DUVALIER
Congresista

Cámara
de Representantes

PROPOSICIÓN
AUDIENCIA PÚBLICA # 19
(Art. 264 numeral 3, Ley 5 de 1992)

Con fundamento en el numeral 3 del artículo 264 de la Ley 5ta de 1992 (Reglamento Interno del Congreso), solicitamos respetuosamente a la Comisión Primera Constitucional Permanente de la Cámara de Representantes que se apruebe la convocatoria a Audiencia Pública para la participación ciudadana sobre el Proyecto de Ley Estatutaria No. 156 de 2023 Cámara *"Por la cual se dictan disposiciones para el régimen general de protección de datos personales"*.

La Audiencia Pública tiene como propósito escuchar a las instituciones públicas, academia, juristas, organizaciones de la sociedad civil, expertos en la materia y ciudadanía en general sobre la actualización del régimen de protección de datos en el país, con el objetivo de conocer las visiones que se pueden presentar sobre la iniciativa legislativa y realizar las modificaciones que sean pertinentes en la ponencia a radicarse para el primer debate en esta Corporación.

Bogotá D.C., 19 de Septiembre de 2023.

De las y los Congresistas,

DUVALIER SANCHEZ ARANGO
Representante a la Cámara Valle del Cauca
Ponente Coordinador

RECIBÍ
COMISIÓN PRIMERA CONSTITUCIONAL
CÁMARA DE REPRESENTANTES
26 SEP 2023
HORA: 11:30
FIRMA:

COMISIÓN PRIMERA
APROBADO
08 NOV 2023
ACTA Nº 19
Unanimidad

Edificio Nuevo del Congreso - Carrera 7 #8-62, oficina 505 B.
Teléfonos: 3823000 - correo electrónico: duvalier.sanchez@camara.gov.co

Anexo 8-11-23

Etiquetado:	Externo

certicámara.

Bogotá D.C., 8 de febrero de 2024.

Honorables representantes:

Duvalier Sánchez Arango
Juan Carlos Wills Ospina
Adriana Carolina Arbeláez Giraldo
Carlos Felipe Quintero Ovalle
Hernán Darío Cadavid Márquez
Astrid Sánchez Montes De Oca
Diógenes Quintero Amaya
Jorge Alejandro Ocampo Giraldo
Luis Alberto Albán Urbano
Marelen Castillo Torres

Ref.: Observaciones al Proyecto de Ley 156 de 2023C "Por la cual se dictan disposiciones para el Régimen General de Protección de Datos Personales"

Respetados representantes,

Reciban un cordial y respetuoso saludo de la **SOCIEDAD CAMERAL DE CERTIFICACIÓN DIGITAL CERTICÁMARA S.A.**

La Cámara de Comercio de Bogotá, en asocio con las Cámaras de Comercio de Medellín para Antioquia, Cali, Bucaramanga, Cúcuta, Aburrá Sur, y la Confederación de Cámaras de Comercio (Confecámaras), crearon la Sociedad Cameral de Certificación Digital Certicámara S.A., Entidad de Certificación Digital Abierta, constituida en el año 2001 con el propósito de asegurar jurídica y técnicamente las transacciones, comunicaciones, aplicaciones, y en general, cualquier proceso de administración de información digital, de conformidad con los presupuestos establecidos en la Ley 527 de 1999 y los estándares técnicos internacionales de rigor en la materia.

Mediante esta comunicación, la compañía respetuosamente remite las observaciones al proyecto de ley referenciado en el asunto, de acuerdo con los siguientes términos:

Etiquetado:	Externo

certicámara.

Art.	Texto del proyecto	Comentarios	Propuesta
4.	**Artículo 4. Datos de personas fallecidas.** 1. Los causahabientes podrán dirigirse al responsable o encargado del tratamiento con el objeto de solicitar el acceso a los datos personales de la persona fallecida y, en su caso, su rectificación o supresión. 2. Las personas o instituciones a las que la persona fallecida hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de éste y, en su caso su rectificación o supresión. La Superintendencia de Industria y Comercio en conjunto con la Registraduría del Estado Civil, señalarán los requisitos y condiciones para acreditar la validez y	Se solicita de forma atenta, que se aclare cuáles son los elementos que los responsables o encargados deberán validar para determinar que un causahabiente cuenta con la legitimidad para ejercer el derecho de rectificación o supresión de datos de una persona fallecida. Adicionalmente, es necesario establecer de qué manera debe proceder el responsable o encargado del tratamiento de los datos personales de una persona fallecida, cuando la misma tenga múltiples causahabientes y no exista unanimidad entre los mismos sobre el ejercicio del derecho de rectificación o supresión de datos de una persona fallecida.	

	vigencia de estas autorizaciones. 3. En caso de fallecimiento de niños, niñas y adolescentes, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Instituto Colombiano de Bienestar Familiar o quien haga sus veces, que podrá actuar de oficio o a instancia de cualquier persona natural o jurídica interesada. 4. En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de quienes ejercen como representantes legales, o por la Defensoría del Pueblo, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo		

	prestadas por el designado. **Parágrafo primero.** Las personas a las que se refiere en numeral 1 del presente artículo, no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los causahabientes a acceder a los datos de carácter patrimonial del causante. **Parágrafo segundo.** La autorización expresa de que trata el numeral segundo podrá realizarse de conformidad con lo establecido en la ley 1996 de 2019 en relación con las directivas anticipadas, o a través de cualquier otro acto por medio cual se exprese dicha autorización.		

certicámara.

5.3	3.«Base de datos de riesgo crediticio»: para todos los efectos de la presente ley se entenderá por Base de Datos de Riesgo Crediticio aquella en la que se almacena y procesa datos personales de carácter financiero, crediticio, comercial y/o de servicios en cuanto al nacimiento, ejecución y extinción de obligaciones dinerarias se refiere; cuya finalidad será el tratamiento de dicha información para crear un perfil de los titulares y calcular su capacidad de endeudamiento y el riesgo crediticio que de ello se desprende, lo anterior bajo los parámetros y plazos de conservación contenidos en la Ley 2157 de 2021 o la que en su momento esté en vigencia.	Incluir dentro de la ámbito de aplicación de la norma, definiciones relacionadas con datos personales de carácter financiero, crediticio, comercial y/o de servicios, puede crear confusión o incluso contrariar lo dispuesto en la ley 1266 de 2008	Solicitamos que se elimine el punto 3 del artículo 5, bajo el entendido de que el ámbito de aplicación de la Ley 1581 que se está modificando, y la Ley 1266 de 2008, son diferentes.
5.6	6.«Cesión o comunicación de datos»: Tratamiento de datos que supone su revelación a una persona distinta del titular y/o encargado de tratamiento.	Es necesario hacer una distinción entre comunicación y cesión. Lo anterior, teniendo en cuenta que, las implicaciones de una cesión de datos personales es diferentes a la comunicación de los mismos, la definición	Que el artículo 5.6-Definiciones-«Cesión o comunicación de datos» se modifique en el siguiente sentido:

		consignada en este punto es atribuible a lo ya definido por la Superintendencia de industria y comercio como una transmisión de datos personales que implica la comunicación de los datos por parte de un responsable a un encargado, sin que el rol del responsable que transmite cambie.	6. **Transmisión de datos:** Tratamiento de datos que supone su revelación **por parte del responsable de los datos personales** a una persona distinta del titular **identificado como encargado de tratamiento**.
5.7-	7.«Consentimiento del titular»: toda manifestación de voluntad libre, consciente, específica espontánea, informada e inequívoca por la que el titular acepta de forma previa, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de los datos personales que le conciernen;	Es importante que el medio para la obtención de la autorización garantice que se tenga evidencia de autorización	Que el artículo 5.7- Definiciones, se modifique en el siguiente sentido: 1.«Consentimiento del titular»: toda manifestación de voluntad libre, consciente, específica espontánea, informada e inequívoca por la que el titular acepta de forma previa, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de los datos personales que le conciernen. **Sin perjuicio de lo anterior, quien lleve a cabo el tratamiento de los datos, garantizará y guardará evidencia**

			de la existencia de la autorización respectiva.
5.8-	8.«Datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona natural que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;	La Superintendencia de industria y Comercio ha definido los datos biométricos indicando que "**son datos sensibles** que permiten identificar a una persona natural a través del reconocimiento de una característica física **e intransferible**, que, al ser única de cada individuo, permite distinguir a un ser humano de otro." Adicionalmente, menciona que los datos biométricos son los relativos a la biometría definida en el diccionario de la real academia de la lengua así: "una tecnología de seguridad basada en el reconocimiento de una característica física e intransferible de las personas, como la huella digital, que [sic] al ser una característica única de cada individuo, permite distinguir a un ser humano de otro" En este sentido, consideramos que se debe incluir en la definición aspectos que ya han sido desarrollados por la Superintendencia de industria y comercio.	Que el artículo 5.8- Definiciones, se modifique en el siguiente sentido: "Datos biométricos: Son **datos sensibles** que permiten identificar a una persona natural a través de **una tecnología de seguridad basada en el** reconocimiento de una característica física e intransferible, que, al ser única de cada individuo, permite distinguir a un ser humano de otro, como imágenes faciales o datos dactiloscópicos."

certicámara.

5.14-	14.«Destinatario o tercero»: Persona natural o jurídica, pública o privada, al que se comuniquen datos personales, distinta del titular, responsable de tratamiento y encargado. No se considerarán destinatarios a las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el artículo 2, numeral 2, literal c) y e) de la presente ley;	La definición de destinatarios debe ser lo suficientemente clara como para determinar la calidad y responsabilidades que deben cumplir los mismos. Así mismo, sin perjuicio de la finalidad para la que se recibe la información, así se trate de autoridades públicas, las mismas tienen la obligación de no dar un uso a la información, que difiera de la finalidad para la cual la recibió.	Solicitamos amablemente se elimine toda mención a lo largo del proyecto de Ley, referente a un tercero o destinatario, bajo el entendido de que no se acopla a alguna ni tiene responsabilidades definidas como si es el caso de los titulares, responsables y encargados del tratamiento de los datos personales.
5.25	25. «Queja»: reclamación de interés particular dirigida a la autoridad de control que busca el amparo del derecho fundamental a la protección de los datos personales.	Durante el desarrollo del Proyecto de Ley los términos de queja, solicitud y reclamo son usados sin distinción, por lo que resulta importante que este proyecto normativo incluya las definiciones de cada uno de estos términos para que sean usados de manera correcta con la implementación de esta nueva Ley. Lo anterior, dado que, la diferenciación entre los mismos toma relevancia dentro de las obligaciones que tiene a su cargo el responsable, como lo es la actualización en el Registro Nacional de Bases de Datos.	Se sugiere se haga la distinción entre solicitud, queja, reclamo, ya que, al tratarse de agrupar los tres significados, los cuales tienen un alcance diferente, se genera confusión. Por lo tanto, con el fin de que se tenga una definición clara sobre estos términos, se incluyan los siguientes: Solicitud: Comunicación del titular del

certicámara.

			tratamiento de los datos personales al responsable y/o encargado del tratamiento de los datos cuya finalidad esté relacionada con la rectificación, actualización, supresión de sus datos personales. Reclamo: Comunicación del titular del tratamiento de los datos personales al responsable y/o encargado del tratamiento de los datos cuando el responsable y/o encargado no atendió adecuadamente la solicitud realizada por el titular previamente.
5.33	33.«Transferencia internacional de datos personales» Tratamiento que supone un flujo de datos en el que un responsable y/o encargado del tratamiento ubicado en el territorio nacional	No es posible acoger en una misma definición dos situaciones que tienen implicaciones diferentes como lo es la transferencia de responsable a responsable y la transmisión de responsable a encargado. Es necesario que se haga una distinción entre las	Sugerimos se adopte la definición de transferencia que contiene la Ley 1581 de 2012 y sus Decretos reglamentarios.

certicámara.

	envía datos personales a destinatarios y/o encargados ubicados fuera del territorio nacional u organizaciones internacionales.	transferencias totales y parciales, ya que en algunos casos el responsable identificado como cedente, tras el perfeccionamiento de la cesión conserva algunas obligaciones frente tratamiento de los datos personales, lo anterior atendiendo la diversidad y dinamismo del mundo de los negocios.	
10.	**Artículo 10. Condiciones para el tratamiento en la ejecución de un contrato.** 1. Se recolectarán los datos necesarios para la ejecución del contrato, todos aquellos datos que no se requieran para la existencia y ejecución del mismo, necesitarán de otra base legitimadora para su tratamiento. 2. El plazo de conservación de los datos estará determinado por la duración del contrato, salvo que, en cumplimiento de un deber legal el responsable esté	Resulta de gran importancia conocer el procedimiento que pretende implementar el Artículo 10. Condiciones para el tratamiento en la ejecución de un contrato en su numeral 4, el cual pretende implementar el procedimiento o solicitud de devolución de los datos personales al titular al finalizar una relación contractual, pues su redacción resulta confusa y de difícil aplicación en la práctica. Lo anterior, teniendo en cuenta que el ámbito de aplicación de la ley son los datos de carácter personal, no los datos en general, de estos últimos deberán encargarse las partes al momento de establecer las reglas o condiciones de confidencialidad de la información compartida entre las mismas.	Sugerimos se adopte la siguiente redacción: Una vez terminada la relación contractual por cualquier causa, incluida la nulidad, los datos de carácter personal podrán ser eliminados por parte del responsable a solicitud del titular de los datos dentro de los 30 días siguientes a la terminación del contrato o luego de la sentencia ejecutoriada que declara la nulidad. Con posterioridad a los 30 días de la terminación del contrato, los datos podrán ser suprimidos por el responsable. No

	obligado a exceder ese plazo. 3. La contratación que se lleve a cabo por entidades públicas, también le serán aplicables los principios y demás obligaciones establecidas en la presente ley. 4. Una vez terminada la relación contractual por cualquier causa, incluida la nulidad, los datos de carácter personal se devolverán al titular, si éste los solicita dentro de los 30 días siguientes a la terminación del contrato o luego de la sentencia ejecutoriada que declara la nulidad. Con posterioridad a los 30 días, los datos podrán ser suprimidos por el responsable. No procederá la supresión de los datos cuando exista una disposición legal que exija su conservación, en cuyo caso, deberá procederse a la devolución de los mismos garantizando el responsable del		procederá la supresión de los datos cuando exista una disposición legal que exija su conservación.

certicámara.

	tratamiento dicha conservación. 5. El responsable del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación contractual con el titular, excepto para la puesta a disposición por orden judicial, o por orden de la fiscalía general de la nación, o por la Superintendencia de Industria y Comercio, y cuando proceda, la Superintendencia Financiera de Colombia.		
14.	**Artículo 14. Condiciones para el tratamiento necesario para la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero.** 1. Una vez se haya examinado que el tratamiento no puede ser realizado en el supuesto de otra base legitimadora, el responsable podrá basar	Solicitamos amablemente se aclare si para el tratamiento necesario al que hace referencia el artículo 14, es requisito que se cumplan la totalidad de condiciones generales y específicas mencionadas en el mismo artículo, o si por el contrario, con la verificación de solo una de las condiciones el responsable podrá basar el tratamiento de los datos personales en el interés legítimo.	

	el tratamiento de datos personales en el interés legítimo siempre que se verifiquen las siguientes condiciones generales y específicas para dicho tratamiento: a) Debe representar un interés real y actual, es decir, no debe ser especulativo. b) Debe existir una relación pertinente y apropiada entre el titular y el responsable, como en situaciones en las que el titular es cliente o está al servicio del responsable. c) No es aplicable al tratamiento realizado por las entidades públicas en ejercicio de sus funciones. d) No puede ser invocado cuando se traten datos sensibles. e) Cuando se trate de una transferencia internacional basándose en un interés legítimo imperioso, debe cumplir con los requisitos		

	establecidos en el artículo 67 de la presente ley. 2. Dependiendo del estado de la técnica, recursos a disposición y las circunstancias del tratamiento, el interés legítimo puede convertirse en una de las bases legitimadoras mencionadas en el artículo 7, y se tomará aquella como preferente. 3. El interés legítimo siempre debe estar acompañado de un examen de ponderación, excepto cuando: a) Se realiza tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales. b) El tratamiento está relacionado con la realización de determinadas operaciones mercantiles de conformidad con el artículo 87 de la presente Ley.		

	c) El tratamiento es necesario para la prevención del fraude. d) Se transmiten datos personales dentro de un grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados. 4. El examen que se menciona en el numeral 3 del presente artículo, es una evaluación que se compone de tres diferentes fases preclusivas. El mismo tiene como objeto comprobar si el tratamiento es lícito y este examen, debe quedar documentado, en cumplimiento del principio de responsabilidad demostrada "Accountability" y, de una forma clara y transparente, en virtud del principio de transparencia, dicho examen debe partir con la descripción del		

	tratamiento. Las fases que componen el examen de interés legítimo son las siguientes: a) Test de finalidad (" satisfacción de intereses legítimos del responsable"): teniendo en cuenta la finalidad o el propósito específico del tratamiento analizado, debe identificarse cuál es el beneficio concreto sobre el que se sustenta dicho tratamiento; b) Test de necesidad ("¿es necesario el tratamiento?"): resulta imprescindible analizar si dicho tratamiento es necesario y proporcional para la consecución de los objetivos propuestos o si por el contrario concurren otras alternativas para satisfacer esos intereses; c) Test de equilibrio ("que sobre dichos		

certicámara.

	intereses no prevalezcan los intereses o los derechos y garantías fundamentales del titular"): si resultara que no existe otra alternativa o esta exigiera esfuerzos desproporcionados, procede realizar la prueba de sopesamiento. Dicha prueba consiste en analizar el impacto y/o el daño o perjuicio potencial del concreto tratamiento en los derechos y garantías de los titulares, para lo cual se tendrá en cuenta: i) Origen de los datos; ii) Categoría de los datos; iii) Si existe o no una relación previa con el titular; iv) Expectativa; v) Si afecta los intereses, derechos y garantías del titular; vi) Agentes implicados en el tratamiento; vii) Garantías adicionales para limitar su impacto en los derechos y		

certicámara.

	garantías fundamentales. 5. El tratamiento puede basarse en un interés legítimo cuando el test de equilibrio sea a favor del responsable.		
20.	3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al titular, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente en virtud del numeral 2. 4. Las disposiciones de los numerales 1, 2 y 3 no serán aplicables en la medida en que el titular ya disponga de la información y exista prueba de ello.	En cuanto al numeral 3 del artículo 20, no es claro el procedimiento que se debe surtir en aquellos casos en los cuales los datos personales son tratados para finalidades diferentes a las autorizadas. Toda vez que de la redacción del artículo se podría interpretar que basta con informar al titular y no es necesario solicitar la autorización del mismo.	
27.	**Artículo 27. Derecho de supresión («el derecho al olvido»).**	En Colombia, la "supresión de datos" y el "derecho al olvido" están relacionados con la protección de datos	

	1. El titular tendrá derecho a obtener del responsable del tratamiento la supresión de los datos personales que le concierne, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las siguientes circunstancias: a) Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; b) El titular retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 7, numeral 1, literal a), o el artículo 15, numeral 2, literal a), y este no se fundamente en otra base legitimadora; c) El titular se oponga al tratamiento con arreglo al artículo 33, numeral 1 y 2, y no prevalezcan otros motivos legítimos.	personales, pero tienen enfoques ligeramente diferentes. La supresión de datos se refiere a la eliminación de datos personales de las bases de datos, mientras que el derecho al olvido se relaciona más con el control sobre la visibilidad continua de la información personal en entornos en línea.	

certicámara.

	d) Los datos personales hayan sido tratados ilícitamente; e) Los datos personales deban suprimirse para el cumplimiento de una obligación legal que se aplique al responsable del tratamiento; f) Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información a menores de edad mencionados en el artículo 9, numeral 3. g) La Autoridad de Control Competente determine que en el tratamiento ha incurrido en conductas contrarias a la Constitución o esta ley y las demás normas que la modifiquen o adicionen. 2. Cuando haya cedido los datos personales y esté obligado, en virtud de lo dispuesto en el numeral 1, a suprimir dichos datos, el responsable del tratamiento teniendo en cuenta la tecnología		

certicámara.

	disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los destinatarios o terceros que estén tratando los datos personales de la solicitud del titular de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos. 3. Los numerales 1 y 2 no se aplicarán cuando el tratamiento sea necesario: a) Para ejercer el derecho a la libertad de expresión e información; b) Para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por la ley que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;		

certicámara.

	c) Por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 15, numeral 2, literales h) e i), y numeral 3; d) Con fines de archivo en interés público, investigación científica, o estadística, de conformidad con el artículo 85, numeral 1, en la medida en que el derecho de supresión pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o; e) Para la formulación, el ejercicio o la defensa de reclamaciones administrativas o judiciales.		
32.2	2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el numeral 1, el titular tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.	La naturaleza jurídica de la transmisión no es la del tratamiento que se relaciona en este numeral.	2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el numeral 1, el titular tendrá derecho a que los datos personales se **transfieran** directamente de responsable a

certicámara.

			responsable cuando sea técnicamente posible.
35.	**Artículo 35. Derecho a presentar una queja ante la Autoridad de Control.** 1. Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo titular que considere que su derecho fundamental a la protección de datos ha sido vulnerado por infracción a la presente ley tendrá derecho a presentar una queja ante la autoridad de control competente. 2. La queja se formulará mediante solicitud dirigida a la Autoridad de Control y deberá contener, por lo menos: a) La identificación del titular y/o su representante legal junto con los documentos que acrediten tal calidad; b) El objeto de la queja, es decir, lo	Teniendo en cuenta las sugerencias elevadas en cuanto a lo contemplado en el artículo 5 de la presente ley consideramos que se deben hacer ajustes en la terminología empleada en la redacción del presente artículo.	**Artículo 35. Derecho a presentar una queja ante la Autoridad de Control.** 1. Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo titular que considere que su derecho fundamental a la protección de datos ha sido vulnerado por infracción a la presente ley tendrá derecho a presentar una queja ante la autoridad de control competente. 2. La queja se formulará mediante solicitud dirigida a la Autoridad de Control y deberá contener, por lo menos: a) La identificación del titular y/o su representante legal junto con los documentos que acrediten tal calidad; b) El objeto de la queja, es decir, lo

certicámara.

	que se persigue con ella; c) La descripción clara de los hechos que fundamentan el reclamo; d) La dirección de notificación; e) Los documentos que soporten la acreditación del requisito de procedibilidad establecido en el numeral 3 del presente artículo, y; f) Los demás documentos que se quiera hacer valer en el trámite administrativo. 3. El titular o quien represente sus intereses solo podrá elevar queja ante la Autoridad de Control una vez que haya agotado el requisito de procedibilidad, esto es, la presentación de una solicitud previa, con ejercicio de derechos, ante el responsable o el encargado según sea el		que se persigue con ella; c) La descripción clara de los hechos que fundamentan el reclamo; d) La dirección de notificación; e) Los documentos que soporten la acreditación del requisito de procedibilidad establecido en el numeral 3 del presente artículo, y; f) Los demás documentos que se quiera hacer valer en el trámite administrativo. 3. El titular o quien represente sus intereses solo podrá elevar queja ante la Autoridad de Control una vez que haya agotado el requisito de procedibilidad, esto es, la presentación de **un reclamo previo**, con ejercicio de derechos, ante el responsable o el encargado según sea el caso siempre que, habiendo

	caso siempre que, habiendo transcurrido el término establecido en esta ley para la solución del reclamo previo, el sujeto obligado no se hubiese pronunciado o, de existir respuesta, esta no satisfaga los intereses del titular de la información. 4. La Autoridad de Control tendrá la obligación de examinar integralmente la petición, y en ningún caso, podrá estimarla como incompleta por falta de requisitos o documentos que no se encuentren dentro del marco jurídico vigente, que no sean necesarios para resolverla o que se encuentren dentro de sus archivos. Si el reclamo resulta incompleto, se requerirá al titular dentro de los diez (10) días siguientes a la fecha de radicación de la queja para que la complete, otorgándole al solicitante el término de un (1) mes para ello. Transcurrido el término		transcurrido el término establecido en esta ley para la solución del reclamo previo, el sujeto obligado no se hubiese pronunciado o, de no existir respuesta, esta no satisfaga los intereses del titular de la información. 4. La Autoridad de Control tendrá la obligación de examinar integralmente la **queja**, y en ningún caso, podrá estimarla como incompleta por falta de requisitos o documentos que no se encuentren dentro del marco jurídico vigente, que no sean necesarios para resolverla o que se encuentren dentro de sus archivos. Si **la queja** resulta incompleto, se requerirá al titular dentro de los diez (10) días siguientes a la fecha de radicación de la queja para que la complete, otorgándole al

certicámara.

