura y actividades del talento humano y su gestión adecuada para evitar su ocurrencia en las organizaciones. Constituye una traslación normativa europea, como la inmensa mayoría de las normas colombianas de protección de datos, que conforme al artículo 35 del Reglamento General de Datos Personales - RGPD, se volvió obligatoria en Europa para ciertas organizaciones cuando existe alto riesgo para los derechos y libertades de los Titulares.

En Colombia, el primer antecedente de referencia a las EIPD no se dio de manera normativa, sino por vía de doctrina en el caso Facebook adelantado por la Superintendencia de Industria y Comercio y en virtud del cual, mediante Resolución 1321 del 24 de enero de 2019, confirmada mediante Resolución 4885 del 13 de febrero de 2020, se le ordenó a la trasnacional de las redes sociales «(…) *desarrollar, implementar y mantener evaluaciones de impacto en la protección de datos (sic.) personales (o evaluaciones de impacto en privacidad), "DPIAS" o "PIAs" por sus nombres en inglés, que evalúen los riesgos inherentes al tratamiento (sic.) de dicha información respecto del uso de la plataforma web o la*

[19] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 620 de 2020, art. 2, parágrafo 2.

Aplicación (sic.) móvil complementaria de Facebook, sus productos, o cualquier otro medio a través del cual Facebook recolecte, use o comparta datos (sic.) personales».

Ahora bien, con base en el artículo 2.2.17.5.2 del Decreto 1078 de 2015 (subrogado por el artículo 1 del Decreto 620 de 2020), se ha ordenado a los prestadores de los servicios ciudadanos digitales que, previo al inicio de las operaciones, deberán realizar la EIPD, exigiéndose al menos los siguientes aspectos:

1. "*Una descripción detallada de las operaciones de tratamiento de datos personales que involucran la prestación de los servicios ciudadanos digitales y de los fines del tratamiento.*

2. *Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.*

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

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

Sobre la redacción utilizada por el creador de la norma, habrá de decirse que, al restringir la obligación sobre "*(…) los prestadores de los servicios ciudadanos digitales*", deja por fuera a otros actores involucrados en los servicios digitales que debieron haberse incluido, por ejemplo al mismo Articulador, esto es, la AND.

Orienta las tareas a ejecutar en virtud de la realización de las actividades de una EIPD, los casos que, conforme al artículo 75 del RGPD Europeo, se han señalado como riesgos de nivel alto para los derechos y libertades ciudadanas, que ameritan la ejecución del mandato establecido en el artículo 35 de la norma en mención, sobre todo si hay gran enorme volumen de datos y gran cantidad de titulares cuya información se soporta en herramientas de nueva tecnología, a saber:

Primera Categoría. Riesgos Subjetivos por condiciones particulares del Titular: Se configuran cuando, en razón de ciertas características subjetivas del Titular, se le expone a sufrir perjuicios económicos o sociales significativos, por el tratamiento no conforme a la ley. Son ejemplos, sin que sean los únicos, los siguientes:

- Discriminación del Titular si el dato es tratado sin su autorización o amparo legal o judicial. (Ejemplo: Divulgación del estado contagiado del Titular de determinada enfermedad).
- Afectación al Titular si el dato es tratado sin su consentimiento o amparo legal o judicial, por tratarse de una persona en condición de vulnerabilidad. (Ejemplo: Divulgación de la calidad de beneficiaria de servicio por estar en condición de pobreza extrema).
- Afectación al Titular si el dato es tratado sin su consentimiento o amparo legal o judicial, por tratarse de una persona menor de edad. (Ejemplo: Divulgación de datos de una menor de edad, en condición de pobreza extrema que padece una determinada enfermedad.)
- Afectación al Titular si el dato es tratado sin su consentimiento o amparo legal o judicial, por tratarse de una persona perteneciente a grupos con determinada orientación sexual o creencia étnica, racial, religiosa, filosófica, ideológica o partidista. (Ejemplo: Divulgación de la calidad de miembro a una secta o credo.)

Segunda Categoría. Riesgos Objetivos: Se configuran cuando, en razón de ciertas características objetivas del dato o su tratamiento, se le expone al Titular a sufrir perjuicios económicos o sociales significativos, por el tratamiento no conforme a la ley. Son ejemplos, sin que sean los únicos, los siguientes:

- Usurpación fraudulenta de identidad (Ejemplo: Acceso no autorizado a número de cuenta bancaria y clave de acceso).
- Divulgación no consentida de estado patrimonial (Ejemplo: Divulgación no autorizada de las condiciones económicas de un Titular).
- Afectación no consentida de la disponibilidad del dato. (Ejemplo: Cifrado extorsivo)
- Acceso no autorizado a información protegida por secreto profesional. (Ejemplo: Divulgación no consentida de información de un feligrés dada en confesión.)