	de un (1) mes desde la fecha del requerimiento sin que el solicitante presente la información requerida, se entenderá que ha desistido de su queja, salvo que antes del vencimiento de dicho plazo éste solicite prórroga hasta por un término igual. 5. La autoridad de control ante la que se haya presentado la queja informará a solicitud del reclamante sobre el curso del trámite administrativo y en cualquier caso sobre las etapas que la normativa procesal así determine como obligatorias.		solicitante el término de un (1) mes para ello. Transcurrido el término de un (1) mes desde la fecha **de la presentación de la queja** sin que el solicitante presente la información requerida, se entenderá que ha desistido de su queja, salvo que antes del vencimiento de dicho plazo éste solicite prórroga hasta por un término igual. 5. La autoridad de control ante la que se haya presentado la queja informará a solicitud del titular o **de la persona que represente sus intereses** sobre el curso del trámite administrativo y en cualquier caso sobre las etapas que la normativa procesal así determine como obligatorias.
37.4	4. El responsable del tratamiento deberá actualizar la información, comunicando de forma oportuna al encargado	Respecto al numeral 4, consideramos oportuno aclarar, ¿qué se debe entender por novedad?.	

certicámara.

	del tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas técnicas y organizativas apropiadas para que la información suministrada a este, se mantenga actualizada.	En caso de que se refiera a incidentes, es ideal que el responsable tenga la oportunidad de realizar la investigación pertinente, en un tiempo definido e informar el detalle de lo sucedido con los hechos y datos investigados.	
40.	**Artículo 40. Representantes de responsables o encargados del tratamiento con domicilio fuera del territorio Nacional.** 1. Cuando sea de aplicación el artículo 3 numeral 2, el responsable o el encargado del tratamiento designará por escrito un representante legal y/o sucursal en Colombia. 2. La obligación establecida en el numeral 1 del presente artículo no será aplicable: a) Al tratamiento de datos que sea ocasional, que no incluyan el manejo a gran escala de	Solicitamos se aclare en el texto, ¿cuál es el alcance, las calidades y facultades que deberán tener los representantes de responsables o encargados del tratamiento con domicilio fuera del territorio Nacional?	

	categorías especiales de datos indicadas en el artículo 15 numeral 1, o de datos personales relativos a delitos y condenas penales a que se refiere el artículo 16, y que sea improbable que entrañe un riesgo para los derechos y garantías de las personas naturales, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento, o; b) A las autoridades u organismos públicos. 3. El responsable o el encargado del tratamiento encomendará al representante las facultades necesarias a fin de garantizar el cumplimiento de lo dispuesto en la presente ley. 4. La designación de un representante por el responsable o el encargado del tratamiento se entenderá sin perjuicio de las acciones que pudieran emprenderse		

certicámara.

	contra el propio responsable o encargado.		
41.1	1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable, éste elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos de la presente ley y garantice la protección de los derechos del titular.	Respecto al numeral 1, sugerimos eliminar la palabra "únicamente." A nuestro juicio esta norma desconoce que puede existir multiplicidad de tratamientos para los cuales se requieran diferentes encargados con el fin de garantizar la protección de los derechos de los titulares de la información. Agradecemos tener en cuenta que la norma impone una restricción innecesaria e injustificada.	1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable, éste elegirá **a** un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos de la presente ley y garantice la protección de los derechos del titular.
49.	**Artículo 49. Notificación de un Incidente de seguridad de los datos personales a la autoridad de control.** 1. En caso de Incidente de seguridad de los datos personales, el responsable del tratamiento lo notificará a la Superintendencia de	Se sugiere modificar el término para la notificación de incidentes de seguridad de los datos personales. Se recomienda mantener el estándar actual. El proyecto de ley eleva el estándar de forma desproporcionada, pasando de 15 días hábiles en la actualidad a 72 horas. Esto representa grandes retos e impactos para	

	Industria y Comercio de conformidad con el artículo 73 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicho Incidente de seguridad constituya un riesgo para los derechos y las garantías de las personas naturales. Si la notificación a la Superintendencia de Industria y Comercio no tiene lugar en el plazo de 72 horas, deberá ir acompañada de los motivos que expliquen la dilación. 2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento los incidentes de seguridad de los datos personales de las que tenga conocimiento. 3. La notificación contemplada en el numeral 1 deberá, como mínimo:	las empresas, particularmente las pequeñas y medianas que no tienen las capacidad administrativas ni operativas para afrontar este tipo de situaciones de manera ágil y eficiente, nuevamente destacamos la importancia de valorar este tipo de impactos. Sumado a lo anterior, es importante considerar que se requiere de 72 horas para la contención, erradicación e investigación del incidente de seguridad. Por lo cual, notificar a las 72 horas podría dar lugar a imprecisiones en la información entregada, o a la generación de alertas innecesarias, se sugiere ampliar el término.	

certicámara.

	a) Describir la naturaleza de la Incidente de seguridad de los datos personales y, cuando sea posible, el número aproximado y tipo de titulares afectados, las categorías de datos y el número aproximado de registros de datos personales afectados; b) Comunicar el nombre y los datos de contacto del oficial de protección de datos o de otro punto de contacto en el que pueda obtenerse más información; c) Describir las posibles consecuencias del Incidente de seguridad de los datos personales; d) Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio al Incidente de seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos. 4. Si no fuera posible facilitar la información		

	descrita en el numeral 3 del presente artículo simultáneamente con la notificación de un incidente de seguridad, y en la medida que esta condición persista, la información se facilitará de manera gradual sin dilación indebida. 5. El responsable del tratamiento documentará cualquier Incidente de seguridad de los datos personales, incluidos los hechos relacionados con este, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo. 6. Los datos personales contenidos en la notificación de una Incidente de seguridad y que fueron comunicados a la Superintendencia de Industria y Comercio, proveedores de tecnologías y servicios de seguridad, podrán ser tratados exclusivamente		

certicámara.

	durante el tiempo y alcance necesario para su análisis, detección protección y respuesta ante el incidente y adoptando medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado		
50.	**Artículo 50. Comunicación de un Incidente de seguridad de los datos personales al titular.** 1. Cuando sea probable que el Incidente de seguridad de los datos personales entrañe un alto riesgo para los derechos y garantías de las personas naturales, el responsable del tratamiento lo comunicará al titular sin dilación indebida. 2. La comunicación al titular contemplada en el numeral 1 del presente artículo deberá describir en un lenguaje claro y sencillo la naturaleza del Incidente de seguridad de los datos personales y contendrá como mínimo la información y las	Solicitamos se aclare qué factores determinan que un incidente de seguridad constituya un alto riesgo para los derechos y garantías de los titulares. Lo anterior, teniendo en cuenta que en la práctica, no tiene utilidad informar todo tipo de incidentes al titular de los datos, por el contrario, esto podría generar pánico masivo, debido a que hay incidentes que no generan un perjuicio o afectación al titular.	

	medidas a que se refiere el artículo 49, numeral 3, literales b), c) y d). 3. La comunicación al titular a la que se refiere el numeral 1 no será necesaria si se cumple alguna de las condiciones siguientes: a) El responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por el Incidente de seguridad, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado; b) El responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y garantías del titular a que se refiere el numeral 1;		

certicámara.

	4. Cuando la comunicación a los titulares suponga un esfuerzo desproporcionado para el responsable del tratamiento, éste podrá optar por una comunicación pública o una medida de difusión semejante por la que se informe de manera igualmente efectiva a los titulares. 5. Cuando el responsable no haya comunicado al titular el Incidente de seguridad de los datos personales, la Superintendencia de Industria y Comercio, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo comunique o podrá confirmar que se cumple alguna de las condiciones mencionadas en el numeral 3.		
52	**Artículo 52. Consulta previa.**	Solicitamos amablemente, indicar ¿cuáles son los criterios con base en los cuales se determine el “alto riesgo” en la	

	1. El responsable del tratamiento consultará ante la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio antes de llevar a cabo un tratamiento cuando, de la evaluación de impacto de que trata del artículo 51, se concluya que dicho tratamiento supondría un alto riesgo para los derechos y garantías de los titulares. 2. Cuando la Delegatura para la Protección de Datos Personales considere que el tratamiento previsto en el numeral 1 suponga un alto riesgo para los derechos y garantías de los titulares, asesorará por escrito al responsable, y en su caso al encargado, entre otras cosas respecto de las medidas técnicas y organizativas que se deberán adoptar previo al tratamiento de los datos. La Delegatura para la Protección de Datos	garantía de los derechos de los titulares.	

	Personales deberá, en un plazo de 3 meses contados a partir de la fecha en que el responsable, o en su caso el encargado, acude ante ella, emitir un concepto. Este plazo podrá prorrogarse, en función de la complejidad del tratamiento, por única vez, por un periodo igual a la inicial, informando al responsable y, en su caso, al encargado del tratamiento de tal prórroga, indicando los motivos de la dilación. 3. El escrito que el responsable del tratamiento allegue a la Superintendencia de Industria y Comercio deberá contener como mínimo la siguiente información: a) En caso de ser procedente, las responsabilidades respectivas del responsable, y los encargados implicados en el tratamiento, en particular en caso de		

certicámara.

	tratamiento dentro de un grupo empresarial; b) Los fines y medios del tratamiento previsto; c) Las medidas establecidas para proteger los derechos y garantías de los titulares de conformidad con la presente Ley; d) En su caso, los datos de contacto del oficial de protección de datos; e) La evaluación de impacto relativa a la protección de datos establecida en el artículo 51 de esta ley; f) Cualquier otra información que solicite la autoridad nacional de protección de datos. Parágrafo: Cuando la Superintendencia de Industria y Comercio deba requerir información y/o documentación adicional, los términos establecidos en el numeral 2 del presente artículo se suspenderán hasta que la información		

certicámara.

	y/o documentación se haya obtenido o hasta que el plazo otorgado para suministrarlos, se haya cumplido.		
103	**Artículo 103. Plazos para la implantación de las medidas de seguridad.** La implantación de las medidas de seguridad previstas en la presente ley deberá producirse con arreglo a las siguientes reglas: 1. Respecto de las bases de datos que existieran al momento de la entrada en vigencia de la presente ley se llevara a cabo de la siguiente manera: a) En el plazo máximo de dieciocho meses desde su entrada en vigencia, deberán implantarse las medidas de seguridad en bases de datos automatizadas. b) Respecto de las bases de datos no automatizadas que existieran al momento de la entrada en vigencia de la presente ley, en el plazo máximo de un año. 2. Las bases de datos, tanto automatizadas	Al ser un Proyecto de Ley que generará gran impacto en las empresas que manejan datos personales como encargados o responsables y en la ciudadanía en general. Consideramos importante que se establezcan rangos de cumplimiento en virtud del número de titulares que se manejen en cada empresa, se tenga un régimen de transición de mayor o menor término según sea el caso. Pues, resultan muy cortos los siguientes términos: • Consentimiento: solo será válido el consentimiento de los titulares recabados con anterioridad a la expedición de esta ley un **año posterior a la entrada en vigencia**, plazo en cuál el responsable del tratamiento deberá obtenerlos en las condiciones previstas en la presente ley o legitimar el tratamiento en otra base jurídica.	

	como no automatizadas, creadas con posterioridad a la fecha de entrada en vigencia de la presente ley deberán tener implantadas, desde el momento de su creación la totalidad de las medidas de seguridad reguladas en esta ley.
	Parágrafo: A requerimiento de la Superintendencia de Industria y Comercio el responsable de Tratamiento deberá demostrar que está llevando a cabo la implementación de las medidas de seguridad en las bases de datos existentes en el momento de la entrada en vigencia de la presente ley.
		• Bases de datos: existieran al momento de la entrada en vigencia de la presente ley se llevará a cabo de la siguiente manera;
		  • En el plazo **máximo de dieciocho meses desde su entrada en vigencia**, deberán implantarse las medidas de seguridad en base de datos automatizadas.
		  • Respectos de las bases de datos no automatizadas que existieran al momento de la entrada en vigencia de la presente ley, en el **plazo máximo de un año**.
		• Los contratos de encargado del tratamiento suscritos con anterioridad a esta ley serán válidos hasta **dieciocho meses después** de su entrada en vigencia. Durante dicho plazo cualquiera de las partes podrá exigir	

certicámara.

		a la otra modificación del contrato. Si bien, consideramos que los datos personales de los ciudadanos colombianos tienen que ser tratados de la mejor manera y bajo la urgencia correspondiente. Estos términos resultarán más difíciles para empresas que administran alto volumen de datos personales, por lo que sugerimos se evalúe términos distintos según el tamaño de la empresa el régimen de transición y se pueda dar un cumplimiento real y efectivo de las disposiciones que contiene este Proyecto de Ley. Lo anterior, contribuirá al correcto tratamiento de datos personales por parte de las empresas que son responsables o encargados de los datos de los ciudadanos, pues incluye la perspectiva de empresas que propenden por el buen manejo de datos personales.	

Agradecemos su atención a las observaciones anteriormente presentadas.

Cordialmente,

CERTICÁMARA S.A.

Etiquetado:	Externo

certicámara.

Carrera 7 No. 26 - 20 Piso 18 / Edificio Seguros Tequendama
www.certicamara.com
Ventas, servicio al cliente y soporte: (601) 744 2727
Línea administrativa: (601) 745 2141

CONGRESO DE LA REPÚBLICA DE COLOMBIA
CÁMARA DE REPRESENTANTES

Debates Comisión Primera <debatescomisionprimera@camara.gov.co>

Comentarios Proyecto de Ley 156 de 2023 Cámara

Javier Enrique Sandoval Gómez <jsandoval@sandovalconsultores.com> 5 de marzo de 2024, 2:40 p.m.
Para: debatescomisionprimera@camara.gov.co

Señores
MESA DIRECTIVA
COMISIÓN PRIMERA CONSTITUCIONAL
CÁMARA DE REPRESENTANTES
COLOMBIA

Asunto: Comentarios Proyecto de Ley 156 de 2023 Cámara por la cual se dictan disposiciones para el Régimen General de Protección de Datos Personales

Reciban un cordial saludo.

Mi nombre es Javier Enrique Sandoval Gómez, soy Administrador de Empresas, y desde hace más de 14 años he venido trabajando y estudiando el Régimen Colombiano de Protección de Datos Personales en Colombia, constituido básicamente por la Ley 1266 de 2008 y la Ley 1581 de 2012, más sus leyes, decretos, jurisprudencia, doctrina y documentos orientativos de la Superintendencia de Industria y Comercio.

Es por esta razón, que les escribo, en particular por la discriminación que se incluyó en el numeral 4 del artículo 54 y el artículo 55 en donde el proyecto de ley establece que, para ser Oficial de Protección de Datos Personales se debe tener *"titulación universitaria que acredite conocimientos especializados en Derecho"*. Esto, a todas luces, **refleja discriminación** hacia todas aquellas personas que somos profesionales en otras disciplinas pero tenemos el suficiente conocimiento, como en mi caso, de más de 14 años en el tema.

Con todo respeto quiero comentarles que, no sólo los abogados tienen la capacidad de diagnosticar, diseñar, documentar, implementar, evaluar y hacer seguimiento a los Programas Integrales de Gestión de Datos Personales. Es más, en mi caso, yo le genero conceptos sobre el tema a los abogados para que ellos proyecten las respectivas respuestas cuando es necesario.

Esto es como si, por otro lado, los Oficiales de Cumplimiento deban ser abogados porque es una ley la que exige la implementación del sistema de lavado de activos y financiación del terrorismo. O que las personas encargadas de los programas de seguridad y salud en el trabajo deban ser abogadas porque es una ley la que obliga a los empleadores contar con la implementación del programa de seguridad y salud en el trabajo.

Adicionalmente, hoy en día, cuando la figura del OPD no es obligatoria per sé, muchas organizaciones ya lo han designado, y, en muchos casos, tienen una profesión diferente a la del derecho.

Eso quiere decir que el PL 156/2023 obligará a las empresas a despedir a esas personas o a que no contraten los servicios a quienes no somos graduados en derecho pero que hemos dedicado gran parte de nuestras vidas profesionales a estudiar y trabajar este tema. Es más, en Linkedin ya sólo se están ofertando perfiles para Oficiales de Protección de Datos Personales sólo para abogados, lo que hace que quienes prestamos nuestros servicios en el tema y no lo seamos abogados no tenemos oportunidad de participar.

Si ustedes pueden revisar las legislaciones en otros países, en ninguna de ellas limitan el ejercicio del OPD a una profesión académica en particular, todo lo contrario, lo dejan abierto pero se enfocan en los altos niveles de conocimiento y ejercicio en el tema. Es más, ni siquiera la Superintendencia de Industria y Comercio, siendo hoy la autoridad colombiana en protección de datos personales, ha limitado el ejercicio del OPD a una profesión académica específica.

Ahora bien, con este PL, todas las personas involucradas "arrancaremos" de cero, tengamos la profesión que tengamos. Todos tendremos que participar en las respectivas capacitaciones y formaciones que la autoridad colombiana imparta sobre la nueva legislación.

Por esta razón, le solicito a los Honorables Representantes de la Comisión Primera de la Cámara que pueda eliminar esta discriminación y permitir que el OPD pueda tener cualquier profesión académica pero con altos estándares de conocimiento y experiencia, pues, como está actualmente, muchas personas nos veremos perjudicadas al no tendríamos oportunidad de trabajar en lo que hemos venido trabajando durante muchos años de nuestras vidas.

--
Cordialmente;

JAVIER ENRIQUE SANDOVAL GÓMEZ
* Experto en el Régimen General de Protección de Datos Personales
* Consultor en la implementación de Programas Integrales de Gestión de Datos Personales
* Auditor de Programas Integrales de Gestión de Datos Personales
* Formador de Oficiales de Protección de Datos Personales
LinkedIn

CONGRESO DE LA REPÚBLICA DE COLOMBIA
CÁMARA DE REPRESENTANTES

Debates Comisión Primera <debatescomisionprimera@camara.gov.co>

Intervención Audiencia Pública - Proyecto de Ley Estatutaria N° 156 de 2023 Cámara de Representantes

Julian Alberto Paez Vargas <j.paez.v@hotmail.com> 6 de marzo de 2024, 7:20 a.m.
Para: "debatescomisionprimera@camara.gov.co" <debatescomisionprimera@camara.gov.co>

Respetados miembros de la Comisión Primera de la Cámara de Representantes:

Cordial saludo. Atendiendo a las instrucciones del formulario de inscripción, relaciono los puntos principales de las observaciones que realizaría en la audiencia pública del proyecto de ley de la referencia:

1. Importancia de la reforma del régimen general de protección de datos personales establecido en la Ley 1581 de 2012, describiendo particularmente el estado de Colombia en el mundo, en lo que respecta al tratamiento de datos personales y el por qué múltiples sectores del país se verían beneficiados de las disposiciones establecidas en el proyecto de ley.
2. Comentario sobre el régimen general de datos en Europa y la experiencia como experto en datos viviendo en Alemania, país mundialmente reconocido por ser uno de los más estrictos en cuanto a la protección de datos se refiere. Lo anterior, considerando que la Ley 1581 de 2012 parte del Derecho Español y que el nuevo proyecto de ley equipara a Colombia con el sistema europeo.
3. Argumentación favorable en torno a las herramientas novedosas dispuestas por el proyecto, relacionadas con la anonimización, el derecho al olvido, los neuro datos y la inteligencia artificial.

Considerando que en este momento estoy domiciliado en Berlín Alemania, agradecería contemplar la posibilidad de realizar mi participación de manera virtual.

Sin otro particular,

Julián Páez Vargas
Abogado
Especialista en Filosofía del Derecho
Docente Universitario
Estudiante Maestría en Política Pública | Hertie School, Berlín Alemania

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Fecha: 2024-03-07 11:35:38 Folios: 17
Radicado: 242021202
Destino: CAMARA DE REPRESENTANTES CONGRESO DE -

Código TRD: 1000

Bogotá D.C.

Honorable Representante
DUVALIER SÁNCHEZ ARANGO
CONGRESO DE LA REPÚBLICA
Edificio Nuevo del Congreso, OF 504B - 505B
Correo: duvalier.sanchez@camara.gov.co

Asunto: Comentarios al Proyecto de Ley Estatutaria Número 156 de 2023 Cámara "Por la cual se dictan disposiciones para el Régimen General de Protección de Datos Personales".

Respetado Representante:

Reciba un cordial saludo del Ministerio de Tecnologías de la Información y las Comunicaciones (Ministerio de TIC o MinTIC).

A continuación, amablemente presentamos las consideraciones de este Ministerio frente al proyecto de ley relacionado en el asunto, en el marco de nuestras competencias:

Lo anterior, toda vez que, si bien el MinTIC no detenta calidad de autoridad de protección de datos en el país, si se encuentra facultado para participar en la formulación de las políticas públicas que rigen el sector de las Tecnologías de la Información y las Comunicaciones.

En particular, el principio de protección de los derechos de los usuarios descrito en el numeral cuarto del artículo 2 de la Ley 1341 de 2009, *"por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones"*, señala expresamente que *"[…] El Estado velará por la adecuada protección de los derechos de los usuarios de las Tecnologías de la Información y de las Comunicaciones,* ***así como por el cumplimiento de los derechos y deberes derivados del Hábeas Data****, asociados a la prestación del servicio. Para tal efecto, los proveedores y/u operadores directos deberán prestar sus servicios a precios de mercado y utilidad razonable, en los niveles de calidad establecidos en los títulos habilitantes o, en su defecto, dentro de los rangos que certifiquen las entidades competentes e idóneas en la materia y con información clara, transparente, necesaria, veraz y anterior, simultánea y de todas maneras oportuna para que los usuarios tomen sus decisiones"* (negrillas fuera del texto).

I. Actual Régimen General de Protección de Datos

La Ley 1581 de 2012, *"por la cual se dictan disposiciones generales para la protección de datos personales"* fue una necesidad de regulación que nace con ocasión del artículo 15 de la Constitución Política de 1995, que establece el derecho fundamental 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, denominado por la jurisprudencia constitucional como derecho al *"habeas data"*.

Sin embargo, con ocasión de los avances tecnológicos y la masificación del tratamiento de datos personales a niveles transfronterizos, se han presentado propuestas de reformas en diferentes jurisdicciones que invitan a adecuar el régimen normativo a las nuevas realidades y a optar por una postura más proteccionista. Es el caso del Reglamento General de Protección de Datos Personales del Parlamento Europeo (2016/679), expedido en 2016, con vigencia desde 2018 y convertido en el estándar internacional más alto en la materia, así como el California Consumer Privacy Act – CCPA, el cual propendió por una visión anglosajona frente a la posibilidad de recopilar información personal de los consumidores por varias fuentes en redes de publicidad, proveedores de servicios, análisis de datos, entidades gubernamentales, sistemas operativos y plataformas digitales, bajo un enfoque mercantil propio de dicho sistema.

En Colombia, estos avances fueron recogidos en las guías y lineamientos expedidos por la autoridad de protección de datos personales en el país, que es la Delegatura de Protección de Datos Personales de la Superintendencia de Industria y Comercio, en virtud de lo dispuesto por el Titulo VII, Capitulo I de la Ley 1581 de 2012.

Ahora bien, en tanto se trata de un derecho fundamental de orden constitucional concebido en el artículo 15 de la Constitución Política, también ha sido objeto de desarrollo por parte de la Corte Constitucional, quien determinó que el derecho al *habeas data* no se agota por lo expresado en dicho artículo y en la ley, sino que existe un núcleo esencial del derecho al *habeas data*, lo que excluye el carácter mercantil previsto en otros ordenamientos jurídicos.

De hecho, la Corte definió el *habeas data* como: "Aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización, y certificación de los datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de bases de datos personales"[1], lo que permite dar una interpretación extensiva de lo que ya se encontraba establecido en la Constitución Política y que identifica que este derecho fundamental al *habeas data* tiene amplia relación con el ejercicio de otros derechos fundamentales, razón por la cual la Corporación estableció que la colisión de derechos sobre este tópico debe someterse a juicios de ponderación y es la razón por la cual aún se presentan pronunciamientos de fondo sobre el ejercicio de este derecho fundamental en el Alto Tribunal.

II. Proyecto de Ley de Reforma

De acuerdo con la revisión efectuada al Proyecto de Ley 156/2023C, se identifica que este busca hacer una reforma de fondo al Régimen General de Protección de Datos Personales en el país, por lo que se derogaría la Ley 1581 de 2012 y se promulgarían nuevas condiciones en la materia. En este sentido, conviene efectuar observaciones sobre aquellos artículos que son viables, pero requieren ajustes, así como aquellos sobre los cuales existe inconveniencia, al contrariar otras normas previstas en el ordenamiento.

ARTÍCULO DEL PROYECTO DE LEY	COMENTARIO
Artículo 2. Ámbito de aplicación material.	Se sugiere modificar el inciso 1 del artículo de la siguiente manera: "*La presente ley se aplica al tratamiento total o parcialmente automatizado, así como el tratamiento no automatizado de los datos personales".* Igualmente, se sugiere modificar el literal c) del numeral 2 de la siguiente manera: *"Por parte de las autoridades competentes con fines de prevención, investigación, detección o procesamiento judicial de actos delictivos, o la ejecución de sanciones penales, así como la de protección frente a amenazas a la seguridad nacional pública y*

[1] CORTE CONSTITUCIONAL DE COLOMBIA. Sentencia de Tutela 729 de 2002. Magistrado ponente: Eduardo Montealegre Lynett, 2002.

	su prevención". Lo anterior, obedece a aplicar mayor seguridad jurídica, por cuanto no son claras las características para determinar que un dato es susceptible de ser incluido en una base de datos. Por otro lado, el inciso 2, al mencionar situaciones particulares como el lavado de activos reduce el ámbito de aplicación de este.
Artículo 4. Datos de personas fallecidas	Se sugiere respetuosamente incluir las condiciones o requisitos para que un causahabiente pueda ejercer derechos en nombre del causante y a su vez, incluir lo pertinente frente a los testamentos que puedan incluir este tipo de disposiciones, ya que la persona cuenta con la libertad de disponer libremente sobre la supresión de sus datos personales al fallecer. Para garantizar seguridad jurídica y coherencia legislativa, sugerimos establecer los requerimientos mínimos para hacer uso de este derecho, la forma de las autorizaciones y la administración de las evidencias que soportan la voluntad del causante. Igualmente, la ley debe ser armónica con preceptos establecidos en el código civil o estatuto notarial frente al régimen de los testamentos y las sentencias emitidas por la Corte Constitucional en la materia.
Artículo 5. Definiciones	Se sugiere respetuosamente suprimir el término de "*Base de datos de riesgo crediticio*", ya que este corresponde al ámbito de aplicación de la Ley 1266 de 2008, modificada y adicionada por la Ley 2157 de 2021. Igualmente, deben eliminarse las definiciones de "*elaboración de perfiles*", "*incidente de seguridad*", "*neurodato*", "*servicio de la sociedad de la información*" y "*usuario*", en tanto que es competencia del Ministerio de Tecnologías de la Información y las Comunicaciones, con el apoyo técnico de la CRC, expedir el glosario de definiciones acordes con los postulados de la UIT y otros organismos internacionales con los cuales sea Colombia firmante de protocolos referidos a estas materias, en los términos previstos por el artículo 6 de la Ley 1341 de 2008, modificado por el Artículo 5 de la Ley 1978 de 2019.
Artículo 6. Principios relativos al tratamiento.	Se sugiere respetuosamente suprimir la mención del principio de neutralidad tecnológica, ya que no lo define y entra en conflicto con la definición dispuesta por el artículo 2 de la Ley 1341 de 2009. Se sugiere la reducción de principios, ya que su finalidad debe ser la de brindar claridad y facilitar la interpretación de la ley como criterio auxiliar.
Artículo 8. Condiciones para el consentimiento	En relación con el numeral 6 del artículo, sugerimos modificación de la siguiente manera: "*El titular tendrá derecho a revocar su consentimiento en cualquier momento. La revocatoria del consentimiento no afectará a la legalidad del tratamiento basada en el consentimiento previo a la revocatoria. Para revocar el consentimiento, el titular deberá acreditar previamente su identidad y el responsable podrá cesar la prestación de los servicios cuando los datos personales sean*

	necesarios para tal fin". Se sugiere la inclusión de la verificación de la identidad del titular para evitar prácticas de suplantación en la revocación del consentimiento, que ocasionen perjuicios a los titulares de los datos. Igualmente, debe incluirse la consideración práctica frente a los elementos esenciales de la prestación del servicio, pues en muchos casos este necesario para ejercicio de funciones o prestación de servicios y en caso de no interrumpirlos podría afectar a los responsables y su conformidad legal frente a la presente Ley.
Artículo 10. Condiciones para el tratamiento en la ejecución de un contrato	Se sugiere modificar el numeral 3 en el siguiente sentido: *" A La contratación que se lleve a cabo por entidades públicas, le será aplicable los principios y, demás, obligaciones establecidas en la presente ley siempre y cuando no choquen con otros principios establecidos en Ley 1712 de 2014, Ley 80 de 1993, Ley 1150 de 2007 y aquellas que la modifiquen, deroguen o adicionen".* Por técnica legislativa y de acuerdo con el criterio de especialidad, se debe establecer la armonía de la norma con el régimen especial de transparencia y acceso a la información pública.
Artículo 13. Condiciones para el tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de funciones públicas conferidas al responsable.	Se sugiere modificar el artículo en el siguiente sentido: *"2. Cuando se habla de una misión realizada en interés público o en ejercicio de funciones públicas, la misma puede ser llevada a cabo por un responsable de naturaleza pública o privada".* A su vez, se recomienda la eliminación del numeral 3. Las funciones públicas son atribuidas por ministerio de la Ley y no debería ser objeto de decisión particular si una entidad es idónea o no para ejercer dichas funciones o llevar a cabo una misión de interés público. Por otro lado, el numeral 3 confunde el régimen aplicable a quienes ejercen funciones públicas de aquellos que no lo hacen, y en tal sentido, no se encuentra pertinente incluir dicho numeral. Lo anterior, dado que puede generar incertidumbre y cargas excesivas para las entidades del sector.
Artículo 14. Condiciones para el tratamiento necesario para la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero.	Se sugiere la eliminación del artículo, debido a que impone un numero de requisitos de manera inclusiva y no facultativa, lo cual genera cargas desmedidas para que la base legal de intereses legítimos pueda ser utilizada.
Artículo 15. Tratamiento de datos sensibles	Se sugiere modificar el literal g)del numeral 2 para reflejar las situaciones en que se requieren estos tratamientos en el ejercicio de la función pública, para lo cual proponemos la siguiente redacción: *"Cuando el tratamiento sea necesario por razones de interés público o necesario para la prestación de servicios públicos o por parte de entidades que ejerzan funciones públicas, de acuerdo*

	con la base de la normativa que faculta para ejercer dichas funciones, debe ser proporcional al objetivo perseguido, respetando el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los derechos y garantías fundamentales del titular".
Artículo 16. Tratamiento de datos personales relativos a delitos y condenas penales	En nuestra consideración, el artículo podría entrar en conflicto con los presupuestos establecidos en la Ley 1712 de 2014, pues existe una obligación de transparencia y acceso a la información pública alrededor de los funcionarios públicos, contratistas y colaboradores de la administración pública. En este contexto, la sentencia T-098 de 2017 de la Corte Constitucional enfatizó sobre la relevancia de la conservación de los antecedentes penales, pues atiende a finalidades constitucionales y legales legítimas respecto de la moralidad de la función pública, aplicación de la ley penal, actividades de inteligencia y la ejecución de la ley.
Artículo 17. Tratamiento de datos relativos a infracciones y sanciones administrativas	En nuestra consideración, la información relativa a las infracciones y sanciones administrativas atiende a finalidades constitucionales y legales legítimas respecto de la moralidad de la función pública, aplicación de la ley penal, actividades de inteligencia y la ejecución de la ley, tal como se señaló en el comentario previo. La Ley 1712 de 2015 coacciona a los sujetos obligados a conservar los datos personales concernientes a la vinculación de funcionarios, contratistas y colaboradores, por lo que resulta necesario efectuar el tratamiento.
Artículo 32. Derecho a la portabilidad de los datos.	Se sugiere modificar el numeral 3 de la siguiente manera, con el fin de contemplar el máximo de los casos de excepción: *"El ejercicio del derecho mencionado en el numeral 1 del presente artículo se entenderá sin perjuicio del artículo 27. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público, en el ejercicio de poderes o funciones públicas conferidas al responsable del tratamiento".*
Artículo 33. Derecho de oposición.	Se sugiere incluir en el artículo un parágrafo estableciendo que: *"Parágrafo. Cuando el titular se oponga al tratamiento de sus datos personales el responsable cesará la prestación del servicio cuando los datos personales del titular sean necesarios para este fin".* Dicha modificación es esencial para que los responsables pueden asegurar la prestación de servicios en conformidad con los requerimientos presentes en la Ley.
Artículo 34. Decisiones individuales automatizadas, incluida la elaboración de perfiles.	Se sugiere eliminar el numeral 3, pues contraviene el carácter de excepción mencionado en el numeral 2, en efecto, si se establecen ciertas excepciones al artículo, los casos de excepción no deberían ser castigados con cargas excesivas de requerimientos adicionales, los cuales pueden afectar a su vez

	el uso de mecanismos de automatización.
Artículo 36. Derecho a presentar una denuncia ante la Autoridad de Control.	Se sugiere detallar los requisitos para instaurar una denuncia ante los entes de control, establecer claramente los requisitos para que una denuncia anónima sea procedente y la descripción de las sanciones que pueden acarrear este tipo de denuncias. Es necesario modificar el artículo con el fin de garantizar la seguridad jurídica y la coherencia con otras normas existentes en materia de denuncias anónimas (Ej: Ley 962 de 2005, Ley 24 de 1992)
Artículo 37. Obligaciones del responsable del tratamiento.	Se sugiere eliminar el numeral 3 del artículo por no tratarse de una obligación del responsable, ya que el contenido del mismo no constituye una obligación y en caso de incluir en el listado del articulo podría dar pie a malinterpretación de la ley y generar cargas injustificadas sobre el responsable del tratamiento. A su vez, sugerimos definir el término “novedades”, del que trata el numeral 4, para aclarar si se trata de incidentes, cambios en la política de datos interna o en la infraestructura o cualquier otro evento que se considere aplicable, así como, elimiarel periodo de tiempo de dos años para la revisión periódica de los sistemas de información , contenido en el numeral 9 de ese artículo. La inclusión de una revisión periódica cada dos años, sin mediar condición especial o aclarar los tipos de novedades por los cuales debería realizarse una revisión implica una carga económica sin justificación, la cual puede impactar negativamente el funcionamiento del responsable.
Artículo 38. Protección de datos desde el diseño y por defecto.	Sugerimos respetuosamente eliminar este artículo en el texto de ponencia, pues la actualización de medidas técnicas y administrativas para cumplir con los principios de protección de datos personales desde el diseño implica una carga económica y técnica que impactaría negativamente al responsable y desconocería las medidas actualmente en uso. Generar un sobrecosto para las entidades, empresas y personas que ostentan la calidad de responsable y puede impactar negativamente diferentes sectores de la economía.
Artículo 40. Representantes de responsables o encargados del tratamiento con domicilio fuera del territorio Nacional.	Sugerimos respetuosamente eliminar este artículo en el texto de ponencia, porque comporta una carga injustificada para las empresas extranjeras que prestan servicios en Colombia y puede ocasionar desincentivo a la prestación de servicios de multinacionales en el país, afectando los mercados, la innovación, la competencia y en última instancia a los usuarios/ clientes/ beneficiarios de dichas empresas.
Artículo 43. Registro de las actividades de tratamiento.	Se sugiere incluir los casos de excepción para los cuales esta obligación no aplicaría. Se recomienda incluir la siguiente excepción: “*No se aplicará a una empresa u organización que emplee a menos de 200 personas, a menos que el tratamiento que lleve a cabo pueda suponer un riesgo para los derechos y libertades de los interesados, el tratamiento no sea ocasional o el tratamiento*

	incluya las categorías especiales de datos a las que se refiere el artículo 15 numeral 1". En concordancia con la Ley 590 de 2000 se requiere establecer un marco especial para la micro, pequeña y mediana empresa en Colombia con el fin de promover el desarrollo integral de este tipo de compañías y los mercados alrededor de las mismas. En efecto, de no tenerse consideración particular se establecerían cargas administrativas de gran envergadura, las cuales pueden convertirse en barreras para el desarrollo de este tipo de empresas.
Artículo 48. Medidas de seguridad en el ámbito del sector público.	Se identifica que este artículo invade las competencias del Ministerio de Tecnologías de la Información y las Comunicaciones respecto a lo que atañe a la Política de Gobierno Digital y Seguridad Digital, como políticas del Modelo Integrado de Gestión de la Función Pública, ya que involucra aspectos de seguridad de la información. Así las cosas, resulta necesario precisar que la seguridad y privacidad de la información del sector público constituye un habilitador de la ejecución de la Política de Gobierno Digital y el elemento fundamental de la Política de Seguridad Digital de las cuales es líder el Ministerio de TIC por lo que los sujetos obligados, es decir, todos los que relaciona el artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones administrativas, tienen la obligación de desarrollar capacidades para la implementación de los lineamientos de seguridad y privacidad de la información expedidos por el Ministerio de Tecnologías de la Información y las Comunicaciones. Al respecto y en cumplimiento de la determinación legal, fue reglamentado por el Gobierno Nacional en el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones (Decreto 1078 de 2015), normativa que en el artículo 2.2.9.1.1.2. establece que: *"Los sujetos obligados a las disposiciones contenidas en el presente Capítulo serán las entidades que conforman la administración pública en los términos del artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones administrativas"*. Así mismo, el artículo 2.2.9.1.2.1 de la misma norma, manifiesta que la Política de Gobierno Digital se compone de una estructura que involucra elementos de gobernanza, innovación pública digital, habilitadores, líneas de acción e iniciativas dinamizadoras, dentro de los cuales resaltan los habilitadores como capacidades que permitan ejecutar las líneas de acción de la Política de Gobierno Digital. En tal sentido, se sugiere la inclusión de un párrafo que señale: "Todas las entidades de la administración pública deberán adelantar las acciones que señale el Gobierno nacional a través del Ministerio de Tecnologías de la Información y las Comunicaciones para la implementación de la Política de Gobierno Digital". En desarrollo de la mencionada Política se establece que, la seguridad y privacidad de la información hace parte de dichos habilitadores, de manera que propende por el desarrollo de capacidades en aplicación de los

	lineamientos de seguridad y privacidad de la información, hoy dispuestos reglamentariamente en los términos establecidos por el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015 de la siguiente manera: "[...] Habilitadores: Los sujetos obligados desarrollarán las capacidades que les permitan ejecutar las Líneas de Acción de la Política de Gobierno Digital, mediante la implementación de los siguientes habilitadores: [...] 3.2. Seguridad y privacidad de la información: Este habilitador busca que los sujetos obligados desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos". Lo anterior se concatena con lo señalado en el numeral 12 del artículo 2.2.22.2.1. del Decreto 1083 de 2015, "Decreto Único Reglamentario del Sector Función Pública", el cual indica que la política de Seguridad Digital forma parte de las políticas de Gestión y Desempeño Institucional, y en concordancia, el numeral 5 del artículo 2.2.22.3.6 del mismo Decreto define como una de las funciones de los Comités Sectoriales de Gestión y Desempeño "[d]irigir y articular a las entidades del sector administrativo en la operación de las políticas de gestión y desempeño y de las directrices impartidas por la Presidencia de la República y el Ministerio de Tecnologías de la Información y las Comunicaciones en materia de Gobierno y Seguridad digital". En esta medida, la seguridad y privacidad de la información hace parte integral de la Política de Gobierno Digital, la cual es de obligatorio cumplimiento, en los términos señalados por el artículo 230 de la Ley 1450 de 2011, modificado por el artículo 148 de la Ley 1955 de 2019, al señalar que "[t]odas las entidades de la administración pública deberán adelantar las acciones que señale el Gobierno nacional a través del Ministerio de Tecnologías de la Información y las Comunicaciones para la implementación de la política de Gobierno Digital", en donde destaca el cumplimiento de los lineamientos y estándares para el incremento de la confianza y la seguridad digital. Así, con fundamento en las competencias determinadas por el Legislador se expidieron la Resolución 500 de 2021, "[p]or la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital" y el Decreto 338 de 2022, que adiciona el Título 21 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, como parte de la estrategia de la Política Nacional de Confianza y Seguridad Digital, Conpes 3995 de 2020).

	En particular, la Política de Gobierno Digital ya hoy establece definiciones tales como ciberdefensa, gobernanza de la seguridad digital para Colombia, riesgo de seguridad digital, seguridad de la información y seguridad digital. En consecuencia, existe un riesgo de antinomia entre el artículo del proyecto de ley al involucrar a otras entidades públicas en cuestiones de seguridad de los datos personales, ya que existe un marco jurídico robusto que comprende una estrategia de ciberseguridad multisectorial delimitada por el numeral 8 del artículo 2 de la Ley 1341 de 2009, el numeral 2 del artículo 17 de la Ley 1341 de 2009, el artículo 64 de la Ley 1437 de 2011, los artículos 2.2.9.1.2.1, 2.2.9.1.2.1 y 2.2.21.1.1.3. del Decreto 1078 de 2015, el numeral 12 del artículo 2.2.22.2.1. y el numeral 5 del artículo 2.2.22.3.6 del Decreto 1083 de 2015, el Conpes 3854 de 2016 sobre la Política Nacional de Seguridad Digital, el artículo 147 de la Ley 1955 de 2019, el artículo 230 de la Ley 1450 de 2011 (modificado por el artículo 148 de la Ley 1955 de 2019), el Conpes 3995 de 2020 sobre la Política Nacional de Confianza y Seguridad digital.
Artículo 49. Notificación de un incidente de seguridad de los datos personales a la Autoridad de Control.	Por claridad de la norma se sugiere modificar el termino incluido en el numeral 1 de “tenido constancia“ por ” tenido conocimiento”. Igualmente, se sugiere mantener el estándar actual de reporte de un incidente de seguridad a la autoridad competente. El término constancia describe de manera confusa a partir de cuándo comienza el plazo para notificar a la autoridad, es por ello que se requiere incluir un lenguaje más directo. El plazo de 72 horas es mucho más exigente que el estándar actual y puede no corresponder a las acciones técnicas que se deben realizar, en efecto un incidente requiere de un análisis inicial para determinar si corresponde a un incidente o no; así que 72 horas desde el conocimiento del evento no es un tiempo suficiente y parece más adecuado 15 días.
Artículo 51. Evaluación de impacto relativa a la protección de datos.	Se sugiere ajustar las expresiones “Observación sistemática a gran escala” y “alto riesgo”, ya que no es posible determinar su alcance en la redacción actual. A su vez, se sugiere en el numeral 4 establecer que la evaluación de impacto solo se realizara posterior a la publicación por parte de la Superintendencia de Industria y Comercio, con fundamento en la lista de los tipos de operaciones de tratamiento que requieran dicha evaluación. Por técnica legislativa, claridad y seguridad jurídica se sugiere incluir el significado de los dos términos mencionados y así evitar controversias en la implementación de la norma, al igual que garantizar la aplicación correcta de la misma a partir de los lineamientos de la SIC.
Artículo 52. Consulta previa.	La consulta previa obligatoria implica una barrera al desarrollo de actividades de los responsables, la espera por un concepto de la autoridad para realizar el tratamiento puede constituir un desincentivo para que las empresas y entidades adopten los procedimientos de evaluación de impacto, esto con el fin de evitar dilaciones en las actividades.
Artículo 53. Designación del Oficial de protección de datos.	El artículo contempla obligaciones asociadas a la prestación del servicio de telecomunicaciones y servicios de la sociedad de la información, por lo que

	involucra las definiciones previstas en la Ley 1341 de 2009, cuyo artículo 3 describe que hace parte de la sociedad de la información y el conocimiento "[...] el despliegue y uso eficiente de la infraestructura, el desarrollo de contenidos y aplicaciones, la protección a los usuarios, la formación de talento humano en estas tecnologías y su carácter transversal". Así las cosas, no hay claridad sobre el alcance de la protección de los derechos previstos en el proyecto de ley, en aquellos casos en los cuales la autoridad de datos personales carezca de competencias jurisdiccionales frente aquellos casos de carácter extraterritorial. Si bien el proyecto de ley se inspira en el RGPD del Parlamento Europeo, hay que considerar que nuestra jurisdicción no cuenta con la misma integración economía y política de dicho territorio.
Artículo 54. Calidades del Oficial de protección de datos	Se sugiere suprimir los numerales 2 y 3, toda vez que cada autoridad u organismo público constituye una persona jurídica diferente y por ende las condiciones de la organización varían dimensión y alcance de la Política Integral de Protección de Datos Personales. Resulta necesario ajustar la redacción del numeral 4, ya que es un despropósito restringir el rol de Oficial de Datos Personales a la profesión de abogado. En la actualidad, los programas de posgrado en el país para derecho informático, derecho de las telecomunicaciones, derecho de las TIC, innovación legal, seguridad de la información, seguridad informática, ciberseguridad, legaltech o privacidad permiten que cualquier profesional tenga la posibilidad de acceder a dicha formación, sin necesidad de ser jurista. No hay claridad sobre el alcance del numeral 8, ya que no se establecen diferencias especificas frente a la dedicación de tiempo del Oficial de Datos dentro de la organización. Si el objetivo es señalar que el oficial debe ser de tiempo completo frente datos personales sensibles o que entrañan riesgos, esto debe señalarse expresamente. La redacción actual presenta ambigüedades y no cumple su propósito.
Artículo 55. Cualificación del oficial de protección de datos.	Se sugiere que los mecanismos voluntarios de certificación que sean tenidos en cuenta para la cualificación de un oficial de datos personales se dejen a discreción de la autoridad de datos personales en el país. Lo anterior, dado que bajo la redacción actual cualquier persona con una certificación de cualquier naturaleza, podría ocupar el rol, lo que afecta el carácter especializado que esta materia ocupa. Si se exigirán estudios universitarios, se debe especificar exactamente el nivel de formación, si corresponde a educación no formal como un diplomado, o a una especialización o maestría como actualmente se oferta en el mercado.
Artículo 56. Posición del Oficial de protección de datos.	Resulta necesario ajustar la redacción del numeral 4, ya que plantea la posibilidad de que los titulares utilicen canales de comunicación diferentes a los contemplados la Política de Seguridad y Privacidad de la organización, lo que podría afectar el derecho a la intimidad del Oficial de Datos Personales. En este sentido, se debe aclarar que dicho contacto debe hacerse a través de los medios dispuestos para el ejercicio del derecho al *habeas data*