- Acceso no autorizado a perfiles personales tales como movilidad, hábitos de consumo, o análisis o predicción de aspectos relacionados al rendimiento en el trabajo, preferencias o intereses personales, comportamientos o confiabilidad,
- Divulgación no consentida de información reputacional (Ejemplo: Divulgación extemporánea de antecedentes penales o disciplinarios sin consentimiento.)
- Divulgación no consentida de datos genéticos o de salud. (Ejemplo: Divulgación de ADN de un Titular)
- Ingeniería inversa no autorizada para revesar seudonominazación o anonimización de Titulares. (Ejemplo: Divulgación de nombre de menores involucrados en procesos penales amparados por sigilo en la sentencia.)

2. Oficial de Protección de Datos

Llamado en Europa el Delegado de Protección de Datos – DPD y en Colombia Oficial de Protección de Datos – OPD, esta figura aparece con el surgimiento mismo de las normativas de hábeas data en los diferentes países, aun cuando su obligatoriedad no ha sido generalizada en todos.

Conforme lo señala la misma Comisión Europea, se "*Deberá nombrar un DPD, tanto si es un responsable como un encargado del tratamiento, si sus* ***actividades principales*** *guardan relación con el tratamiento de* ***datos sensibles*** *a* ***gran escala*** *o si sus actividades principales guardan relación con* ***la observación habitual y sistemática a gran escala*** *de personas. En este sentido, la observación del comportamiento de los interesados incluye todas las formas de seguimiento y elaboración de perfiles por internet, incluso para los fines de publicidad comportamental.*

Las administraciones públicas siempre tienen la obligación de nombrar un DPD (salvo los tribunales en el ejercicio de su función judicial).

El DPD puede ser un miembro del personal de su organización o puede contratar uno externo en el marco de un contrato de servicio. El DPD puede ser una persona o una organización"[20].

[20] COMISIÓN EUROPEA. ¿Mi organización debe tener un delegado de protección de datos (DPD)?. Rescatado de: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-

Para el caso colombiano, aun cuando no hay norma alguna que lo defina de manera expresa, se ha desprendido su exigencia del sentir del artículo 23 del Decreto 1377 de 2013, ahora refundido en el 2.2.2.25.3.1 del Decreto 1074 de 2015, que ordena contar con una "*Persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización*"*,* pero no se había establecido con carácter de obligatoriedad en norma alguna, hasta la expedición del Decreto 620 del 2020.

Se ha de tener en cuenta que el OPD, como encargado de dirigir el Sistema de Protección de Datos Personales en la organización y responsable de velar por el cumplimiento del mismo en ella, se encarga, entre otras, de cumplir con las siguientes actividades:

- "*Orientar la constitución del Gobierno del Sistema de Protección de Datos, esto es la asignación de roles y responsabilidades asociadas al habeas data y a la gestión del Sistema de Protección de Datos en las áreas internas involucradas.*

- *Monitorear del Sistema de Protección de Datos, haciendo seguimiento y control del cumplimiento de la obligación legal asociada al habeas data, en las operaciones de la organización, mediante la implementación de indicadores y evaluaciones de cumplimiento.*

- *Gestionar el cumplimiento del principio de responsabilidad demostrada o Accountability, mediante el aseguramiento de la documentación y conservación de las evidencias de todas las actividades desarrolladas para el mantenimiento de la protección de los datos personales de sus titulares (…).*

- *Mantener actualizado el sistema de protección de datos frente a los cambios, cuando por la dinámica de la operación existan variaciones en los elementos inherentes al Sistema de Protección de Datos (Datos personales, Titulares de datos personales, Finalidades de tratamiento, etc.).*

---

business-and-organisations/obligations/data-protection-officers/does-my-company-organisation-need-have-data-protection-officer-dpo_es

- *Asegurarse le implementación de la Política de Tratamiento de la Información, el Aviso de Privacidad y el manual de políticas y procedimientos de protección de datos adecuados a las características propias de la organización.*

- *Gestionar y mantener actualizado el Registro Nacional de Bases de Datos – RNBD, ante la SIC.*

- *Orientar la evaluación de los riesgos a que estén expuestas las Bases de Datos, lo mismo que su gestión conforme al nivel de riesgo que posea cada una de ellas.*

- *Asegurarse en general el cumplimiento de las obligaciones legales, y sobre todo, que las autorizaciones se recolecten siempre de manera previa, expresa e informada de los titulares o sus representantes*"[21].