	únicamente. El numeral 6 debería presentar mayores restricciones, en tanto que en la práctica se evidencia que las organizaciones atienden al régimen de protección de datos personales como un elemento subsidiario a la gestión jurídica, por lo que el rol de Oficial de Datos Personales coincide con el Oficial de Cumplimiento (en lo concerniente a SAGRILAFT) y el Oficial de Transparencia. Se deja la observación para que el Legislador analice que es lo más conveniente para el cumplimiento normativo frente al ejercicio de un derecho fundamental.
Artículo 58. Códigos de conducta	Reconocer potestades de inspección, control y vigilancia alrededor del ejercicio de un derecho fundamental a particulares es inconstitucional, ya que esto obedece de la función de policía administrativa. Se debe dejar claridad que la competencia para la expedición de guías, lineamientos y directrices de obligatorio cumplimiento está en cabeza de la SIC, so pena de malinterpretaciones de la ley.
Artículo 59. Supervisión de códigos de conducta aprobados	La redacción del artículo permite interpretar una cesión del ejercicio de la función de policía administrativa a los particulares, lo cual no es acertado, ya que no es viable que quienes ejerzan el tratamiento de datos personales se vigilen a sí mismos. De ahí que la inspección, control y vigilancia sea una de las potestades exclusivas a la administración pública. En este contexto, se sugiere que las funciones de policía administrativa en materia de datos personales continúen exclusivamente en cabeza de la SIC como autoridad pública. Es diferente si la intención del Legislador es la de crear un régimen de auditorías con particulares habilitados para emitir certificaciones, pero ello debe distinguirse claramente de la actividad administrativa en sí misma.
Artículo 80. Tratamiento de la Cédula de Ciudadanía.	La redacción del artículo no distingue entre los datos públicos y los datos sensibles de la cédula de ciudadanía. Debe separarse de la redacción lo que corresponde al nombre y número de identificación, de las huellas, fecha de nacimiento y la fecha de expedición del documento. La exigencia del numeral 3 respecto a la anonimización del número de identificación de la titular contraria los presupuestos de acceso a la información pública descritos en la Ley 1712 de 2014. Por tanto, se sugiere incluir un parágrafo que señale que lo descrito en dicho numeral no aplica cuando se trate de personas naturales en el ejercicio de una función pública.
Artículo 81. Tratamientos con fines de videovigilancia.	La redacción actual, parece indicar que es una carga para el responsable o encargado la conservación de videograbaciones que prueben la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. Esto es desproporcional, porque dadas las dimensiones de la organización, es poco factible conocer el detalle de cada una de las grabaciones. En este sentido, la redacción debería orientarse a la colaboración con las autoridades judiciales, más no en la imposición de la carga.
Artículo 82. Sistemas de exclusión	El Registro de Números Excluidos (RNE) existente en virtud de la Resolución

publicitaria.	CRC 5050 de 2016, atiende exclusivamente a las competencias de la dinámica propia del sector de las telecomunicaciones en lo correspondiente a la prestación del servicio, para lo que se llevaron a cabo mesas de trabajo conjuntas con los diferentes agentes del sector. La inscripción de números de usuarios móviles en dicha base de datos tiene como fin evitar la recepción de mensajes cortos de texto (SMS) y/o mensajes multimedia (MMS), con fines publicitarios o comerciales, pero únicamente por estos dos canales. El artículo del proyecto de ley no distingue entre canales, por lo que es desproporcionado imponer a la CRC la carga de exclusión de tratamiento de datos personales frente al envío de comunicaciones comerciales, considerando que dicha entidad no tiene competencias para el tratamiento de datos personales. Si la intención del Legislador es crear una exclusión pata el tratamiento de datos personales, el responsable de ese manejo debe ser la autoridad de datos personales en el país.
Artículo 89. Inteligencia artificial.	Sugerimos respetuosamente la eliminación del artículo, por lo cual expondremos más ampliamente algunas consideraciones en el siguiente punto.
Artículo 90. Neuroderechos	Se reitera lo dicho en relación con artículo anterior frente a la importancia del principio de neutralidad tecnológica y de neutralidad de la red. El artículo se debe eliminar, ya que el estado de arte de las neurotecnologías es incipiente y aún no se tiene claridad sobre el impacto que este tendrá realmente en los diversos mercados. En todo caso, no hay distinción sobre el ejercicio del derecho al *habeas data* entre tecnologías, ya que este es el mismo en todos los medios y discriminar sobre su ejercicio no atiende a la técnica legislativa. En caso de presentarse un rápido desarrollo de neurotecnologías y que estas lleguen al país, el tratamiento de los datos personales será adsorbido por el régimen general de tratamiento de datos personales.
Artículo 92. Derecho a indemnización y responsabilidad	Si bien el artículo es una reproducción del apartado de derecho a indemnización y responsabilidad del RGPD del Parlamento Europeo, este no se ajusta adecuadamente a la realidad de nuestro propio ordenamiento jurídico. El camino que encontró el Legislador del año 2012 fue encaminar el incumplimiento al régimen de tratamiento de datos personales por conducto de multa o sanción, pero no se encontró conveniente asociarlo al régimen de responsabilidad civil dado que se trata de la afectación de un derecho fundamental. Bajo esta idea, el único mecanismo idóneo para cesar vulneración del derecho o la ocurrencia de un perjuicio irremediable es justamente atender al adecuado tratamiento de los datos personales o efectuar la supresión del dato. Por tal razón, se sugiere la supresión de este artículo. Ahora bien, si es intención del Legislador implementar un régimen de responsabilidad en materia de datos personales, este debe establecerse adecuadamente y atendiendo a las previsiones de la ley, de modo que es

	menester aclarar cuáles son los daños que dan lugar a la responsabilidad y cuáles son las situaciones fácticas dentro del tratamiento de datos personales que darían lugar a un nexo causal. No se puede pasar por alto que Colombia atiende a un sistema de responsabilidad retributiva, por lo que la causalidad siempre tiene que estar presente en la responsabilidad. Así mismo, es relevante considerar el rol del juez, quien sería el único competente para determinar que el perjuicio exista, sea cierto, la cuantía y que haya sido reparado.
Artículo 102. Condiciones del consentimiento.	Dado que la mayor parte de los consentimientos y autorizaciones para el tratamiento de datos personales se perfeccionaron a través de un contrato, se sugiere aplicar la ultractividad como efecto de la ley en el tiempo para este caso. Lo anterior, dado que supeditar las autorizaciones otorgadas con anterioridad a la expedición de la ley al término de un año, podría afectar el ciclo de vida del dato, alterar el objeto del tratamiento de los datos y desnaturalizar el procedimiento de supresión o revocación de la autorización ya previsto en el ordenamiento, previamente establecido en el acuerdo original, generando inseguridad jurídica

III. Consideraciones al artículo 89

En relación con el artículo 89, respecto a Inteligencia Artificial – IA - procedemos a realizar unas observaciones adicionales:

Artículo 89:

> "*Inteligencia artificial. Las empresas y organizaciones que utilicen Inteligencias Artificiales u otras tecnologías y/o sistemas informáticos con capacidad de aprendizaje, autonomía y toma de decisiones, y gran capacidad de procesamiento y análisis avanzados para el tratamiento de datos personales deben cumplir con los principios y disposiciones establecidos en la presente ley, y en particular:*
>
> *1. El procesamiento de datos personales debe priorizar la aplicación de mecanismos de anonimización o disociación.*
> *2. En caso de que sea necesario identificar al titular de los datos para el entrenamiento de la tecnología se debe observar la protección de datos desde el diseño y por defecto.*
> *3. Se deberá realizar evaluaciones de impacto para identificar y mitigar los riesgos asociados al uso de estas tecnologías en el procesamiento de datos personales.*
>
> *La Superintendencia de Industria y Comercio será responsable de mantener una lista actualizada de las Inteligencias Artificiales o tecnologías similares prohibidas. Las empresas y organizaciones que no cumplan con estas disposiciones estarán sujetas a las sanciones establecidas en la presente ley."*

Al respecto, consideramos necesario precisar que no es conveniente regular temas asociados a la Inteligencia Artificial (IA) por el momento y se recomienda que el debate se pueda realizar evaluando cada sector, tipo de modelos y tipo de aplicaciones de IA de manera independiente. Es crucial considerar el desarrollo de la tecnología para luego efectuar las consideraciones regulatorias en torno a la mitigación de riesgos, en tanto que reglamentar con limitaciones o restricciones de forma apresurada tiene el potencial de afectar la innovación y el crecimiento de la economía digital en el país.

Ahora bien, en el texto de la propuesta se resaltan los siguientes elementos:

a) Asimilar Inteligencia Artificial a la tecnología y/o sistema informático con capacidad de aprendizaje, autonomía y toma de decisiones, y gran capacidad de procesamiento y análisis avanzados.
b) La obligación de la Superintendencia de Industria y Comercio de realizar un registro de Inteligencias Artificiales o tecnologías similares prohibidas.

Sobre esos aspectos debe recordarse que para que la regulación de una nueva tecnología sea efectiva se requiere precisión y rigor en los términos que se utilizan para que su aplicación sea predecible, dinámica a los avances técnicos y efectiva en obtener los objetivos que el legislador pretende alcanzar.

Las definiciones empleadas por el ordenamiento jurídico deben tener en cuenta los siguientes criterios[2]:

1. Alcance. Las definiciones legales no deben ser ni excesivas ni insuficientemente inclusivas. La inclusión excesiva o insuficiente se refiere al objetivo regulatorio. Una definición es demasiado inclusiva cuando incluye casos que no necesitan regulación de acuerdo con el objetivo regulatorio. Es insuficientemente inclusivo cuando no se incluyen casos que deberían haberse incorporado en su alcance.

2. Precisión. Las definiciones legales deben ser precisas. Debe ser posible determinar claramente si un caso particular entra o no dentro de la definición. Idealmente, todos los elementos de la definición son dicotómicos, es decir, las condiciones son cumplidas o no. No debería haber un rango de cuánto se cumple una condición.

3. Integralidad. Las definiciones legales deben ser exhaustivas. Los regulados deben poder comprender si la regulación es aplicable o no para poder ajustar su comportamiento en consecuencia. Por lo tanto, la definición debe basarse en el significado existente de los términos y respetar el uso natural del lenguaje. En principio, las personas sin conocimientos expertos deberían poder aplicar la definición.

4. Practicidad. Las definiciones legales deberían ser prácticas. Los regulados, las autoridades judiciales y administrativas deben poder determinar con poco esfuerzo si un caso concreto es cubierto o no por la definición. La evaluación de todos los elementos debería ser posible sobre la base de la información que normalmente tienen a su disposición.

5. Permanencia. Las definiciones legales deben ser permanentes. Las autoridades no deberían utilizar elementos que probablemente cambien en un futuro próximo. Se debería evitar la necesidad de actualizar la legislación constantemente.

La definición de Inteligencia Artificial contemplada en la propuesta, la define como todo sistema o herramienta que cuente con la capacidad de aprendizaje, autonomía y toma de decisiones, y gran capacidad de procesamiento y análisis avanzados, implica que al operador jurídico que le corresponda aplicarla deba comparar el resultado generado por la tecnología o sistema y determinar si lo percibe equivalente a la inteligencia humana (aprendizaje, autonomía y toma de decisiones) y, con esa evaluación, calificarlo como inteligencia artificial. En ese sentido, la literatura especializada explica que los sistemas de Inteligencia Artificial no son máquinas pensantes inteligentes en ningún sentido significativo, esas tecnologías pueden producir resultados útiles e "inteligentes" sin inteligencia, a través de métodos heurísticos: detectan patrones en los datos y utilizan conocimientos, reglas e información que han sido codificados específicamente por personas en formas que pueden ser procesadas por computadoras[3].

[2] Ver: Black J (1997). Rules and Regulators. Oxford University Press.

[3] Surden, H. (2019). Artificial intelligence and law: An overview. *Georgia State University Law Review*, *35*, 19-22.

En otras palabras, la propuesta etiqueta como Inteligencia Artificial con cuán inteligente se percibe los resultados (capacidad de aprendizaje, autonomía y toma de decisiones) de un proceso computacional, en la práctica cuando un operador jurídico aplique esta propuesta deberá realizar la siguiente operación lógica: "la Inteligencia Artificial es lo que llamamos Inteligencia Artificial", una definición circular y subjetiva, lo que la torna problemática como base para la toma de decisiones legales. En ese sentido, en ausencia de una definición de Inteligencia Artificial que cumpla con los requisitos de efectividad de las definiciones legales expuestos anteriormente, sugerimos de manera respetuosa que se procure definir ciertos diseños, casos de uso y/o capacidades siguiendo un enfoque basado en riesgos para determinar cuáles serían las aplicaciones tecnológicas sujetas a regulación[4].

Adicionalmente, la propuesta expresa que una autoridad administrativa, la Superintendencia de Industria y Comercio, estaría facultada para realizar un registro de las Inteligencias Artificiales o tecnologías similares prohibidas, sin que se establezca cuáles son las razones o criterios ni la autoridad encargada de definir que algoritmo[5], o mecanismo computacional no puede ser aplicado en Colombia.

Por último, y como lo expresa la doctrina especializada una nueva tecnología puede parecer que crea nuevos desafíos, sin embargo, esos problemas constituyen simplemente una versión de un problema que las leyes ya abordan de manera efectiva[6]. En ese sentido, las normas de protección de datos personales, tanto las vigentes, como aquellas que se pretenden promulgar con la propuesta estudiada, resultan aplicables a las bases de datos que sirven de insumo a los modelos de aprendizaje de la máquina y otras herramientas computacionales.

IV. Sobre el debate global de la regulación

En este complejo marco técnico de la adopción de la Inteligencia Artificial frente a sus potenciales riesgos, actualmente existe un debate mundial en el cual se presentan diversos enfoques sobre la regulación de la IA, desde una legislación exigente (*hard law*) en materia de cumplimiento en distintas etapas del desarrollo de esta tecnología (enfoque europeo a través del Acto de IA que cursa actualmente en el Parlamento Europeo) hasta modelos de auto regulación o regulaciones experimentales (*sandboxes* regulatorios) que buscan evitar los efectos de rezago en los desarrollos tecnológicos y potenciales desincentivos a la innovación que puede traer consigo una regulación sobre una tecnología que evoluciona de manera muy acelerada. En los Estados Unidos de América (EEUU), el enfoque reciente del gobierno fue de auto regulación, suscribiendo con las grandes empresas desarrolladoras de IA compromisos voluntarios en materia de seguridad en sus desarrollos de IA (julio de 2023).

Posteriormente, en octubre de 2023, El Presidente de EEUU emitió una orden ejecutiva sobre el desarrollo y uso seguro y confiable de la inteligencia artificial desde un enfoque basado en la seguridad[7].
Se recomienda que los reguladores de cada sector evalúen la necesidad de regulaciones específicas, en línea con prácticas internacionales, a partir del análisis de las necesidades de cada sector y de la utilización de herramientas de gestión de riesgos, la realización de *sandboxes* regulatorios y del análisis de las distintas estandarizaciones y autorregulaciones del mercado.

Esto decantaría en que en un mismo sector como por ejemplo el del transporte, se considera que no es lo mismo la regulación de la IA aplicada al transporte masivo, la IA aplicada al transporte tipo Uber, o la IA que se aplicaría en el

[4] Schuett, Jonas (2021), Defining the Scope of AI Regulations. *Law, Innovation and Technology, Legal Priorities Project Working Paper Series No. 9*, Disponible en: https://ssrn.com/abstract=3453632 or http://dx.doi.org/10.2139/ssrn.3453632

[5] Una especificación inequívoca de cómo resolver una clase de problemas. Estos problemas pueden incluir ordenar posibles opciones (priorización), categorizar elementos (clasificación), encontrar vínculos entre elementos (asociación) y eliminar información irrelevante (filtrado), o una combinación de estos. Los algoritmos de aprendizaje automático (ML) más sofisticados están diseñados para aprender, es decir, modificar su programación para tener en cuenta nuevos datos.

[6] Buiten, M. C. (2019). Towards intelligent regulation of artificial intelligence. *European Journal of Risk Regulation*, *10*(1), 41-59. Página 48.

[7] https://ai.gov/es/acciones/ [Orden ejecutiva sobre inteligencia artificial]

transporte aéreo, encontrando en cada uno de estos subsectores con parámetros de datos, información, desarrollos técnicos y riesgos de seguridad muy disímiles entre sí, los cuales ameritarían regulaciones específicas para cada caso.

Si bien ya existen amplios consensos internacionales sobre la necesidad de mitigar los riesgos, prevenir los potenciales incidentes, y en general, concebir un enfoque de seguridad en la implementación de una IA confiable, como lo ejemplifica la reciente Declaración de Bletchley emanada en noviembre de 2023 de la Cumbre de Seguridad del Reino Unido, o un enfoque de uso ético bajo instrumentos a los que se ha adherido el país como la recomendación de la OCDE sobre la Inteligencia Artificial o los principios éticos de la UNESCO, desde el gobierno colombiano se considera que la regulación mundial se encuentra en una etapa prematura en la que no se tiene evidencia aún sobre las mejores prácticas regulatorias en relación con sus impactos sobre el desarrollo de la IA.

Sumado a lo anterior, vale la pena resaltar que desde el segundo semestre de 2023 se concibió el Laboratorio de Inteligencia Artificial del MinTIC que buscará impulsar la adopción masiva de esta tecnología en el país, para lo cual incluirá en sus pilares de trabajo el análisis de las necesidades regulatorias y marcos de implementación bajo un enfoque de implementación de una Inteligencia Artificial con propósito social y multisectorial, que fortalezca la productividad en las pequeñas y medianas empresas impactando positivamente la economía popular y la reindustrialización y brindando soluciones a los problemas sociales de Colombia generando mayor bienestar para los ciudadanos.

Así las cosas, se encuentra inconveniente que mediante una ley general se definan reglas de cómo una tecnología se desarrolla, en especial, teniendo en cuenta el principio de neutralidad tecnológica consagrado en el numeral 6 del artículo 2 de la Ley 1341 del 2009, el cual atribuye al Estado el deber de garantizar, de un lado, la libre adopción de tecnologías, y del otro, la libre y leal competencia. Dice el precepto en comento:

> *"(...) ARTÍCULO 2o. PRINCIPIOS ORIENTADORES. (...) 6. Neutralidad Tecnológica. El Estado garantizará la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones y garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible"*

La aplicación del principio de neutralidad tecnológica ha llevado a que Colombia se mantenga actualizado frente a los estándares internacionales en materia de desarrollo y adopción de tecnologías. Así mismo, ha permitido la garantía de los derechos a la libertad de empresa y a un ambiente competitivo sano, entre otros.

Por lo anterior, desde el MinTIC se sugiere avanzar en el desarrollo de la política y la estrategia de Laboratorio de IA, bajo principios de estándares éticos actuales, mientras que, en paralelo, se puedan estudiar rigurosamente las mejores experiencias de impacto regulatorio a nivel internacional en la medida que estos modelos se empiezan a implementar en el mundo, e incluso se introducen esquemas de *sandbox* regulatorio, en aras de definir, establecer y adoptar, en el mediano plazo, los marcos de ley necesarios que se ajusten a las particularidades del desarrollo de la IA en el país, garantizando un balance entre el uso ético, la seguridad, la innovación y el amplio despliegue que permita democratizar esta tecnología en Colombia.
Adicionalmente, el MinTIC también sugiere expandir las metodologías y *frameworks* tradicionales de innovación, creación de productos y desarrollo de soluciones tecnológicas que involucren el uso de modelos y herramientas de IA, para que incluyan un componente transversal enfocado en mecanismos de intervención estratégica y política. Esta expansión, en consonancia con las directrices de *"Principled Artificial Intelligence"* del Berkman Klein Center de Harvard, implica adaptar principios éticos y basados en los derechos humanos en el desarrollo de la IA en Colombia. Al integrar consideraciones sociales y éticas en todas las etapas de desarrollo y aplicación de estas metodologías y *frameworks*, se sugiere fomentar estándares que equilibren innovación con un uso ético y socialmente responsable de la IA para la sociedad colombiana.

V. La inconveniencia de regular la IA antes de su consolidación y adopción

La IA es una tecnología de propósito general, como los computadores, o las comunicaciones. Sus impactos sobre la productividad y el empleo sólo empezarán a observarse en dos o tres años. Los diferentes modelos y generaciones de IA (Language Action Models (LAM) *modelos de lenguaje de acción* y los Large Language Models (LLM) *modelos de lenguaje de gran tamaño.*), aprendizaje de máquina y aprendizaje profundo, entre otros, están apenas en gestación y algunas de ellas desaparecerán para dar lugar a versiones más potentes y fáciles de usar. El intento de regular la IA sin que se hayan estabilizado los ecosistemas de creación, su estructura de industria, y no existan problemas visibles o previsibles que exijan atención de la política pública es altamente **inconveniente** porque puede crear costos de transacción en la adopción y con ello reducir su necesario impacto en el aumento del crecimiento de la productividad del Producto Interno Bruto – PIB -, y en la creación de más y mejores empleos (paradójicamente en contravía del propósito de defender el derecho al trabajo). Esto hubiera sido equivalente hace 30 años, a intentar frenar el despliegue de la telefonía celular para asegurar el empleo de los trabajadores de la telefonía fija.

Así las cosas, este Ministerio queda a su disposición para atender cualquier información adicional en relación con el particular y manifiesta su voluntad de colaborar con la actividad legislativa, dentro de los parámetros constitucionales y legales vigentes.

Cordialmente,

[Firmado Digitalmente]
MAURICIO LIZCANO ARANGO
Ministro de Tecnologías de la Información y las Comunicaciones

Proyectó: Margarita María Fandiño López - GIT de Seguridad y Privacidad de la Información
Jhon Caballero Martinez - GIT de Seguridad y Privacidad de la Información
Juan Carlos Garay - Asesor Viceministerio de Conectividad
Julián Moncada Español - Equipo Legislativo

Revisó: Sindey Carolina Bernal – Viceministra de Transformación Digital
Angela Janeth Cortes Hernández - Coordinadora del GIT de Seguridad y Privacidad de la Información
Juan Garay - Asesor Viceministerio de Transformación Digital
Luisa Fernanda Medina– Directora de Gobierno Digital (E)
Marco Emilio Sánchez – Gobierno Digital
Lucas Quevedo - Director Jurídico
Luis Leonardo Monguí - Coordinador GIT Doctrina y Seguridad Jurídica
Julián Moncada Español - Equipo Legislativo

REGISTRO DE FIRMAS ELECTRONICAS

242021202_21401

Ministerio de Tecnología de la Información y las Comunicaciones
gestionado por: azsign.com.co

Id Acuerdo: 20240307-113616-634c82-43593201 Creación: 2024-03-07 11:36:16

Estado: Finalizado Finalización: 2024-03-07 11:38:26

Escanee el código para verificación

Firma: Firmante

Mauricio Lizcano Arango
C.C 79.960.663
mlizcano@mintic.gov.co

REPORTE DE TRAZABILIDAD

242021202_21401

Ministerio de Tecnología de la Información y las Comunicaciones
gestionado por: azsign.com.co

Id Acuerdo: 20240307-113616-634c82-43593201 Creación: 2024-03-07 11:36:16

Estado: Finalizado Finalización: 2024-03-07 11:38:26

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Firma	Mauricio Lizcano Arango mlizcano@mintic.gov.co	Aprobado	Env.: 2024-03-07 11:36:17 Lec.: 2024-03-07 11:36:57 Res.: 2024-03-07 11:38:26 IP Res.: 190.71.137.3

Bogotá, 05 de marzo de 2024.

Honorable Representante
Duvalier Sanchez Arango
Cámara de Representantes
CONGRESO DE LA REPÚBLICA
Ciudad

Asunto: Comentarios al Proyecto de Ley 156 Cámara *"Por la cual se dictan disposiciones para el Régimen General de Protección de Datos Personales"*

Cordial saludo Honorable Representante,

Escuela de Privacidad organización privada que trabaja en pro de la protección de datos, la privacidad y seguridad digital, y qué también genera espacios de discusión y reflexión en torno a estos temas, hemos propuesto algunas observaciones al proyecto de ley referenciado en el asunto, en conjunto con otros profesionales de otros sectores, y que por medio de la presente comunicación, remitimos los comentarios.

Artículo del Proyecto	Comentario	Propuesta
Artículo 5. Definiciones 2. «Autoridad de control»	Se recomienda adecuar el proyecto de ley a términos y conceptos propios del marco jurídico colombiano, y/o cultural colombiano. Algunos conceptos que introduce la ley son propios de la legislación española, que si bien en muchos casos, puede tener el mismo significado en el contexto colombiano, son términos que pueden parecer extraños. Por otro lado, la transición de una ley a otra puede ser menos caótica, y brindar seguridad jurídica, si se conservan y se respetan	Artículo 5. Definiciones 2. «Autoridad de control»: Cambiar por Autoridad de Protección de Datos.

Artículo del Proyecto	Comentario	Propuesta
	los mismos criterios conceptuales bajo se ha venido forjando una cultura de respeto hacia los datos personales.	
Artículo 5 3. «Base de datos de riesgo crediticio»: 17. «fuentes»: 23. «Operadores» 36. «Usuarios»	Se recomienda eliminar del alcance del proyecto de ley, los aspectos que ya se encarga la ley 1266 de 2008, relativo al habeas data financiero. Sería generar conflicto en interpretaciones, y regular aspectos que ya se encuentra definido en otras normativas. Se recomiendo excluir o eliminar, los siguientes	Eliminar conceptos: Artículo 5 3. «Base de datos de riesgo crediticio»: 17. «fuentes»: 23. «Operadores» 36. «Usuarios»
18. «Grupo empresarial: 28. «Servicio de la sociedad de la información» «Principio de Neutralidad Tecnológica»	Se describen conceptos que ya se encuentran definidos o regulados por otras legislaciones, o existe regulación específica para ello, por lo que abriría la ventana a conflictos de interpretación. Supongo que lo definen por las BCR, no obstante, considerar que ya la ley 222 de 1995. Por técnica legislativa, no es tan apropiado generar definiciones que las leyes especiales ya traen. Por otro lado, la Ley 1341 de 2009, ya aborda esta temática, tanto en su artículo 3, como en el artículo 2, numeral 6.	Eliminar los conceptos: 18. «Grupo empresarial: 28. «Servicio de la sociedad de la información» «Principio de Neutralidad Tecnológica»

Artículo del Proyecto	Comentario	Propuesta
Artículo 100. Prescripción de la Sanción	Establecen condiciones que son propias del derecho administrativo, por lo que no se debería entrar a establecer reglas puntuales, sino reglas que ya están inmersas en el sistema jurídico colombiano.	Eliminar articulo
Artículo 101. Caducidad de la facultad sancionatoria de la Autoridad de Control.	Establecen condiciones que son propias del derecho administrativo, por lo que no se debería entrar a establecer reglas puntuales, sino reglas que ya están inmersas en el sistema jurídico colombiano.	Eliminar articulo
Artículo 7. Bases legales del tratamiento d) El tratamiento es necesario para proteger intereses vitales del titular o de otra persona natural;	Se sugiere que se cambie las expresiones por aquellos términos que actualmente se usan en el contexto colombiano. Los términos no deben ser los mismos que utiliza el estándar europeo, lo importante es que sean equivalentes a lo que se pretende legislar.	Cambiarse por: e) El tratamiento es necesario para el cumplimiento de una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.

Artículo del Proyecto	Comentario	Propuesta
Artículo 79. Tratamiento y acceso a documentos públicos. 1. Los datos personales de documentos públicos en posesión de algún ente de naturaleza pública o un particular que se encuentre en ejercicio de una misión para el interés público, podrán ser comunicados por ésta, de conformidad con la legislación nacional, a fin de conciliar el derecho de las personas a acceder a documentos públicos y el derecho a la protección de los datos personales en virtud de la presente ley.	Se sugiere eliminar este artículo, es lo mismo que establece la ley 1712 de 2014 y el Decreto 103 del 2015. Las disposiciones relativas a la transparencia y acceso a la información pública establecen lineamientos específicos para dicho fin. Sería entrar a establecer lineamientos para el derecho de acceso a la información pública en una ley de protección de datos.	Eliminar artículo.
Artículo 80. Tratamiento de la Cédula de Ciudadanía. 1. El responsable y encargado del tratamiento implantarán las medidas técnicas y organizativas en atención al riesgo para evitar la circulación no autorizada de reproducciones digitales, copias o fotocopias de la cédula de ciudadanía como documento que contiene datos de carácter personal, teniendo en cuenta, entre otros, los siguientes criterios:	Esto puede ser parte de una reglamentación, pero no de una ley estatutaria. Por otro lado, debería ser extensible para otros documentos de identidad, no solo la cédula de ciudadanía.	eliminar el artículo.
Artículo 84 Tratamiento en ámbito laboral En el ámbito de las relaciones laborales, el empleador debe cumplir además de las obligaciones contenidas en esta ley, las siguientes:	Es un articulo que sobra, las organizaciones sin necesidad de este articulado ha incoporado la normativa de protección de datos al cumplmiento de las relaciones laborales	eliminar el artículo.

Artículo del Proyecto	Comentario	Propuesta
Artículo 5. Definiciones 25. «Queja.	Replantear la definición ya que está limitada solo a la autoridad y no contempla el responsable y/o encargado. Puede confundirse con las solicitudes a cada entididad y no solo al ente de control.	«Queja»: reclamación de interés particular que busca el amparo del derecho fundamental a la protección de los datos personales.
Artículo 53. Designación del Oficial de protección de datos. Numeral "e"	Ampliar esta obligación a las entidades de Seguridad Social y Parafiscal, sin limitar a solo aquellas que manejan Historias Clínicas, ejemplo de ello son las Cajas de Compensación que manejan información sensible de los trabajadores y sus familias	e) Las instituciones que integran el Sistema General de Seguridad Social y Parafiscal. Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.
Artículo 54. Calidades del Oficial de protección de datos. 4. El Oficial de protección de datos será designado según su profesión y, en particular, por sus conocimientos especializados en Derecho y la práctica en materia de protección de datos, así como a su capacidad para desempeñar las funciones indicadas en el artículo 57.	Eliminar el numeral 4. el cual establece el requisito de la profesión y el cual limita a que sea un profesional en Derecho, teniendo en cuenta que existen profesionales que se han fortalecido en el manejo de datos personales. No considero que debe ser obligatoria la formación universitaria en derecho para el oficial, pero si tener experiencia y conocimeintos en el tema	

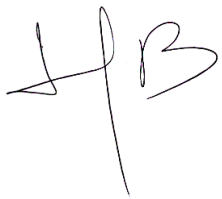
Artículo del Proyecto	Comentario	Propuesta
Artículo 55. Cualificación del oficial de protección de datos.	Se sugiere liminar el artículo 55 debido a que la cualificación del Oficial en cuanto a que su obligación sea que debe tener conocimientos especializados en Derecho. No considero que debe ser obligatoria la formación universitaria en derecho para el oficial, pero si tener experiencia y conocimeintos en el tema	Eliminar el artículo 55.
Artículo 86. Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales.	Se debe regir por las reglas generales que ya dispone la ley, más bien haciendo referencia a datos personales en general.	Eliminar artículo.
Artículo 102. Condiciones del consentimiento. El consentimiento de los titulares recabados con anterioridad a la expedición de esta ley será válido durante un año posterior a la entrada en vigencia, plazo en el cual el responsable del tratamiento deberá obtenerlos en las condiciones previstas en la presente ley o legitimar el tratamiento en otra base jurídica de conformidad con el artículo 7.	Las autorizaciones deben seguir vigentes, lo que debe suceder es que deben ser actualizadas, pero dejar sin validez la autorización después de todo el esfuerzo de las organizaciones en recabarlas es un retroceso. Por lo anterior, se sugiere una redacción al artículo.	Artículo 102. Condiciones del consentimiento. El consentimiento de los titulares recabados con anterioridad a la expedición de esta ley seguirán siendo válido. No obstante, los responsables tendrán un año posterior a la entrada en vigencia de la presente ley para actualizarlos en los términos de la misma.

Artículo del Proyecto	Comentario	Propuesta
2. «Principio de responsabilidad demostrada» «accountability»:	Esta definición puede mejorar de manera sustancial, y articularse con la definición que la SIC ha desarrollado a través de su doctrina.	El responsable del tratamiento de datos debe aplicar medidas técnicas y organizativas adecuadas, no solo para cumplir con la normativa, sino para demostrar su cumplimiento ante la autoridad de protección de datos y titulares.
Artículo 32. Derecho a la portabilidad de los datos.	Uno de los inconvenientes en el ejercicio de este derecho, es la falta de consenso en los tipos de formatos y en general, en los estándares que se deben considerar para que la portabilidad pueda darse. En dicho sentido, se propone una mejora con el propósito de dinamizar este derecho.	La Superintendencia de Industria y Comercio junto con el Ministerio TIC podrán definir lineamientos para los formatos estructurados de uso común y lectura mecánica.
Artículo 81. Tratamientos con fines de videovigilancia. 1. Las personas naturales o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de videovigilancia con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.	Considero que establecer estas reglas para las actividades de videovigilancia las cuales pueden ser por múltiples razones podría limitar dicha actividad. También considerando que hay sectores como el financiero que tiene disposiciones especiales en la conservación de esta información o de policía para fines judiciales e investigativos.	Eliminar artículo.
Artículo 105. Contratos de encargados del tratamiento. Los contratos de encargado del tratamiento suscritos con anterioridad a esta ley serán válidos hasta dieciocho meses	Este articulo puede generar inseguridad jurídica entre las partes. El artículo debería quedar redactado como una actualización, pero no	**Artículo 105. Contratos de encargados del tratamiento.** Los contratos de encargado del tratamiento suscritos con anterioridad a esta ley

Artículo del Proyecto	Comentario	Propuesta
después de su entrada en vigencia. Durante dicho plazo cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 41 de la presente ley. **Parágrafo:** los contratos firmados con posterioridad a la fecha de entrada en vigencia de la presente ley deberán cumplir con los requisitos establecidos en el artículo 41.	perder vigencia los acuerdos actuales. En la medida en que pueden encontrarse compromisos adquiridos, condiciones establecidas que pueden afectar a las partes, incluso a los titulares, en la forma como se negoció dicho encargo.	continuaran siendo válidos. No obstante, las partes tendrán hasta dieciocho meses después de su entrada en vigencia, para su actualización conforme a los términos establecidos en la ley. Durante dicho plazo cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 41 de la presente ley. **Parágrafo:** los contratos firmados con posterioridad a la fecha de entrada en vigencia de la presente ley deberán cumplir con los requisitos establecidos en el artículo 41.
Artículo 69. Autoridad Nacional de Protección de Datos. 1. La Superintendencia de Industria y Comercio ejercerá la función de autoridad nacional de control en materia de protección de datos personales, garantizando el efectivo cumplimiento de los principios, derechos, garantías y los procedimientos establecidos en la presente ley en aras de facilitar la libre circulación de datos.	No se hace referencia a las medidas sancionatorias ni medidas de vigilancia para las entidades públicas. Este aspecto es crucial, debido a que el Estado administra muchos tipos de bases de datos de ciudadanos y no hay actualmente un ejercicio activo de vigilancia y protección de estos datos. Se debería incluir un apartado para que una entidad del Estado se encargue de la investigación.	Adicionar un nuevo párrafo: La Procuraduría General de la Nación hará las veces de Autoridad de Protección de Datos para el sector público. Ella misma definirá su reglamentación.
Artículo 53. Designación del Oficial de protección de datos. 1. El responsable y el encargado	Se sugiere no excluir a la rama judicial, de esta obligación. La rama	La redacción quedaría así: a) El tratamiento lo lleve a cabo una autoridad u

Artículo del Proyecto	Comentario	Propuesta
del tratamiento designarán un Oficial 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;	judicial maneja información altamente sensible, relativo a antecedentes penales y judiciales. También gestionan archivos con información privada de las partes del proceso. Excluir a la rama judicial, sería una desprotección de los datos personales para los ciudadanos.	organismos público, incluyendo los tribunales que actúen en ejercicio de su función judicial;

Cordialmente,



Heidy Elieth Balanta. CC 29.352.653
Representante Legal- Escuela de Privacidad

Víctor Alfonso Buitrago Ramírez CC 1.010.066.495
Administrador de Empresas – Sector

Vanessa Osorio Villegas CC 1039451243
Abogada-

Bogotá D.C., 7 de marzo de 2024.

Honorables Representantes
Mesa Directiva
Comisión Primera de la Honorable Cámara de Representantes
Congreso de la República de Colombia
La ciudad

Respetados señores:

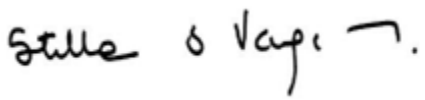
Por medio de la presente me permito agradecer la invitación extendida el pasado 28 de febrero de 2024, con el fin de participar en la Audiencia Pública del Proyecto de Ley Estatutaria N° 156 de la Cámara, "Por la cual se dictan disposiciones para el Régimen General de Protección de Datos Personales".

Es una oportunidad muy valiosa poder presentar mis comentarios y poner de presente lo que considero son los puntos más urgentes para nuestra legislación en materia de protección de datos personales, algunos de los cuales han sido compartidos y analizados en el seno de ADAPRI.

En consecuencia, por medio del presente les comparto mis observaciones esperando que estas resulten de utilidad con el fin de lograr una propuesta que proteja el derecho de habeas data, teniendo en cuenta la sociedad actual, los retos que existen para los Responsables y Encargados del Tratamiento y la necesidad de generar consciencia en los Titulares acerca del cuidado propio de la información personal para contribuir a un ecosistema sano, dinámico y seguro.

Estoy muy atenta a cualquier inquietud, así como en caso de que requieran una ampliación o discusión sobre los comentarios que les comparto a través de este escrito.

Un cordial saludo,



STELLA VANEGAS MORALES

A continuación, se presentará una breve síntesis de los temas y aspectos relevantes a abordar en la nueva Ley de Régimen General de Protección de Datos Personales, que hemos elaborado desde ADAPRI. La intervención se dividirá en dos apartados: primero, se hará referencia a las dificultades que presenta nuestra normativa actual en datos personales y, posteriormente, se realizará una recopilación de los comentarios más relevantes sobre el proyecto de ley.

I. DIFICULTADES QUE PRESENTA NUESTRA NORMATIVA ACTUAL EN DATOS PERSONALES:

Para llevar a cabo este análisis, resulta indispensable cuestionarse siempre: ¿Qué aspectos hacen falta en la normativa actual?, ¿Por qué sería importante actualizarla?, ¿Genera una desventaja el mantenernos cómo estamos? Hemos basado nuestro análisis en la experiencia local y en la revisión de referentes globales y regionales que orientan mucho la identificación de los puntos críticos a ser revisados, entre ellas GDPR, Ecuador, Panamá y Brasil. Con base en estas consideraciones, se elaboraron los siguientes comentarios:

1. Bases legitimadoras del consentimiento

Actualmente, en Colombia solo se pueden tratar datos personales si se cuenta con la autorización previa, expresa e informada del titular. No obstante, esta base legitimadora para el tratamiento resulta limitada en comparación con las bases que operan en otros ordenamientos. Por ejemplo, al analizar casos como Brasil, Panamá, Ecuador y el Reglamento General de Protección de Datos (GDPR), observamos que en estos marcos normativos existen diversas bases adicionales para legitimar el tratamiento de datos personales. Estas incluyen, por ejemplo, la ejecución de un contrato, la aplicación de medidas precontractuales o el cumplimiento de una obligación legal.

Es importante tener en cuenta que el consentimiento puede resultar engañoso, ya que muchas personas lo firman sin leer detenidamente el contenido del documento. El consentimiento no debería ser la única base legitimadora ni debería ocupar el primer lugar en la jerarquía. Basarse solamente en el consentimiento obliga a llevar todas las acciones que se buscan adelantar con los datos a un formato de finalidades que suele ser largo que en la mayoría de los casos es firmado o aceptado por las personas sin haber sido leído ni entendido.

Hay situaciones claras en las que el Tratamiento no se debe producir basado en el consentimiento, por ej. Si se celebra un contrato de arrendamiento es indispensable que las partes conozcan aquellos datos personales que les permitan llevar adelante la relación contractual, luego en este caso, es el contrato el que legitima el que haya lugar a ese tratamiento. Es importante resaltar que no se protege de mejor manera al Titular de los datos por llevar todo a un consentimiento, cuando de manera razonable hay otras causas como la atrás mencionada o la más obvia, el cumplimiento de un deber legal por parte del Responsable. En estos casos, lo relevante no es obtener un consentimiento independiente separado de la realidad contractual o legal en la que se está inmerso, sino que debe primar la aplicación de los principios de finalidad y transparencia, el revelar de manera adecuada que

datos se recolectarán para cumplir con las obligaciones contractuales o legales que existen. Por lo tanto, sería beneficioso explorar otras bases legitimadoras para el tratamiento de datos personales que simplifiquen las operaciones tanto para los titulares como para los responsables y encargados del tratamiento. A continuación, encontrará un cuadro comparativo sobre este aspecto.

Colombia	GDPR	Ecuador	Panamá	Brasil
Autorización (consentimiento) **(Ley 1581 de 2012, Art. 9)**	Consentimiento Ejecución de un contrato o la aplicación de medidas precontractuales Para el cumplimiento de una obligación legal Para proteger los intereses vitales del titular o de otra persona Cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento Satisfacción de intereses legítimos **(GDPR, Art. 6)**	Consentimiento Obligación legal Orden judicial Cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable Ejecución de medidas precontractuales a petición del titular o para el cumplimiento de obligaciones contractuales Para proteger intereses vitales del interesado o de otra persona natural Satisfacer un interés legítimo del responsable de tratamiento o de tercero. **(Ley orgánica de protección de datos personales, Art. 7)**	Consentimiento Ejecución de una obligación contractual Obligación legal Autorizado por ley **(Ley 81 de 2019, Art. 6)**	Consentimiento Obligación legal o reglamentaria Ejecución de políticas públicas Ejecución de un contrato Proteger la vida o seguridad física del titular o de un tercero Protección de la salud Satisfacer intereses legítimos **(Ley 13.709 de 2018, Art. 7)**

2. Menores de edad

Ahora bien, en relación con los menores de edad, actualmente su tratamiento se encuentra muy limitado. No obstante, con los avances tecnológicos, los menores se están convirtiendo cada vez más en sujetos activos en este mercado y están expuestos al tratamiento de sus datos personales. Por lo tanto, debería considerarse otorgarles autonomía frente a sus datos personales en algunos aspectos y estableciendo una edad específica para ello.

Es necesario adaptar la norma a la realidad que vive la sociedad actualmente. En una sociedad digital los menores desde temprana edad están expuestos al uso de tecnología. Si bien hay que cuidar al menor de edad debe tenerse presente que el criterio que tiene hoy un menor de 16 a 18 años ha evolucionado y que existen productos y servicios que consultan su interés superior y podrían ser manejados de manera directa por éstos sin tener que requerirse que sea su padre o representante legal el que manifieste ese interés. La misma Autoridad de protección de Datos lo ha reconocido para fines educativos, cuando un menor está buscando opciones para adelantar estudios y debe relacionarse con universidades y establecimientos educativos de educación superior. Igualmente, podría pensarse del menor que debe hacer uso de servicios médicos en los que los temas a tratar sean de prevención o de atención que dada la edad representen un grado de intimidad que ese menor de 16 años quiera conservar de

manera reservada. Y sin ir más allá, el acceso a billeteras digitales o redes sociales. Hay que educar al menor adulto para que haga un uso adecuado de sus datos personales, sin que haya necesidad de generar más cargas operativas que a la postre solamente produzcan una protección formal pero no de fondo de los datos de ese menor.

Colombia	**GDPR**
Se prohíbe salvo que se trate de datos públicos y cuando dicho Tratamiento cumpla con los siguientes parámetros y requisitos: 1. Que responda y respete el interés superior de los niños, niñas y adolescentes. 2. Que se asegure el respeto de sus derechos fundamentales. El representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor de su derecho a ser escuchado. **(Decreto 1074 de 2015, artículo 2.2.2.25.2.9.)**	El tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño. **(GDPR, Art. 8)**

3. Transferencia a terceros países.

Por otro lado, en Colombia sería recomendable considerar la posibilidad de incorporar salvaguardias en las transferencias a terceros países, permitiendo operaciones sin requerir una autorización específica de una autoridad de control. Lo anterior, con el objetivo de facilitar esas operaciones para los actores involucrados. Colombia requiere aportar mayor claridad respecto de las transferencias y las transmisiones internacionales. Somos tal vez el único país que diferencia la circulación de los datos hacia un tercero bajo las dos modalidades de transferencia y transmisión, lo cual suele generar trabas pues esta diferenciación no resulta clara para las terceras partes establecidas en el exterior. Por ello, se recomienda revisar el concepto de transferencia como ha sido concebido en otras legislaciones, es decir como un término único para referirse a los intercambios de información de Responsable a Responsable y de Responsable a Encargado.

Colombia	**GDPR**
Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios. Esta prohibición no regirá cuando se trate de: a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia; b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública; c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable; d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad; e) Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la	Podrá tener lugar una transferencia de datos personales a un tercer país o a una organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o más sectores específicos dentro de ese tercer país, o la organización internacional en cuestión garantiza un nivel adecuado de protección. Dicha transferencia no requerirá autorización específica alguna. **(GDPR, Art. 45)** A falta de una decisión (...) un responsable o un encargado podrá transferir datos personales a un tercer país o a una organización internacional sólo si el responsable o el encargado ha proporcionado las garantías adecuadas, y siempre que se respeten los derechos exigibles del interesado y existen recursos legales efectivos para los interesados. Las salvaguardias adecuadas (...) podrán establecerse, sin necesidad de autorización específica de una autoridad de control, mediante: a) un instrumento jurídicamente vinculante y ejecutable entre autoridades u organismos públicos;

ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular; f) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial. **(Ley 1581 de 2012, Art. 26)**	b) normas corporativas vinculantes; c) cláusulas tipo de protección de datos adoptadas por la Comisión; d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión e) un código de conducta aprobado f) un mecanismo de certificación aprobado **(GDPR, Art. 46)**

4. Incidentes de seguridad

En Colombia, no existe una ley específica que regule este tema. El marco normativo actual sobre incidentes de seguridad se ha construido principalmente a través de resoluciones y guías orientadoras de la Superintendencia de Industria y Comercio. Es indispensable que este tema quede documentado en una ley.

El GDPR contempla lo siguiente: En caso de violación de datos personales, el responsable del tratamiento deberá notificar la violación de datos personales a la autoridad de control competente (...) a más tardar 72 horas después de haber tenido conocimiento de ella. (...) La notificación a que se refiere el apartado 1 deberá, como mínimo:

- Describir la naturaleza de la violación de datos personales, incluyendo, (...) las categorías y el número aproximado de interesados afectados (...) y el número aproximado de registros de datos personales afectados;
- Comunicar el nombre y los datos de contacto del delegado de protección de datos
- Describir las posibles consecuencias de la violación de datos personales;
- Describir las medidas adoptadas o propuestas a adoptar por el responsable del tratamiento para abordar la violación de datos personales

El responsable del tratamiento documentará cualquier vulneración de datos personales, incluidos los hechos relacionados con la vulneración de datos personales, sus efectos y las medidas correctivas adoptadas. 2. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento del presente artículo.

Se ve necesario aportar mayor claridad en la Ley, y los criterios del GDPR resultan razonables a la luz de la realidad colombiana. Adopción de criterios de materialidad para reportarlos y mayores garantías procesales que faciliten el que las entidades adopten el camino de la revelación, indicación clara de mecanismos que demuestren el accountability y esquemas de cooperación con la Autoridad y otras organizaciones en procura de identificar patrones comunes que puedan estar afectando a determinadas actividades.

5. Herramientas para afianzar el cumplimiento en datos personales

Privacidad por diseño y por defecto: El GDPR es claro en establecer que El responsable del tratamiento implementará medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se procesen los datos personales que sean necesarios para cada propósito

específico del procesamiento. Esa obligación se aplica a la cantidad de datos personales recopilados, el alcance de su procesamiento, el período de su almacenamiento y su accesibilidad. En particular, tales medidas garantizarán que, por defecto, los datos personales no sean accesibles sin la intervención del individuo a un número indefinido de personas físicas.

Valoración de impacto de proyectos: es una herramienta que permite prever y evaluar de manera anticipada cuales son los potenciales riesgos que conlleva una actividad que implique el procesamiento de datos personales. De esta manera se pueden adoptar medidas oportunas que permitan mitigarlos. El GDPR en el Art. 35 establece:

- 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."
- Esta herramienta es fundamental, contribuye de manera significativa al enfoque preventivo y en el contexto actual de adopción de nuevas tecnologías con un alto uso de datos personales es muy deseable tenerla establecida de manera formal en la Ley"

6. Definición de lineamientos sobre el tratamiento de información personal en fuentes de acceso público y que no constituye un dato de naturaleza pública

La ley debe buscar establecer los lineamientos frente al tratamiento de información personal privada, semiprivada o sensible que puede ser publicada por los Titulares o terceros en fuentes de acceso público como páginas web, blogs, redes sociales, entre otros. Lo anterior, teniendo en cuenta la expectativa de privacidad de los Titulares y la existencia de mecanismos como el web scraping.