En relación con la reglamentación del Oficial de Protección de Datos, ahora establecido como obligatorio en los actores del servicio ciudadano digital, demandará la revisión de la normativa para extenderlo a otras áreas sensibles como, por ejemplo, la salud y el sector financiero, así como para reglamentar un poco más su figura, entregando pautas de su proceso de designación, funciones y competencias, su ubicación en las estructuras de las organizaciones y las obligaciones de Responsable y Encargado para con él, a la manera en que lo ha hecho el RGPD Europeo en sus artículos 37 a 39, al regular la figura del Delegado de Protección de Datos.

3. Privacidad por Diseño y Por Defecto

Esta nueva obligación, que refleja el espíritu proactivo del deber en materia de protección de datos personales, presupone que desde el mismo momento en que un proyecto va a ser abordado por una organización, ha de hacerse un análisis, desde su inicio, acerca de los aspectos vinculados con datos personales y su protección.

Claramente una de las evidencias de privacidad por diseño la constituyen las EIPD, a que se hizo referencia en el numeral 1 de las nuevas obligaciones,

[21] FERSACO S.A.S. Software 1581 - Sistema de Protección de Datos Personales. Rescatado de: https://awsapp.1581.com.co/1581/servlet/com.sgsdp.hlogin

recomendada como el primer paso a ejecutarse por parte de Ann Cavoukian, Comisionada de Protección de Datos de Ontario, Canadá, quien incorporó desde el año 90 este concepto y el cual fue acogido en la 32ª Conferencia Internacional de Comisionados de Protección de Datos y Privacidad desarrollada en Jerusalén en el año 2010, tal como lo refiere la Agencia Española de Protección de Datos Personales en su Guía de Privacidad desde el Diseño.

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

Ilustración 2. Principios de "Privacidad desde el diseño"[22].

Sin lugar a dudas, hacer una análisis de los riesgos justamente al inicio de un proyecto no solo pone de presente la responsabilidad *(accountbility)* del Responsable o Encargado, sino que permite incorporar anticipadamente los mecanismos que en el desarrollo del proyecto y su implantación han de tenerse en cuenta para lograr estar al día con los deberes de seguridad y cuidado que la ley ordena, además de que permite contemplar costos previos que viabilizan la ejecución de los mismos, evitando sorpresas que puedan echar al traste con buenas iniciativas tecnológicas, por ejemplo, pero inviables jurídicamente por las nuevas exigencias nacionales y globales que sobre datos personales existen.

Así, el RGPD en su artículo 25 le exige al responsable del tratamiento (entiéndase Responsable y Encargado) que la protección de datos desde el diseño y por defecto presuponga "*(…) 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*

[22] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía de Privacidad desde el Diseño. España: 2019. Rescatado de: https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

Reglamento y proteger los derechos de los interesados"[23]; así como aplicar "*(…) 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*"[24]; buscando siempre que por defecto, agrega la norma, se garantice, entre otros, el principio de acceso y circulación restringidos.

Por las consideraciones anotadas, es que se estima con acierto que la Universidad de Salamanca señalara, acerca de los beneficios que trae la privacidad, las siguientes manifestaciones:

"*La adopción de la privacidad por diseño es esencial para la minimización de riesgos a la privacidad y también para fomentar la confianza. El diseño de proyectos, procesos y sistemas con la privacidad incorporada desde el inicio conlleva brinda importantes ventajas como:*

- *Los problemas potenciales se detectan en una etapa más temprana, por lo que será más fácil abordarlos (y menos costoso).*

- *El nivel de concienciación sobre privacidad y protección de datos dentro de la organización aumentará de manera natural.*

- *Las organizaciones que adoptan el principio de privacidad por diseño serán mucho más propensas a cumplir con sus obligaciones legales y por lo tanto minimizarán el riesgo de incurrir en sanciones.*

- *Las acciones de la organización serán mucho menos intrusivas y menos propensas a tener un impacto negativo en los individuos cuyos datos se están tratando*"[25].

Es, por tanto, la protección de datos desde el diseño y por defecto otra obligación que, no obstante exigida con carácter obligatorio por mandato del Decreto 620 del

[23] PARLAMENTO EUROPEO & CONSEJO DE LA UNIÓN EUROPEA. Reglamento (UE) 2016/679, art. 25, num. 1.
[24] Ibidem, num. 2.
[25] FUNDACIÓN GENERAL DE LA UNIVERSIDAD DE SALAMANCA. La privacidad por diseño en el Reglamento General de Protección de Datos. Rescatado de: https://fundacion.usal.es/es/empresas-amigas/199-contenidos/2143-la-privacidad-por-diseno-en-el-reglamento-general-de-proteccion-de-datos

2020, deja a la autoridad nacional que desarrolle reglamentos orientadores, aun cuando es de resaltar que ya la SIC ha venido refiriendo la necesidad de su adopción en sus publicaciones, como por ejemplo en la *GUÍA SOBRE EL TRATAMIENTO DE DATOS PERSONALES PARA FINES DE MARKETING Y PUBLICIDAD*.

CONCLUSIONES

El Decreto 620 de 2020, incorpora por primera vez como obligatorios la realización de Evaluaciones De Impacto De Protección de Datos Personales – EIPD, la designación del Oficial de Protección de Datos Personales – OPD y la incorporación como práctica de la Protección de Datos desde el Diseño y Por Defecto.

Las anteriores obligaciones están dirigidas a las nuevas empresas del ecosistema de servicios ciudadanos digitales, esto es, los articuladores, los operadores o prestadores de servicios ciudadanos digitales, los organismos y entidades establecidos en el artículo 2.2.17.1.2 del Decreto 620 de 2020, autoridades del sistema de servicios ciudadanos, autoridades de identificación, aliados tecnológicos.

Queda pendiente, en cabeza de las autoridades nacionales, generar reglamentaciones sobre los temas relacionados con las nuevas obligaciones de forma que orienten el cumplimiento de los deberes de los obligados.

FUENTES BIBLIOGRÁFICAS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía de Privacidad desde el Diseño. España: 2019. Rescatado de: https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

AGENCIA NACIONAL DIGITAL. Nosotros. Rescatado de: https://and.gov.co/nosotros-3/

- Servicios ciudadanos digitales. Rescatado de: https://and.gov.co/servicios-ciudadanos-digitales/

COMISIÓN EUROPEA. ¿Mi organización debe tener un delegado de protección de datos (DPD)?. Rescatado de: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/data-protection-officers/does-my-company-organisation-need-have-data-protection-officer-dpo_es

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1753 de 2015. Rescatado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1753_2015.html

- Ley 1955 de 2019. Rescatado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1955_2019.html

COTE PEÑA, Luis Fernando. Hábeas data en Colombia, un trasplante normativo para la protección de la dignidad y su correlación con la NTC/ISO/IEC 27001:2013. España: Agencia Estatal Boletín Oficial del Estado, 2016. Rescatado de: https://fersaco.com/protecci%C3%B3n-de-datos)

- Riesgos que obligan la Evaluación de Impacto de Protección de Datos. Colombia: 2019. Rescatado de: https://fersaco.wordpress.com/2019/04/13/riesgos-que-obligan-la-evaluacion-de-impacto-de-proteccion-de-datos/

FERSACO S.A.S. Software 1581 - Sistema de Protección de Datos Personales. Rescatado de: https://awsapp.1581.com.co/1581/servlet/com.sgsdp.hlogin

FUNDACIÓN GENERAL DE LA UNIVERSIDAD DE SALAMANCA. La privacidad por diseño en el Reglamento General de Protección de Datos. Rescatado

de: https://fundacion.usal.es/es/empresas-amigas/199-contenidos/2143-la-privacidad-por-diseno-en-el-reglamento-general-de-proteccion-de-datos

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Decreto 1074 de 2015. Rescatado de: https://www.icbf.gov.co/cargues/avance/docs/decreto_1074_2015.htm

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 1413 del 2017. Rescatado de:https://www.mintic.gov.co/portal/604/articles-59399_documento.pdf

- Decreto 620 de 2020. Rescatado de: https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%20620%20DEL%202%20DE%20MAYO%20DE%202020.pdf
- Gobierno digital. Rescatado de: https://estrategia.gobiernoenlinea.gov.co/623/w3-article-18756.html

PARLAMENTO EUROPEO & CONSEJO DE LA UNIÓN EUROPEA. Reglamento (UE) 2016/679. Rescatado de: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e3126-1-1

PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. Decreto 1078 de 2015. Rescatado de: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=62513

- Decreto 2106 de 2019. Rescatado de: https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%202106%20DEL%2022%20DE%20NOVIEMBRE%20DE%202019.pdf

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Guía sobre el tratamiento de datos personales para fines de marketing y publicidad. Colombia: 2019. Rescatado de: https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20marketing%2C%20publicidad%20y%20tratamiento%20de%20datos%202019.pdf

- Resolución 1321 de 2019. Rescatado de: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/Res-1321-de-2019(1).pdf
- Resolución 4885 de 2020. Rescatado de: https://www.sic.gov.co/sites/default/files/files/Noticias/Res%204885%2013II2020%20Facebook%20Colombia%20SAS.pdf