7. Vigencia y periodo de transición:

Dados los cambios y el impacto que generaría esta normativa en el tratamiento de datos personales, se recomienda establecer periodos de transición razonables para que las organizaciones puedan adaptar su Programa Integral de Gestión de Datos Personales de manera gradual, eficiente y responsable. Estos periodos pueden ser diferenciados de acuerdo a la complejidad de estos periodos pueden ser diferenciados acorde con el tamaño de las empresas, pymes, empresas grandes, entidades públicas.

8. Ámbito de aplicación

La ley debe actualizarse incluyendo la aplicación del principio de extraterritorialidad, para estos efectos el GDPR es un muy buen referente. A la fecha la Autoridad se queda corta al

momento de iniciar investigaciones a terceros establecidos fuera del territorio colombiano, pues si bien bajo el Art.21 de la Ley puede adelantar las investigaciones del caso y ordenar medidas, la parte coactiva de esas medidas está sin piso.

II. RECOPILACIÓN DE LOS COMENTARIOS MÁS RELEVANTES SOBRE EL PROYECTO DE LEY

COMENTARIOS GENERALES

1. Lenguaje claro y sencillo: El proyecto debe ir encaminado a brindar un entendimiento claro y sencillo no solo para aquellos que tratan datos personales sino también para los titulares de los datos, así se genera así una mayor conciencia y cultura de protección. La casuística y el lenguaje utilizado en el proyecto para regular en detalle dificulta el entendimiento y, por lo tanto, en un futuro la aplicación del régimen de protección de datos que se propone.

2. Entidades públicas: Las entidades públicas son uno de los principales Responsables en el tratamiento de los datos personales por lo que es importante reforzar las obligaciones que tienen el marco de la estructura del tratamiento en Colombia. Se sugiere revisar la competencia de la Autoridad de Datos en materia de entidades públicas, se echa de menos que no se vigorice el rol de la Procuraduría o que se le asigne esa función también a la SIC.

ARTÍCULO	COMENTARIOS ADAPRI
Artículo 1. Objeto. La presente ley establece las normas relativas a la protección de las personas naturales en lo que respecta a la protección y tratamiento de sus datos personales y las normas relativas a la libre circulación de tales datos. De igual manera, la presente ley protege los derechos y garantías fundamentales de las personas naturales y, en particular, su derecho fundamental a la protección de los datos personales, en los términos descritos en los artículos 15 y 20 de la Constitución Política.	Consideramos que dicho objeto **excluye el tratamiento de datos financieros, crediticios,** etc. de personas jurídicas de acuerdo con lo establecido en la Ley 1266 de 2008 por lo que no deja claridad si el espíritu del proyecto busca o no la unificación del régimen general y especial con los que contamos actualmente.
Artículo 6. Principios relativos al tratamiento.	1. **El Articulo 6 elimina el principio de libertad** que actualmente se encuentra establecido en el artículo 4-literal c) de la Ley 1581 de 2012

1. El tratamiento de datos personales deben darse en virtud de los siguientes principios: a) «Principio de Legalidad»: El tratamiento de los datos personales debe sujetarse a lo establecido en la presente ley y en las demás disposiciones que la desarrollen. b) «Principio de lealtad»: las finalidades con la que se recolectan datos personales encontrarán sus límites en la presente ley y no podrán obtenerse por vías fraudulentas, engañosas, ni por acciones que puedan calificarse como dolosas. c) «Principio de transparencia»: exige que la Información facilitada a los titulares sea concisa, accesible e inteligible utilizando un lenguaje claro y sencillo. d) «Principio de limitación de la finalidad»: los datos deben ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 85, numeral 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, investigación científica, histórica o estadística no se considerará incompatible con los fines iniciales; e) «Principio de minimización de datos»: sólo se deben recabar los datos adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. f) «Principio de exactitud» Los datos de carácter personal deberán ser exactos de tal forma que respondan con veracidad a la situación actual del titular. Si fuera necesario, actualizados; se adoptarán todas las medidas razonables para rectificar o suprimir, sin dilación indebida, los factores	el cual determina que el tratamiento solo puede ejercerse con el consentimiento previo, expreso e informado del titular, salvo que haya base legal o jurídica que legitime el tratamiento. Si bien entendemos que el proyecto de ley busca ampliar las bases jurídicas del tratamiento, sugerimos evaluar la inclusión de una definición similar al principio de libertad que se acople a lo establecido en la propuesta, ya que el consentimiento sigue siendo la base jurídica principal que legitima el tratamiento en la cual se basa la mayoría del proyecto. Además, el principio de libertad ha sido de amplia importancia para el desarrollo jurisprudencial del habeas data en Colombia y es una garantía 4 para la protección de derechos 2. numeral 2 Se modifica la definición de principio de Responsabilidad Demostrada desconociendo todo el desarrollo e implementación realizado a la fecha.

que introducen las inexactitudes en los datos personales con respecto a los fines para los que se tratan. Los datos facilitados directamente por el titular se considerarán exactos. g) « Principio de limitación del plazo de conservación» los datos deben ser mantenidos de forma que se permita la identificación de los titulares 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 en cumplimiento de un deber legal o contractual, atendiendo a las disposiciones aplicables a los aspectos administrativos, contables, fiscales, jurídicos, con fines de archivo en interés público, investigación científica, histórica o estadística, de conformidad con el artículo 85, numeral 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone la presente ley a fin de proteger los derechos y garantías de los titulares; h) «Principio de integridad»: consiste en implantar las medidas de seguridad técnicas y organizativas que garantice que el dato no sea alterado de manera no autorizada. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error; i) «Principio de confidencialidad»: Los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase del tratamiento tendrán el deber de garantizar que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. El responsable y/o	

encargado del tratamiento están obligados a garantizar la reserva de la información, inclusive después de finalizado el tratamiento. El principio señalado en el literal anterior será complementario de los deberes de secreto profesional de conformidad con su normativa aplicable. k) «Principio de seguridad»: Los responsables y/o encargados del tratamiento deberán realizar análisis de riesgos orientado a determinar las medidas técnicas y organizativas necesarias para garantizar la integridad, la disponibilidad y la confidencialidad de los datos personales que traten. l) «Principio de proporcionalidad»: Es una herramienta metodológica que pretende aportar racionalidad, predictibilidad y legitimidad al tratamiento de datos personales. Este principio se traduce en realizar una ponderación atendiendo a tres criterios: a) Idoneidad: La medida es capaz de alcanzar el objetivo propuesto b) Necesidad: No exista otra medida más moderada e igual de eficaz para conseguir tal objetivo c) Proporcionalidad en sentido estricto: Hay que ponderar el beneficio que el tratamiento, desde el punto de vista de la protección de datos, proporciona a la sociedad manteniendo un equilibrio con el impacto que representa sobre otros derechos fundamentales. 2. «Principio de responsabilidad demostrada» «accountability»: El responsable del tratamiento deberá dar cumplimiento a lo dispuesto en la presente	

ley y las disposiciones que la desarrollan, siendo capaz de demostrarlo. 3. «Principio de Neutralidad Tecnológica»: la presente ley se aplicará en el uso de tecnologías y herramientas para el tratamiento de datos personales. Su aplicación no se limita a una única forma de tratar la información, ni es excluyente de tecnologías existentes, ni perderá vigencia frente a las futuras.	
Artículo 8. Condiciones para el consentimiento 1. Cuando el tratamiento se base en el consentimiento del titular, el responsable deberá ser capaz de demostrar que aquel consintió de forma previa el tratamiento de sus datos personales. 2. Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del titular por cualquier medio de prueba admisible en derecho. 3. Si el consentimiento del titular se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, debiendo constar cada finalidad de forma separada, inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción de la presente ley. 4. El responsable establecerá mecanismos o procedimientos que permitan al titular manifestar su consentimiento mediante un acto afirmativo que refleje una manifestación de voluntad libre, espontánea, específica, informada e inequívoca. Cuando el tratamiento tenga varios fines, debe darse	1. numeral 4 Sugerimos evaluar añadir la palabra “expresa” como requisito del consentimiento, de acuerdo al desarrollo jurisprudencial y normativo adelantado por la Corte Constitucional y la SIC 2. Numeral 6 **Se sugiere incluir en el numeral 6 una disposición que indique expresamente en qué supuestos procede la revocatoria del consentimiento** y tener en cuenta que el consentimiento no podrá ser revocado cuando exista una obligación legal o contractual del titular de permanecer en la base de datos.

el consentimiento para todos ellos. El silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. 5. Si el responsable del tratamiento solicita el consentimiento del titular durante la ejecución de un contrato y este no guarda relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al titular que manifieste expresamente su negativa al tratamiento. 6. El titular tendrá derecho a revocar su consentimiento en cualquier momento. La revocatoria del consentimiento no afectará a la legalidad del tratamiento basada en el consentimiento previo a la revocatoria. Será tan fácil revocar el consentimiento como darlo.	
Artículo 15. Tratamiento de datos sensibles. 1. Queda prohibido el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, el tratamiento de datos genéticos, neurodatos, datos biométricos dirigidos a identificar de manera unívoca a una persona natural, datos relativos a la salud o datos relativos a sexo o características biológica, su identidad o expresión de género, la vida sexual o la orientación sexual de una persona natural. 2. El numeral 1 no será de aplicación cuando concurran las siguientes excepciones: a) Cuando el titular dio su consentimiento previo y expreso para el tratamiento de dichos datos personales para uno o más fines específicos, excepto cuando la ley impida al	1. Numeral 1 **Es importante revisar la inclusión de los neurodatos** desde su concepción y regulación internacional teniendo en cuenta que en Colombia aún es tímida su regulación como dato personal 2. Concepción general La concurrencia de las excepciones genera inconvenientes para el tratamiento de datos sensibles. Bajo ninguna circunstancia se debería exigir que todas las excepciones concurran, especialmente porque esto dificultaría la posibilidad de aplicar las mismas y porque incluso pueden ser excluyentes.

titular levantar la prohibición mencionada en el numeral 1. b) Cuando sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del Derecho laboral o de la seguridad social, en la medida en que así lo autorice la ley o un convenio colectivo con arreglo a la normatividad vigente, que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del titular; c) Cuando el tratamiento sea necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto que el titular se encuentre incapacitado física o jurídicamente para autorizar dicho tratamiento; d) Cuando el tratamiento sea realizado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otra organización sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los titulares; e) Cuando el tratamiento se refiera a datos personales que el titular de forma libre y voluntaria decida hacer públicos. No debe ser una divulgación de datos accidental, inadvertida o involuntaria. f) Cuando el tratamiento sea necesario para la formulación, el ejercicio o la defensa de reclamaciones y/o procedimientos	Solo a modo de ejemplo, si el titular está incapacitado ciertamente no podrá otorgar el consentimiento, luego las excepciones no concurrirían como lo requiere el artículo. Adicionalmente, observamos que se plantean demasiadas excepciones a la prohibición de tratar datos sensibles que más bien pareciese la regla 5 excepciones. Algunas de las excepciones resultan incluso poco proteccionistas de los derechos del titular, permitiendo el tratamiento de datos sensibles (sin límite a las finalidades) cuando el titular haga públicos sus datos. En el mismo sentido, dicho literal parece sugerir, por ejemplo, que al publicar una fotografía en redes sociales se está autorizando el tratamiento de esta información de carácter sensibles de manera abierta ilimitada, lo cual sería un despropósito.

administrativos y/o judiciales, así como a procedimientos extrajudiciales o cuando sea un órgano judicial que actúe en ejercicio de su función. g) Cuando el tratamiento sea necesario por razones de interés público sobre la base de la normativa, que debe ser proporcional al objetivo perseguido, respetando el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los derechos y garantías fundamentales del titular; h) Cuando el tratamiento sea necesario para fines de medicina preventiva o laboral, evaluaciones médicas ocupacionales del trabajador, diagnóstico médico, prestación de asistencia o tratamiento médico, o gestión de los sistemas y prestación de servicios de salud, sobre la base de la normativa o en virtud de un contrato con un profesional de la salud y sin perjuicio de las condiciones y garantías contempladas en el numeral 3 del presente artículo; i) Cuando el tratamiento sea necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transnacionales graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base de la norma, que establezca medidas adecuadas y específicas para proteger los derechos y garantías del titular, en particular el secreto profesional. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y garantías de las personas naturales. j) El tratamiento es necesario con fines de archivo en interés público, investigación	

científica, histórica o estadística, de conformidad con el artículo 85, numeral 1, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular. 3. Los datos personales a que se refiere el numeral 1 podrán tratarse a los fines citados en el numeral 2, literal h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto profesional de acuerdo con el artículo 74 de La Constitución Política de Colombia. **Parágrafo**. Cuando por alguna de las causales a las que se refiere el numeral segundo se deban tratar datos sensibles referentes al sexo, identidad o expresión de género y orientación sexual, deberán hacer uso de todas las categorías identitarias diversas, como personas intersexuales y no binarias. En el supuesto de que el titular del dato haya dado su consentimiento para el tratamiento de los datos aquí referidos y ejercite los derechos de rectificación y supresión, no se le exigirán requisitos adicionales para comprobar esta información.	
Artículo 26. Derecho de rectificación en medios de comunicación. 1. El derecho a la rectificación implica la corrección de la información que atente contra el principio de exactitud. Para que sea	**Este artículo no corresponde ni debe ser legislado en una ley de habeas data o datos personales.** La rectificación en medios de comunicación no afecta exclusivamente datos personales, y además

efectivo, debe tener un despliegue comunicativo similar al inicial y que el medio de comunicación reconozca su error. 2. El derecho se ejercitará mediante la presentación de la solicitud de rectificación al oficial de protección de datos o área designada para la protección de datos por el medio de comunicación o, de forma tal que permita tener constancias de su fecha y de su recepción. La rectificación deberá limitarse a la información que se desea rectificar. 3. Siempre que el derecho se ejercite de conformidad con lo establecido en el numeral anterior, el medio de comunicación deberá publicar o difundir íntegramente la rectificación en las condiciones descritas en el numeral 1, dentro de los tres días hábiles siguientes al de su recepción, prorrogables por única vez y por el mismo término, con relevancia semejante a aquella en que se publicó o difundió la información que se rectifica, sin comentarios ni apostillas. Cuando no fuere posible atender la solicitud de rectificación dentro de los tres días hábiles, se informará al titular los motivos de la demora. 4. Podrán ejercitar el derecho de rectificación el titular afectado o sus representantes y, si hubiese fallecido aquél, sus familiares o herederos o los representantes de éstos. 5. Si en el término señalado en el numeral 3, no se hubiera publicado o divulgado la rectificación o se hubiese notificado expresamente por el medio de comunicación que aquella no será difundida, o se haya publicado o divulgado sin respetar lo dispuesto en los numeral 1 y 3, el titular afectado tendrá derecho a ejercer las acciones constitucionales que procedan y	es un asunto ligado al derecho de libertad expresión y de prensa. El artículo debería ser eliminado de este proyecto, entre otras, por las siguientes razones: 1) Si la finalidad es exigir una rectificación de datos personales, ya existen mecanismos legales (incluso incluidos en este mismo proyecto de ley) para lograrlo. 2) Es posible que el artículo vulnere la libertad de expresión, así como varios derechos fundamentales. 3) Ya existe jurisprudencia de la Corte Constitucional que delimita la libertad de expresión y de prensa en relación con el tratamiento de datos personales 4) Es importante recordar que no todo dato es un dato personal. El artículo no lo clarifica, pero sería una vulneración a derechos constitucionales solicitar la supresión o rectificación de datos no personales tratados por un medio de comunicación sin que exista una justa causa. En razón de los puntos anteriores, sugerimos eliminar este artículo

también el derecho de indemnización del que habla el artículo 89 de la presente ley. 6. Los responsables de redes sociales y plataformas de servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación del contenido que otros usuarios difundan y atente contra el principio de exactitud en Internet.	
Artículo 40. Representantes de responsables o encargados del tratamiento con domicilio fuera del territorio Nacional. 1. Cuando sea de aplicación el artículo 3 numeral 2, el responsable o el encargado del tratamiento designará por escrito un representante legal y/o sucursal en Colombia. 2. La obligación establecida en el numeral 1 del presente artículo no será aplicable: a) Al tratamiento de datos que sea ocasional, que no incluyan el manejo a gran escala de categorías especiales de datos indicadas en el artículo 15 numeral 1, o de datos personales relativos a delitos y condenas penales a que se refiere el artículo 16, y que sea improbable que entrañe un riesgo para los derechos y garantías de las personas naturales, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento, o; b) A las autoridades u organismos públicos. 3. El responsable o el encargado del tratamiento encomendará al representante las facultades necesarias a fin de garantizar el cumplimiento de lo dispuesto en la presente ley. 4. La designación de un representante por el responsable o el encargado del tratamiento	Numeral 2 Se establece un tratamiento de datos "ocasional" situación que puede traer interpretaciones distintas frente al tratamiento de datos por lo que el tratamiento así sea ocasional ya genera tratamiento y podría estar vulnerando el derecho del titular a ejercer sus derechos frente al responsable Este artículo no es claro, en nuestra opinión genera confusiones con el régimen corporativo de sucursales o establecimientos permanentes. Deberían fijarse mecanismos que faciliten el cumplimiento del régimen local de datos por las entidades extranjeras que realicen el tratamiento en Colombia; no consideramos que obligarlas a crear una sucursal o nombrar un representante legal por el solo tratamiento de los datos sea adecuado, ni legal. **No se puede obligar a una entidad, a constituir una entidad legal por el simple hecho de realizar un tratamiento de datos, generando obligaciones en materia tributaria y corporativa que parecerían desproporcionadas.** Tratándose del representante sugerimos que no sea denominado "representante legal",

se entenderá sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable o encargado.	así como aclarar como funcionaría ese mecanismo. Sin embargo, es clara la necesidad de lograr coercibilidad frente a procesadores de datos que estén fuera del territorio nacional. Se recomienda revisar cuál sería la mejor forma de hacerlo sin generar un impacto adverso que haga excesivamente oneroso o difícil el poder desarrollar la actividad.
Artículo 49. Notificación de un Incidente de seguridad de los datos personales a la autoridad de control. 1. En caso de Incidente de seguridad de los datos personales, el responsable del tratamiento lo notificará a la Superintendencia de Industria y Comercio de conformidad con el artículo 73 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicho Incidente de seguridad constituya un riesgo para los derechos y las garantías de las personas naturales. Si la notificación a la Superintendencia de Industria y Comercio no tiene lugar en el plazo de 72 horas, deberá ir acompañada de los motivos que expliquen la dilación. 2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento los incidentes de seguridad de los datos personales de las que tenga conocimiento. 3. La notificación contemplada en el numeral 1 deberá, como mínimo: a) Describir la naturaleza de la Incidente de seguridad de los datos personales y, cuando sea posible, el número aproximado y tipo de titulares afectados, las categorías de datos y	La regla que se propone no es clara, ¿puede haber incidentes que no deban reportarse o lo único que cambia es el plazo? Si lo que se busca es que no todos los incidentes sean notificados, se debería entonces ser claro en cuanto a la definición de qué incidentes constituyen riesgos o garantías Por otro lado, 72 horas es insuficiente, en compañías medianas y grandes la realización de estos reportes implica la coordinación de diferentes áreas, lo que no es posible en el tiempo planteado. Los 15 días hábiles que actualmente se contemplan en la Circular Única de la SIC son razonables y atienden a la realidad de los negocios.

el número aproximado de registros de datos personales afectados; b) Comunicar el nombre y los datos de contacto del oficial de protección de datos o de otro punto de contacto en el que pueda obtenerse más información; c) Describir las posibles consecuencias del Incidente de seguridad de los datos personales; d) Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio al Incidente de seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos. 4. Si no fuera posible facilitar la información descrita en el numeral 3 del presente artículo simultáneamente con la notificación de un incidente de seguridad, y en la medida que esta condición persista, la información se facilitará de manera gradual sin dilación indebida. 5. El responsable del tratamiento documentará cualquier Incidente de seguridad de los datos personales, incluidos los hechos relacionados con este, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo. 6. Los datos personales contenidos en la notificación de una Incidente de seguridad y que fueron comunicados a la Superintendencia de Industria y Comercio, proveedores de tecnologías y servicios de seguridad, podrán ser tratados exclusivamente durante el tiempo y alcance necesario para su análisis, detección protección y respuesta ante el incidente y	

adoptando medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.	
Artículo 52. Consulta previa. 1. El responsable del tratamiento consultará ante la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio antes de llevar a cabo un tratamiento cuando, de la evaluación de impacto de que trata del artículo 51, se concluya que dicho tratamiento supondría un alto riesgo para los derechos y garantías de los titulares. 2. Cuando la Delegatura para la Protección de Datos Personales considere que el tratamiento previsto en el numeral 1 suponga un alto riesgo para los derechos y garantías de los titulares, asesorará por escrito al responsable, y en su caso al encargado, entre otras cosas respecto de las medidas técnicas y organizativas que se deberán adoptar previo al tratamiento de los datos. La Delegatura para la Protección de Datos Personales deberá, en un plazo de 3 meses contados a partir de la fecha en que el responsable, o en su caso el encargado, acude ante ella, emitir un concepto. Este plazo podrá prorrogarse, en función de la complejidad del tratamiento, por única vez, por un periodo igual a la inicial, informando al responsable y, en su caso, al encargado del tratamiento de tal prórroga, indicando los motivos de la dilación. 3. El escrito que el responsable del tratamiento allegue a la Superintendencia de Industria y Comercio deberá contener como mínimo la siguiente información:	1. numeral 2 **Dicha disposición impone una carga a la Superintendencia de Industria y Comercio de asesoría concreta que puede superar el capital humano y técnico y puede ralentizar los procesos.** Se sugiere eliminar la asesoría personalizada y reemplazarlo por el establecimiento de lineamientos generales. Así mismo se sugiere modificar la consulta previa para que no sea entendido como un requisito de procedibilidad para llevar a cabo el tratamiento sino más bien una medida de responsabilidad demostrada que acredite ante la SIC que hubo un estudio previo. 2. Así mismo, el parágrafo debería establecer un plazo máximo para que la SIC pueda pedir la complementación de la información (e.g., 15 días hábiles desde la presentación de la solicitud).

a) En caso de ser procedente, las responsabilidades respectivas del responsable, y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial; b) Los fines y medios del tratamiento previsto; c) Las medidas establecidas para proteger los derechos y garantías de los titulares de conformidad con la presente Ley; d) En su caso, los datos de contacto del oficial de protección de datos; e) La evaluación de impacto relativa a la protección de datos establecida en el artículo 51 de esta ley; f) Cualquier otra información que solicite la autoridad nacional de protección de datos. **Parágrafo:** Cuando la Superintendencia de Industria y Comercio deba requerir información y/o documentación adicional, los términos establecidos en el numeral 2 del presente artículo se suspenderán hasta que la información y/o documentación se haya obtenido o hasta que el plazo otorgado para suministrarlos, se haya cumplido.	
Artículo 92. Derecho a indemnización y responsabilidad. 1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia del incumplimiento de cualquiera de las obligaciones contenidos en la presente ley, tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos. 2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que	En lo relativo al régimen indemnizatorio propuesto, sugerimos evaluar los siguientes aspectos: 1) Primero, si el régimen también contempla a subencargados o a terceros cesionarios como sujetos responsables, pues es evidente que estos también pueden cometer infracciones.

dicha operación no cumpla lo dispuesto por la presente ley. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento, cuando no haya cumplido con las obligaciones de la presente ley dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable. 3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del numeral 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios. 4. Cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado hayan participado en la misma operación de tratamiento y sean, de conformidad a los numerales 2 y 3, responsables de cualquier daño o perjuicio causado por dicho tratamiento, cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado. 5. Cuando, de conformidad con el numeral 4, un responsable o encargado del tratamiento haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados, de conformidad con las condiciones fijadas en el numeral 2. 6. La Superintendencia de Industria y Comercio será competente para conocer y decidir sobre la acción descrita en el	2) Recomendamos evaluar la pertinencia de añadir este artículo al proyecto, ya que, de cara al régimen de responsabilidad civil extracontractual, es posible que se le esté atribuyendo a la SIC jurisdicción en una materia que no debería ser de su conocimiento; o de ser el caso debería aclararse que se le están otorgando funciones jurisdiccionales en esta materia. y así modificar las funciones de dicha dependencia.

presente artículo por el incumplimiento de las obligaciones de la presente ley, sin perjuicio del derecho que tiene el titular de acceder a la administración de justicia.	
Artículo 108. Vigencia y Derogatorias. La presente ley entra en vigencia desde su promulgación y será de aplicación obligatoria seis meses después, salvaguarda los derechos adquiridos y deroga todas las disposiciones que le sean contrarias. También deroga la Ley 1581 de 2012, sus decretos reglamentarios y demás normativa relacionada que sea contraria a las disposiciones de la presente ley.	Haciendo referencia a nuestro comentario anterior sobre los numerales 2 y 23 del artículo 5, solicitamos evaluar la posibilidad de clarificar que el régimen de protección de datos **continuará con una estructura dividida entre un régimen general y un régimen especial de habeas data financiero y creditico**, ya que encontramos una contradicción entre lo dispuesto en la exposición de motivos y el articulado del proyecto de ley, que en ningún momento unifica regímenes ni deroga o modifica integralmente ningún artículo de las leyes 1266 de 2008 y 2157 de 2021. Debido a lo anterior y para evitar confusiones jurídicas, vacíos legales y contradicción entre los regímenes, sugerimos regular en el marco normativo la coexistencia de regímenes existentes.

COLOMBIA POTENCIA DE LA VIDA

Industria y Comercio
SUPERINTENDENCIA

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO	
RADICACION: 24-97083- -0-0	**FECHA:** 2024-03-05 08:08:05
DEPENDENCIA: 12 GRUPO DE TRABAJO DE REGULACIÓN	**EVENTO:** SIN EVENTO
TRAMITE: 334 REMISIINFORMA	**FOLIOS:** 10
ACTUACION: 425 REMISIONIFORMACI	

Bogotá D.C.

Doctora
AMPARO YANETH CALDERÓN PERDOMO
Comisión Primera Constitucional Permanente
CÁMARA DE REPRESENTANTES
CONGRESO DE LA REPÚBLICA
comision.primera@camara.gov.co

Asunto: Comentarios de la **SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO** al texto radicado del Proyecto de Ley Estatutaria No. 156 de 2023 (**CÁMARA**) "*Por la cual se dictan disposiciones para el régimen general de datos personales*" (en adelante el "*proyecto*").

Respetada Doctora:

Esta Superintendencia realiza un seguimiento permanente a los proyectos de ley que pueden tener incidencia en el ejercicio de las funciones que le han sido asignadas. En consecuencia, y después de haber revisado la iniciativa indicada en el asunto, nos permitimos poner a su consideración los siguientes comentarios:

Para comenzar, es pertinente mencionar que, si bien el proyecto se presenta como respuesta a varias inquietudes que se han planteado sobre el régimen de protección de datos establecido por la Ley Estatutaria 1581 del 2012, se considera indispensable no dejar de lado lo implementado y aprendido en los últimos 10 años. Por lo tanto, en consideración de esta Entidad resulta más adecuado fortalecer o complementar el régimen jurídico vigente en lugar de derogar la norma actual e implementar nuevas disposiciones; situación con la potencialidad de generar un escenario de inseguridad jurídica tanto para los administrados como para la autoridad competente de su implementación.

Lo anterior en la medida en que, existen conceptos y principios que a la fecha cuentan con un entendimiento, aplicación y desarrollo no sólo por los administrados (responsables, encargados, titulares, etc.) sino por la misma autoridad de datos y la **CORTE CONSTITUCIONAL**. En tal sentido, se resaltan conceptos como "*encargado*", "*responsable*", "*transmisión/ transferencia nacional o internacional*", "*Titulares*", "*contrato de transmisión*", "*política de tratamiento de información*", entre otros, que funcionan adecuadamente sin perjuicio de ser susceptibles de mejora.

Así mismo, el trámite de una reforma a la Ley Estatutaria 1581 de 2012 y no una sustitución normativa podría ser más expedito, considerando la extensión del texto y, además, no se

exigiría la revisión de la **CORTE CONSTITUCIONAL** en asuntos que ya fueron objeto de evaluación en la Sentencia C-748 de 2011[1].

De otra parte, la casuística y el lenguaje utilizado en el proyecto para regular en detalle, dificulta el entendimiento y, por lo tanto, en un futuro, la aplicación del régimen de protección de datos propuesto. Una estructura basada en reglas generales y principios tal y como se ha venido implementando, permite que la ley tenga mayor vigencia en el tiempo, pues mantendrá la capacidad de adaptarse a nuevos escenarios y situaciones. Solamente por excepción deberían regularse de manera detallada temas que, por su particularidad o la falta de antecedentes normativos, lo ameriten.

En este sentido, el proyecto debería encaminarse a brindar un entendimiento claro y sencillo no sólo para aquellos que tratan datos personales, sino también para los titulares y responsables, generando así una mayor conciencia y cultura en la materia.

Adicionalmente, el proyecto propone una modificación del régimen sancionatorio. En tal sentido, estaríamos pasando de un régimen en el que se analiza el incumplimiento de los deberes a donde se analiza si el sujeto obligado realizó una conducta prohibida (tipificación de conductas), lo cual puede llegar a ser problemático toda vez que la norma en un futuro podría quedarse corta ante la hipótesis de un acto que si bien es contraria a la norma —alguna obligación— no esté tipificado.

En consecuencia, para poder garantizar una mayor cobertura en la protección del derecho fundamental se debe evitar entrar en detalles o situaciones particularizadas, pues si el Legislador regula de esa manera, en la práctica se estarían generando mayores riesgos de desprotección para los titulares de la información.

Al respecto, es pertinente mencionar que, una de las grandes ventajas del régimen actual es la neutralidad temática y tecnológica, pues esto ha permitido su vigencia en el tiempo, en tanto las disposiciones abarcan situaciones generales y no específicas; es decir, el régimen de protección de datos personales actual es general y aplica para unas actividades en específico. Por consiguiente, se sugiere conservar esas características para evitar así una pronta obsolescencia legislativa por los mismos cambios sociales y tecnológicos.

Hechas las anteriores salvedades, a continuación, se remiten sugerencias frente a los artículos que consideramos deberían permanecer en el proyecto, pero merecen algunas modificaciones:

[1] Precisamente, en la Sentencia C-748 de 2011 de la **CORTE CONSTITUCIONAL** se adelantó el análisis del proyecto correspondiente a la Ley Estatutaria 1581 de 2012.

Artículo	Observaciones de esta Superintendencia
2 **Ámbito de aplicación material**	"***Artículo 2. Ámbito de aplicación material.*** *1. La presente ley se aplica al tratamiento total o parcialmente automatizado, así como el tratamiento no automatizado de los datos personales registrados o destinados a ser incluidos en bases de datos.* *2. La presente ley no se aplicará al tratamiento de datos personales cuando:* ~~*a) En el ejercicio de una actividad no comprendida en el ámbito de aplicación del ordenamiento jurídico colombiano;*~~ *b) Efectuado por una persona natural en el ejercicio de actividades exclusivamente personales o domésticas;* *c) Por parte de las autoridades competentes con fines de prevención, investigación, detección o monitoreo de actos delictivos incluido el lavado de activos y financiación de terrorismo, la ejecución de sanciones penales, así como la de protección frente a amenazas a la seguridad nacional pública y su prevención.* *d) A las bases de datos y archivos de información periodística y otros contenidos editoriales, mientras que su tratamiento no represente una vulneración a los derechos de protección de datos personales y otros derechos fundamentales y garantías constitucionales de los titulares.* *e) A las bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia* *Parágrafo 1: El Gobierno Nacional, ~~legislará~~ reglamentará sobre de protección de datos personales tratados para fines de prevención, investigación, detección o monitoreo de actos delictivos incluido el lavado de activos y financiación de terrorismo, la ejecución de sanciones penales.* *Parágrafo 2: Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley*". (El texto subrayado corresponde a la modificación propuesta por esta Entidad).
3 **Ámbito de aplicación territorial**	"***Artículo 3. Ámbito territorial.*** *1. La presente ley se aplica al tratamiento de datos personales en el contexto de las actividades de los responsables o del encargado con domicilio y/o residencia en territorio nacional, independientemente de que el tratamiento tenga lugar o no en Colombia.* *2. La presente ley se aplica al tratamiento de datos personales de titulares que residan en territorio nacional por parte de un responsable o encargado no establecido en Colombia, cuando las actividades de tratamiento estén relacionadas con:*

	a) La oferta de bienes o servicios a dichos titulares en Colombia, ~~independientemente de si estos son de carácter oneroso,~~ o; *b) El control de su comportamiento, en la medida en que este tenga lugar en Colombia.* *3. Cuando proceda la aplicación de la legislación nacional en virtud del Derecho Internacional público, la presente ley deberá aplicarse también a todo responsable no establecido en Colombia pero que actúa en virtud de una misión diplomática, embajada u oficina consular".* (El texto subrayado corresponde a la modificación propuesta por esta Entidad).
4 **Datos de personas fallecidas**	"***Artículo 4. Datos de personas fallecidas.*** *Los causahabientes podrán dirigirse al responsable o encargado del Tratamiento con el objeto de solicitar el acceso, rectificación o supresión de los datos personales de la persona fallecida*". (El texto subrayado corresponde a la modificación propuesta por esta Entidad).
5 **Definiciones**	Se sugiere suprimir definiciones referentes a la Leyes Estatutarias 1266 de 2008 y 2157 de 2021, e incluir la definición de "*Encargado*" en los términos de la Ley Estatutaria 1581 de 2012, así: "*Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento*". Además, se encuentra necesario diferenciar "*cesión o comunicación de datos personales*" con "*transferencia de datos personales*"; así mismo, considerar la posibilidad de una definición amplia (nacional o internacional) de "*Transferencia*". Por ejemplo: "*La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país*". Por último, se sugiere analizar la definición de "*incidente de seguridad*" desde la Circular Única de esta Entidad, la cual enuncia: "*Se refiere a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el Responsable del Tratamiento o por su Encargado".* Y analizar la conveniencia de dejar las siguientes definiciones: "*Grupo empresarial*", "*elaboración de perfiles*", "*organización internacional*".
6 **Principios**	Se recomienda fortalecer el principio de "*Responsabilidad Demostrada*", como aquel ya establecido en la Ley Estatutaria 2157 de 2021, según el cual: "*Todas las personas que intervengan en el Tratamiento deben ser capaces de demostrar que han implementado medidas apropiadas, efectivas y verificables para cumplir con las obligaciones establecidas en la presente ley y sus normas reglamentarias*". De igual forma, es pertinente mantener el "*principio de acceso y circulación restringida*", así: "*Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley*".

	En relación con el "*Principio de Proporcionalidad*", se sugiere agregar: "*Este principio se traduce en realizar una ponderación atendiendo, entre otros, los siguientes tres criterios:* (…)" (el texto subrayado corresponde a la modificación propuesta por esta Entidad).
7 **Bases que legitiman el Tratamiento de la información**	En el literal e) —y en el resto del texto donde se reitera la expresión— se sugiere cambiar "*una misión realizada*" por "*una función realizada*".
19 **Transparencia**	Frente al numeral 5, se sugiere la siguiente modificación: "(…) *5. La información facilitada en virtud de los artículos 20 y 21 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 24 a 34 y 50 serán a título gratuito. ~~Cuando las solicitudes sean carentes de fundamento legal, temeraria y/o excesivas, especialmente debido a su carácter reiterativo, el responsable del tratamiento podrá:~~* *~~a) En el caso de ser una solicitud ya resuelta, remitirse a las respuestas anteriores;~~* *~~b) Cobrar al titular los gastos administrativos por proporcionar la información, la comunicación o realizar la actuación solicitada;~~* *~~c) Negarse a actuar respecto de la solicitud, por considerarse temeraria y reiterativa.~~* *~~Para tal efecto, se podrá considerar reiterativo el ejercicio del derecho de acceso en más de una ocasión en menos de un mes, a menos que exista causa legítima para ello. El responsable deberá demostrar a la Autoridad de Control, cuando ésta así lo requiera, que la conducta del titular es carente de fundamento legal, temeraria y/o reiterativa.~~* (…)" (el texto subrayado corresponde a la modificación propuesta por esta Entidad). Adicionalmente, para esta Superintendencia no es claro si ¿Solamente podrán utilizarse los "*iconos normalizados*" para lo establecido en el numeral 7 o si existirán otras circunstancias en las cuales se implementen para facilitar la transmisión de información a los titulares?
20 **Información que debe facilitarse cuando los datos personales se obtengan del titular**	Los dos (2) primeros numerales del artículo se deberían unificar, generando una lista más homogénea acerca de las medidas destinadas a garantizar un debido tratamiento por parte de los sujetos obligados.

21 Información que deberá facilitarse cuando los datos personales no se hayan obtenido del titular	En el numeral 2 se establece un procedimiento que se debe agotar cuando se obtienen los datos, en el cual se brinda una cierta información al titular; pero surgen las siguientes incógnitas, si la información se recolecta sin conocimiento este último ¿Cómo se cumplirá con lo propuesto en dicho numeral?, ¿Qué medidas deben adoptar los responsables? Así mismo, se contradice el numeral 2 con el 3, puesto que: el numeral 3 habla del momento en el cual se debe informar al titular; no obstante, el numeral 2 se afirma que dicha la información sobre el tratamiento se suministra "*en el momento en que se obtengan los datos personales*". Lo que genera una redacción confusa, además de las inquietudes planteadas en el párrafo anterior. Por último, se sugiere incluir lo previsto en el numeral 4 en la lista del numeral 2 del artículo en cuestión.
22 Aviso de Privacidad	Se sugiere dejar solamente la expresión "*aviso de privacidad*" para evitar la eclosión de términos o sinónimos que luego pueden llevar a tener dificultades en la interpretación de la Ley.
23 Disposiciones generales sobre el ejercicio de los derechos	En el numeral 1 del artículo se habla de la Ley 1996 de 2019 —"*Por medio de la cual se establece el régimen para el ejercicio de la capacidad legal de las personas con discapacidad mayores de edad*"—, para referir la manera como pueden un tercero puede actuar en nombre de un titular mayor de edad con discapacidad. No obstante, también es pertinente hacer referencia a la Ley 1306 de 2009 —"*Por la cual se dictan normas para la Protección de Personas con Discapacidad Mental y se establece el Régimen de la Representación Legal de Incapaces Emancipados*"—, así como a las disposiciones civiles relativas a los actos y declaraciones de la voluntad que sean aplicables.
24 Derecho de acceso	Se sugiere suprimir la siguiente expresión: "*el responsable podrá cobrar al titular los gastos administrativos por cualquier otra copia solicitada*". Esto, por cuanto en el régimen actual no se establece una norma en tal sentido y adoptar una medida así representaría una nueva carga para el titular. Además, en el numeral 1 se sugiere agregar, "*derecho de acceso a los Datos Personales y, entre otra, a la siguiente información*"; y en el numeral 2 incluir la lista de información que podría solicitarse. Por último, es pertinente suprimir el resto de los numerales.
35 Derecho a presentar una queja ante la Autoridad de Control	La propuesta contraviene lo establecido en el numeral 2 del artículo 69, toda vez que se está dejando a esta Entidad sin la facultad de proteger los derechos fundamentales. De ahí que, no habría porque contar con un mecanismo de queja, pero sí el de denuncia. En ese sentido, se sugiere suprimir los numerales 2, 4 y 5 de aquel artículo, pues los asuntos ahí referidos están regulados en la Ley 1437 de 2011. Por otro lado, se sugiere delimitar las facultades que tiene esta autoridad sobre la protección de los derechos de los titulares de la información. Por ejemplo, en la actualidad es clara la posibilidad de impartir ordenes administrativas. En tal sentido, la norma no permite identificar qué actuaciones puede adelantar la Entidad a efectos de salvaguardar el derecho de habeas data.
36 Derecho a presentar una denuncia ante la Autoridad de Control	En el numeral 1, surge la duda sobre si: ¿Se hace referencia a la protección de un interés colectivo e individual? Lo anterior, cuando se menciona: "*persiguiendo la protección del interés general y el derecho a la protección de datos personales*".

37 Obligaciones del responsable del Tratamiento	Se recomienda incluir en este artículo todos los deberes, así sea de una manera enunciativa para luego desarrollarlos. Por ejemplo, "*Los responsables del Tratamiento deberán contar con un Oficial de Protección de Datos Personales en los términos de la presente ley*".
38 Protección de Datos desde el Diseño y por Defecto	Se recomienda redactar este artículo como un deber, o incluir un nuevo artículo donde se hable de los deberes de los Responsables y Encargados de cara a la protección de datos desde el diseño y por defecto. Esto, para no solo tener un procedimiento relacionado con la materia, sino alcanzar mayor claridad acerca de qué debe hacer cada obligado para atender la "*protección de datos desde el diseño y por defecto*".
41 Encargado del Tratamiento	Los encargados del tratamiento no sólo deben de tener obligaciones contractuales y, en cambio, deberían tener obligaciones legales; así como se encuentra previsto en la Ley Estatutaria 1581 de 2012. Esto, nos permitiría ejercer de mejor manera nuestras funciones de inspección, vigilancia y control. Además, se observa que, las sanciones van dirigidas al Responsable pero no al Encargado, aun cuando ambos son sujetos obligados a la debida protección del derecho de habeas data. Esto es de suma importancia para el ejercicio efectivo de las funciones a cargo de esta Entidad. Por otro lado, técnicamente es impreciso decir "*Contrato con arreglo a las leyes civiles*", puesto que, también habrían asuntos sujetos al derecho mercantil.
44 Disposición del Registro de las actividades de Tratamiento	Se recomienda, incluir además de los registros de actividades el Registro Nacional de Bases de Datos, así: "*El Registro Nacional de Bases de Datos es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país. El registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos*".
47 Seguridad del Tratamiento	Considera esta Entidad que "*seguridad*" y "*confidencialidad*" debería estar prevista como una infracción muy grave.
51 Evaluación de impacto de privacidad	Se recomienda incluir esta evaluación como un deber de los responsables del tratamiento.
52 Consulta previa	Se recomienda, en lugar de dejar un plazo tan amplio en la Ley, establecer que sea "*En el menor tiempo posible*". También se sugiere suprimir el numeral 3 y el parágrafo.
53 Designación de un oficial de protección de datos personales	Se recomienda mejorar la redacción del literal e), ya que, no es muy claro, e incluir, además de los obligados ya establecidos, a las compañías de telecomunicaciones y a las grandes superficies de venta. Así mismo, vincular estas funciones a los deberes de los responsables del tratamiento.
58 Códigos de Conducta	Se recomienda analizar la pertinencia de cada uno de los numerales, pues se consideran viables el primero y segundo, mientras el resto se puede desarrollar vía decreto reglamentario.
59 Supervisión de Códigos de Conducta aprobados	Consideramos importante analizar con el **ORGANISMO NACIONAL DE ACREDITACIÓN DE COLOMBIA** (en adelante, **ONAC**) la posibilidad de que esta Superintendencia acredite personas para supervisar el cumplimiento de los códigos de conducta.

60 Certificación	Consideramos importante analizar con la **ONAC** la posibilidad de que esta Superintendencia tenga funciones de acreditación. De ser posible, debería dejarse bien estructurado en un solo artículo, mientras el artículo 61 podría suprimirse para ser objeto de reglamentación.
63 Transferencia basada en una declaración de conformidad	Terminología de declaración de conformidad – nivel adecuado. Sugerimos para el segundo numeral incluir los requisitos actuales, a saber: **(i)** normas aplicables al tratamiento de datos; **(ii)** consagración de principios; **(iii)** consagración de derechos de los titulares; **(iv)** consagración de deberes para responsables y encargados; **(v)** medios y vías tanto judiciales como administrativas para garantizar tutela efectiva; **(vi)** existencia de autoridad encargada de la supervisión del tratamiento. Del numeral 3 para en adelante, los asuntos pueden ser materia de decreto reglamentario o incluso de circular como lo es hoy en día.
65 Normas Corporativas Vinculantes	Se sugiere dejar como en la Ley Estatutaria 1581 de 2012, de lo contrario, acudir a cómo está en el Decreto 255 de 2022, pues se considera que el desarrollo es más claro en la reglamentación actual a como se pone en este artículo.
67 Excepciones para situaciones especificas	Es preferible la terminología de "*Reconocimiento de país con nivel adecuado*".
69 Autoridad de Control	Respecto al numeral 1, es más apropiada la redacción contenida en la Ley Estatutaria 1581 de 2012 y; en relación con el numeral 2, se sugiere aclarar el alcance de las funciones a cargo de los jueces de tutela, pues pareciera que estos últimos estarían llamados a desplazar las funciones ordinarias de la Superintendencia como autoridad administrativa en materia de datos personales. Igualmente, cuando se propone que los jueces de tutela sustituyan las competencias de esta Entidad, también da a entender que eventualmente podríamos llegar a tener facultades similares en lo jurisdiccional. En ese sentido, es más apropiado aclarar que las competencias de otras autoridades son complementarias, en tanto: **(i)** esta Superintendencia funge como autoridad administrativa; **(ii)** los jueces de tutela, como autoridades judiciales garantes del derecho fundamental de habeas data y; **(iii)** la **FISCALÍA GENERAL DE LA NACIÓN** como la competente de la persecución penal de ciertas conductas. Por tanto, no se trata de una "*sustitución de competencias*".
91 Tecnologías de Rastreo	Se sugiere considerar si, las condiciones propuestas en el artículo deben cumplirse todas o alguna de ellas.
92 Derecho de indemnización y responsabilidad	Consideramos que las facultades jurisdiccionales de reconocer daños y perjuicios deberían ser una facultad que se otorgue a la Delegatura para Asuntos Jurisdiccionales y no a la Delegatura para la Protección de Datos Personales en sede administrativa. Así mismo, es altamente inconveniente e incluso, contrario a la Constitución Política, dejar dentro de las facultades administrativas de esta Superintendencia la posibilidad de establecer indemnizaciones, pues esto corresponde a una actividad a cargo de las autoridades judiciales.

	Por tanto, se insiste, esto podría estudiarse como una facultad jurisdiccional a cargo de la Entidad, más no una atribución propia de la administración.
94 Condiciones generales para la imposición de sanciones	Consideramos problemática la redacción de los siguientes literales: a), b), c), f), l) y r). Se hace necesario considerar ¿Cuáles serían atenuantes y cuáles agravantes?; De igual forma, las condiciones generales para imposición de sanciones, así como las conductas típicas deberían estar en un punto intermedio entre el gran detalle (que genera dificultad probatoria y sancionatoria) y la generalidad (que no cumple el principio de tipicidad). Es necesario ser conscientes que sólo podremos sancionar por aquello establecido en los artículos; precisamente por la forma como se encuentra redactado el proyecto.
95-100 Régimen Sancionatorio	Desde la autoridad no vemos claro la facultad de sancionar a un encargado del tratamiento. Los deberes legales no están establecidos. De acuerdo con la jurisprudencia de la **CORTE CONSTITUCIONAL** es necesario que existan una lista de deberes claros para el adecuado ejercicio de las funciones de inspección, vigilancia y control. Al hilo de lo expuesto, sugiere que la falta de seguridad de la información se prevea como una infracción gravísima. En el artículo 99, se recomienda cambiar "*obligados al Registro de Bases de Datos*", por "*aquellos obligados a registrar sus bases de datos en el Registro Nacional de Bases de Datos.*" Igualmente, se podría incluir como una falta grave la no inscripción de las bases de datos en el "*Registro Nacional de Bases de Datos*". La expresión "*supongan una vulneración sustancial de los artículos de la presente ley*" no cumplen el estándar de tipicidad de la norma. Se deben tener presentes los artículos que se vayan a suprimir o modificar realizando las adecuaciones a las tipificaciones establecidas. El numeral 10 del artículo 96 podría tener problemas en la tipicidad. Se recomienda incluir dentro de las infracciones aquella establecida en el literal h) del artículo 17 de la Ley Estatutaria 1581 de 2012, a saber: "*h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley*". De igual forma, aquella establecida en el literal o) de la misma disposición: "*o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio*". Así mismo, en el proyecto de ley no se encuentra el deber de los responsables y encargados de "*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*". Aquel es un deber que es importante incluir en la normativa. Adicionalmente, se considera que el monto de 2000 salarios mínimos legales mensuales vigentes es una sanción baja para hoy en día. Sería interesante ver la posibilidad de aumentar el rango del valor.

	Lo anterior, permitiría que las sanciones en la materia sean mucho más disuasorias. No obstante, se recomienda tener presente la regla establecida en el artículo 313 de la Ley 2294 de 2023, respecto de la necesidad de establecer las sanciones (entre otros emolumentos) en Unidades de Valor Básico (**UVB**). En el artículo 99, se sugiere modificar, así: "*Se sancionarán con multas por un valor máximo de (...)*".
106 Transferencia internacional	Al mencionar las "*declaraciones de conformidad a terceros países*" se puede tener el problema de entender el procedimiento de solicitud de un "*Declaración de Conformidad*" regulada por la Circular Única de esta Superintendencia. Por tanto, se sugiere utilizar la terminología de "*Los reconocimientos a países con nivel adecuado por parte de la **SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO** a través de su Circular Única tendrán una validez de hasta 2 años contados a partir de la entrada en vigencia de la presente ley*".

Ahora bien, desde esta Entidad se considera conveniente suprimir los artículos 10, 11, 12, 13, 14, 16, 17, 18, 26, 28, 29, 48, 54, 55, 61, 66, 70, 71, 72, 73,78, 80, 81, 82, 83, 84, 85, 86, 87, 88 y 89, para garantizar la naturaleza de una norma estatutaria; donde se aborda un marco general y no especifico. Por cuanto la mayoría de los asuntos referidos en estas disposiciones se pueden desarrollar por vía reglamentaria.

Por otro lado, frente a los artículos 1, 8, 15, 25, 27, 30, 31, 32, 33, 34, 39, 40, 42, 43, 45, 46, 50, 56, 57, 62, 64, 68, 74, 75, 76, 77, 79, 90 y 93, no se advierte la necesidad de proponer modificaciones sustanciales, por lo tanto, en esta ocasión no se harán comentarios sobre ellos, sin perjuicio de observaciones futuras en aras de logar una mayor armonía y coherencia en el proyecto objeto de comentarios.

De esta forma esperamos haber contribuido al enriquecimiento de tan importante iniciativa, quedando a disposición para resolver cualquier inquietud que se presente sobre el particular.

Cordialmente,

CIELO RUSINQUE URREGO
SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

Elaboró: Alejandro Londoño
Revisó: Grenfieth Sierra /Héctor Barragán /Aurora Wberth /Gabriel Turbay
Aprobó: María Isabel Salazar Rojas

Etiquetado:	Externo

certicámara.

Bogotá D.C., 8 de febrero de 2024.

Honorables representantes:

Duvalier Sánchez Arango
Juan Carlos Wills Ospina
Adriana Carolina Arbeláez Giraldo
Carlos Felipe Quintero Ovalle
Hernán Darío Cadavid Márquez
Astrid Sánchez Montes De Oca
Diógenes Quintero Amaya
Jorge Alejandro Ocampo Giraldo
Luis Alberto Albán Urbano
Marelen Castillo Torres

Ref.: Observaciones al Proyecto de Ley 156 de 2023C "Por la cual se dictan disposiciones para el Régimen General de Protección de Datos Personales"

Respetados representantes,

Reciban un cordial y respetuoso saludo de la **SOCIEDAD CAMERAL DE CERTIFICACIÓN DIGITAL CERTICÁMARA S.A.**

La Cámara de Comercio de Bogotá, en asocio con las Cámaras de Comercio de Medellín para Antioquia, Cali, Bucaramanga, Cúcuta, Aburrá Sur, y la Confederación de Cámaras de Comercio (Confecámaras), crearon la Sociedad Cameral de Certificación Digital Certicámara S.A., Entidad de Certificación Digital Abierta, constituida en el año 2001 con el propósito de asegurar jurídica y técnicamente las transacciones, comunicaciones, aplicaciones, y en general, cualquier proceso de administración de información digital, de conformidad con los presupuestos establecidos en la Ley 527 de 1999 y los estándares técnicos internacionales de rigor en la materia.

Mediante esta comunicación, la compañía respetuosamente remite las observaciones al proyecto de ley referenciado en el asunto, de acuerdo con los siguientes términos:

Etiquetado:	Externo

certicámara.

Art.	Texto del proyecto	Comentarios	Propuesta
4.	**Artículo 4. Datos de personas fallecidas.** 1. Los causahabientes podrán dirigirse al responsable o encargado del tratamiento con el objeto de solicitar el acceso a los datos personales de la persona fallecida y, en su caso, su rectificación o supresión. 2. Las personas o instituciones a las que la persona fallecida hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de éste y, en su caso su rectificación o supresión. La Superintendencia de Industria y Comercio en conjunto con la Registraduría del Estado Civil, señalarán los requisitos y condiciones para acreditar la validez y	Se solicita de forma atenta, que se aclare cuáles son los elementos que los responsables o encargados deberán validar para determinar que un causahabiente cuenta con la legitimidad para ejercer el derecho de rectificación o supresión de datos de una persona fallecida. Adicionalmente, es necesario establecer de qué manera debe proceder el responsable o encargado del tratamiento de los datos personales de una persona fallecida, cuando la misma tenga múltiples causahabientes y no exista unanimidad entre los mismos sobre el ejercicio del derecho de rectificación o supresión de datos de una persona fallecida.	

	vigencia de estas autorizaciones. 3. En caso de fallecimiento de niños, niñas y adolescentes, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Instituto Colombiano de Bienestar Familiar o quien haga sus veces, que podrá actuar de oficio o a instancia de cualquier persona natural o jurídica interesada. 4. En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de quienes ejercen como representantes legales, o por la Defensoría del Pueblo, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo		

	prestadas por el designado. **Parágrafo primero.** Las personas a las que se refiere en numeral 1 del presente artículo, no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los causahabientes a acceder a los datos de carácter patrimonial del causante. **Parágrafo segundo.** La autorización expresa de que trata el numeral segundo podrá realizarse de conformidad con lo establecido en la ley 1996 de 2019 en relación con las directivas anticipadas, o a través de cualquier otro acto por medio cual se exprese dicha autorización.		

certicámara.

5.3	3.«Base de datos de riesgo crediticio»: para todos los efectos de la presente ley se entenderá por Base de Datos de Riesgo Crediticio aquella en la que se almacena y procesa datos personales de carácter financiero, crediticio, comercial y/o de servicios en cuanto al nacimiento, ejecución y extinción de obligaciones dinerarias se refiere; cuya finalidad será el tratamiento de dicha información para crear un perfil de los titulares y calcular su capacidad de endeudamiento y el riesgo crediticio que de ello se desprende, lo anterior bajo los parámetros y plazos de conservación contenidos en la Ley 2157 de 2021 o la que en su momento esté en vigencia.	Incluir dentro de la ámbito de aplicación de la norma, definiciones relacionadas con datos personales de carácter financiero, crediticio, comercial y/o de servicios, puede crear confusión o incluso contrariar lo dispuesto en la ley 1266 de 2008	Solicitamos que se elimine el punto 3 del artículo 5, bajo el entendido de que el ámbito de aplicación de la Ley 1581 que se está modificando, y la Ley 1266 de 2008, son diferentes.
5.6	6.«Cesión o comunicación de datos»: Tratamiento de datos que supone su revelación a una persona distinta del titular y/o encargado de tratamiento.	Es necesario hacer una distinción entre comunicación y cesión. Lo anterior, teniendo en cuenta que, las implicaciones de una cesión de datos personales es diferentes a la comunicación de los mismos, la definición	Que el artículo 5.6-Definiciones-«Cesión o comunicación de datos» se modifique en el siguiente sentido:

		consignada en este punto es atribuible a lo ya definido por la Superintendencia de industria y comercio como una transmisión de datos personales que implica la comunicación de los datos por parte de un responsable a un encargado, sin que el rol del responsable que transmite cambie.	6. **Transmisión de datos:** Tratamiento de datos que supone su revelación **por parte del responsable de los datos personales** a una persona distinta del titular **identificado como encargado de tratamiento**.
5.7-	7.«Consentimiento del titular»: toda manifestación de voluntad libre, consciente, específica espontánea, informada e inequívoca por la que el titular acepta de forma previa, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de los datos personales que le conciernen;	Es importante que el medio para la obtención de la autorización garantice que se tenga evidencia de autorización	Que el artículo 5.7- Definiciones, se modifique en el siguiente sentido: 1.«Consentimiento del titular»: toda manifestación de voluntad libre, consciente, específica espontánea, informada e inequívoca por la que el titular acepta de forma previa, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de los datos personales que le conciernen. **Sin perjuicio de lo anterior, quien lleve a cabo el tratamiento de los datos, garantizará y guardará evidencia**

			de la existencia de la autorización respectiva.
5.8-	8.«Datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona natural que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;	La Superintendencia de industria y Comercio ha definido los datos biométricos indicando que "**son datos sensibles** que permiten identificar a una persona natural a través del reconocimiento de una característica física **e intransferible**, que, al ser única de cada individuo, permite distinguir a un ser humano de otro." Adicionalmente, menciona que los datos biométricos son los relativos a la biometría definida en el diccionario de la real academia de la lengua así: "una tecnología de seguridad basada en el reconocimiento de una característica física e intransferible de las personas, como la huella digital, que [sic] al ser una característica única de cada individuo, permite distinguir a un ser humano de otro" En este sentido, consideramos que se debe incluir en la definición aspectos que ya han sido desarrollados por la Superintendencia de industria y comercio.	Que el artículo 5.8- Definiciones, se modifique en el siguiente sentido: "Datos biométricos: Son **datos sensibles** que permiten identificar a una persona natural a través de **una tecnología de seguridad basada en el** reconocimiento de una característica física e intransferible, que, al ser única de cada individuo, permite distinguir a un ser humano de otro, como imágenes faciales o datos dactiloscópicos."

certicámara.

5.14-	14.«Destinatario o tercero»: Persona natural o jurídica, pública o privada, al que se comuniquen datos personales, distinta del titular, responsable de tratamiento y encargado. No se considerarán destinatarios a las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el artículo 2, numeral 2, literal c) y e) de la presente ley;	La definición de destinatarios debe ser lo suficientemente clara como para determinar la calidad y responsabilidades que deben cumplir los mismos. Así mismo, sin perjuicio de la finalidad para la que se recibe la información, así se trate de autoridades públicas, las mismas tienen la obligación de no dar un uso a la información, que difiera de la finalidad para la cual la recibió.	Solicitamos amablemente se elimine toda mención a lo largo del proyecto de Ley, referente a un tercero o destinatario, bajo el entendido de que no se acopla a alguna ni tiene responsabilidades definidas como si es el caso de los titulares, responsables y encargados del tratamiento de los datos personales.
5.25	25. «Queja»: reclamación de interés particular dirigida a la autoridad de control que busca el amparo del derecho fundamental a la protección de los datos personales.	Durante el desarrollo del Proyecto de Ley los términos de queja, solicitud y reclamo son usados sin distinción, por lo que resulta importante que este proyecto normativo incluya las definiciones de cada uno de estos términos para que sean usados de manera correcta con la implementación de esta nueva Ley. Lo anterior, dado que, la diferenciación entre los mismos toma relevancia dentro de las obligaciones que tiene a su cargo el responsable, como lo es la actualización en el Registro Nacional de Bases de Datos.	Se sugiere se haga la distinción entre solicitud, queja, reclamo, ya que, al tratarse de agrupar los tres significados, los cuales tienen un alcance diferente, se genera confusión. Por lo tanto, con el fin de que se tenga una definición clara sobre estos términos, se incluyan los siguientes: Solicitud: Comunicación del titular del

certicámara.

			tratamiento de los datos personales al responsable y/o encargado del tratamiento de los datos cuya finalidad esté relacionada con la rectificación, actualización, supresión de sus datos personales. Reclamo: Comunicación del titular del tratamiento de los datos personales al responsable y/o encargado del tratamiento de los datos cuando el responsable y/o encargado no atendió adecuadamente la solicitud realizada por el titular previamente.
5.33	33.«Transferencia internacional de datos personales» Tratamiento que supone un flujo de datos en el que un responsable y/o encargado del tratamiento ubicado en el territorio nacional	No es posible acoger en una misma definición dos situaciones que tienen implicaciones diferentes como lo es la transferencia de responsable a responsable y la transmisión de responsable a encargado. Es necesario que se haga una distinción entre las	Sugerimos se adopte la definición de transferencia que contiene la Ley 1581 de 2012 y sus Decretos reglamentarios.

certicámara.

	envía datos personales a destinatarios y/o encargados ubicados fuera del territorio nacional u organizaciones internacionales.	transferencias totales y parciales, ya que en algunos casos el responsable identificado como cedente, tras el perfeccionamiento de la cesión conserva algunas obligaciones frente tratamiento de los datos personales, lo anterior atendiendo la diversidad y dinamismo del mundo de los negocios.	
10.	**Artículo 10. Condiciones para el tratamiento en la ejecución de un contrato.** 1. Se recolectarán los datos necesarios para la ejecución del contrato, todos aquellos datos que no se requieran para la existencia y ejecución del mismo, necesitarán de otra base legitimadora para su tratamiento. 2. El plazo de conservación de los datos estará determinado por la duración del contrato, salvo que, en cumplimiento de un deber legal el responsable esté	Resulta de gran importancia conocer el procedimiento que pretende implementar el Artículo 10. Condiciones para el tratamiento en la ejecución de un contrato en su numeral 4, el cual pretende implementar el procedimiento o solicitud de devolución de los datos personales al titular al finalizar una relación contractual, pues su redacción resulta confusa y de difícil aplicación en la práctica. Lo anterior, teniendo en cuenta que el ámbito de aplicación de la ley son los datos de carácter personal, no los datos en general, de estos últimos deberán encargarse las partes al momento de establecer las reglas o condiciones de confidencialidad de la información compartida entre las mismas.	Sugerimos se adopte la siguiente redacción: Una vez terminada la relación contractual por cualquier causa, incluida la nulidad, los datos de carácter personal podrán ser eliminados por parte del responsable a solicitud del titular de los datos dentro de los 30 días siguientes a la terminación del contrato o luego de la sentencia ejecutoriada que declara la nulidad. Con posterioridad a los 30 días de la terminación del contrato, los datos podrán ser suprimidos por el responsable. No

	obligado a exceder ese plazo. 3. La contratación que se lleve a cabo por entidades públicas, también le serán aplicables los principios y demás obligaciones establecidas en la presente ley. 4. Una vez terminada la relación contractual por cualquier causa, incluida la nulidad, los datos de carácter personal se devolverán al titular, si éste los solicita dentro de los 30 días siguientes a la terminación del contrato o luego de la sentencia ejecutoriada que declara la nulidad. Con posterioridad a los 30 días, los datos podrán ser suprimidos por el responsable. No procederá la supresión de los datos cuando exista una disposición legal que exija su conservación, en cuyo caso, deberá procederse a la devolución de los mismos garantizando el responsable del		procederá la supresión de los datos cuando exista una disposición legal que exija su conservación.

certicámara.

	tratamiento dicha conservación. 5. El responsable del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación contractual con el titular, excepto para la puesta a disposición por orden judicial, o por orden de la fiscalía general de la nación, o por la Superintendencia de Industria y Comercio, y cuando proceda, la Superintendencia Financiera de Colombia.		
14.	**Artículo 14. Condiciones para el tratamiento necesario para la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero.** 1. Una vez se haya examinado que el tratamiento no puede ser realizado en el supuesto de otra base legitimadora, el responsable podrá basar	Solicitamos amablemente se aclare si para el tratamiento necesario al que hace referencia el artículo 14, es requisito que se cumplan la totalidad de condiciones generales y específicas mencionadas en el mismo artículo, o si por el contrario, con la verificación de solo una de las condiciones el responsable podrá basar el tratamiento de los datos personales en el interés legítimo.	

	el tratamiento de datos personales en el interés legítimo siempre que se verifiquen las siguientes condiciones generales y específicas para dicho tratamiento: a) Debe representar un interés real y actual, es decir, no debe ser especulativo. b) Debe existir una relación pertinente y apropiada entre el titular y el responsable, como en situaciones en las que el titular es cliente o está al servicio del responsable. c) No es aplicable al tratamiento realizado por las entidades públicas en ejercicio de sus funciones. d) No puede ser invocado cuando se traten datos sensibles. e) Cuando se trate de una transferencia internacional basándose en un interés legítimo imperioso, debe cumplir con los requisitos		

	establecidos en el artículo 67 de la presente ley. 2. Dependiendo del estado de la técnica, recursos a disposición y las circunstancias del tratamiento, el interés legítimo puede convertirse en una de las bases legitimadoras mencionadas en el artículo 7, y se tomará aquella como preferente. 3. El interés legítimo siempre debe estar acompañado de un examen de ponderación, excepto cuando: a) Se realiza tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales. b) El tratamiento está relacionado con la realización de determinadas operaciones mercantiles de conformidad con el artículo 87 de la presente Ley.		

	c) El tratamiento es necesario para la prevención del fraude. d) Se transmiten datos personales dentro de un grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados. 4. El examen que se menciona en el numeral 3 del presente artículo, es una evaluación que se compone de tres diferentes fases preclusivas. El mismo tiene como objeto comprobar si el tratamiento es lícito y este examen, debe quedar documentado, en cumplimiento del principio de responsabilidad demostrada "Accountability" y, de una forma clara y transparente, en virtud del principio de transparencia, dicho examen debe partir con la descripción del		

	tratamiento. Las fases que componen el examen de interés legítimo son las siguientes: a) Test de finalidad (" satisfacción de intereses legítimos del responsable"): teniendo en cuenta la finalidad o el propósito específico del tratamiento analizado, debe identificarse cuál es el beneficio concreto sobre el que se sustenta dicho tratamiento; b) Test de necesidad ("¿es necesario el tratamiento?"): resulta imprescindible analizar si dicho tratamiento es necesario y proporcional para la consecución de los objetivos propuestos o si por el contrario concurren otras alternativas para satisfacer esos intereses; c) Test de equilibrio ("que sobre dichos		

certicámara.

	intereses no prevalezcan los intereses o los derechos y garantías fundamentales del titular"): si resultara que no existe otra alternativa o esta exigiera esfuerzos desproporcionados, procede realizar la prueba de sopesamiento. Dicha prueba consiste en analizar el impacto y/o el daño o perjuicio potencial del concreto tratamiento en los derechos y garantías de los titulares, para lo cual se tendrá en cuenta: i) Origen de los datos; ii) Categoría de los datos; iii) Si existe o no una relación previa con el titular; iv) Expectativa; v) Si afecta los intereses, derechos y garantías del titular; vi) Agentes implicados en el tratamiento; vii) Garantías adicionales para limitar su impacto en los derechos y		

certicámara.

	garantías fundamentales. 5. El tratamiento puede basarse en un interés legítimo cuando el test de equilibrio sea a favor del responsable.		
20.	3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al titular, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente en virtud del numeral 2. 4. Las disposiciones de los numerales 1, 2 y 3 no serán aplicables en la medida en que el titular ya disponga de la información y exista prueba de ello.	En cuanto al numeral 3 del artículo 20, no es claro el procedimiento que se debe surtir en aquellos casos en los cuales los datos personales son tratados para finalidades diferentes a las autorizadas. Toda vez que de la redacción del artículo se podría interpretar que basta con informar al titular y no es necesario solicitar la autorización del mismo.	
27.	**Artículo 27. Derecho de supresión («el derecho al olvido»).**	En Colombia, la "supresión de datos" y el "derecho al olvido" están relacionados con la protección de datos	

	1. El titular tendrá derecho a obtener del responsable del tratamiento la supresión de los datos personales que le concierne, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las siguientes circunstancias: a) Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; b) El titular retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 7, numeral 1, literal a), o el artículo 15, numeral 2, literal a), y este no se fundamente en otra base legitimadora; c) El titular se oponga al tratamiento con arreglo al artículo 33, numeral 1 y 2, y no prevalezcan otros motivos legítimos.	personales, pero tienen enfoques ligeramente diferentes. La supresión de datos se refiere a la eliminación de datos personales de las bases de datos, mientras que el derecho al olvido se relaciona más con el control sobre la visibilidad continua de la información personal en entornos en línea.	

certicámara.

	d) Los datos personales hayan sido tratados ilícitamente; e) Los datos personales deban suprimirse para el cumplimiento de una obligación legal que se aplique al responsable del tratamiento; f) Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información a menores de edad mencionados en el artículo 9, numeral 3. g) La Autoridad de Control Competente determine que en el tratamiento ha incurrido en conductas contrarias a la Constitución o esta ley y las demás normas que la modifiquen o adicionen. 2. Cuando haya cedido los datos personales y esté obligado, en virtud de lo dispuesto en el numeral 1, a suprimir dichos datos, el responsable del tratamiento teniendo en cuenta la tecnología		

certicámara.

	disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los destinatarios o terceros que estén tratando los datos personales de la solicitud del titular de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos. 3. Los numerales 1 y 2 no se aplicarán cuando el tratamiento sea necesario: a) Para ejercer el derecho a la libertad de expresión e información; b) Para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por la ley que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;		

certicámara.

	c) Por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 15, numeral 2, literales h) e i), y numeral 3; d) Con fines de archivo en interés público, investigación científica, o estadística, de conformidad con el artículo 85, numeral 1, en la medida en que el derecho de supresión pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o; e) Para la formulación, el ejercicio o la defensa de reclamaciones administrativas o judiciales.		
32.2	2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el numeral 1, el titular tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.	La naturaleza jurídica de la transmisión no es la del tratamiento que se relaciona en este numeral.	2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el numeral 1, el titular tendrá derecho a que los datos personales se **transfieran** directamente de responsable a

certicámara.

			responsable cuando sea técnicamente posible.
35.	**Artículo 35. Derecho a presentar una queja ante la Autoridad de Control.** 1. Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo titular que considere que su derecho fundamental a la protección de datos ha sido vulnerado por infracción a la presente ley tendrá derecho a presentar una queja ante la autoridad de control competente. 2. La queja se formulará mediante solicitud dirigida a la Autoridad de Control y deberá contener, por lo menos: a) La identificación del titular y/o su representante legal junto con los documentos que acrediten tal calidad; b) El objeto de la queja, es decir, lo	Teniendo en cuenta las sugerencias elevadas en cuanto a lo contemplado en el artículo 5 de la presente ley consideramos que se deben hacer ajustes en la terminología empleada en la redacción del presente artículo.	**Artículo 35. Derecho a presentar una queja ante la Autoridad de Control.** 1. Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo titular que considere que su derecho fundamental a la protección de datos ha sido vulnerado por infracción a la presente ley tendrá derecho a presentar una queja ante la autoridad de control competente. 2. La queja se formulará mediante solicitud dirigida a la Autoridad de Control y deberá contener, por lo menos: a) La identificación del titular y/o su representante legal junto con los documentos que acrediten tal calidad; b) El objeto de la queja, es decir, lo

certicámara.

	que se persigue con ella; c) La descripción clara de los hechos que fundamentan el reclamo; d) La dirección de notificación; e) Los documentos que soporten la acreditación del requisito de procedibilidad establecido en el numeral 3 del presente artículo, y; f) Los demás documentos que se quiera hacer valer en el trámite administrativo. 3. El titular o quien represente sus intereses solo podrá elevar queja ante la Autoridad de Control una vez que haya agotado el requisito de procedibilidad, esto es, la presentación de una solicitud previa, con ejercicio de derechos, ante el responsable o el encargado según sea el		que se persigue con ella; c) La descripción clara de los hechos que fundamentan el reclamo; d) La dirección de notificación; e) Los documentos que soporten la acreditación del requisito de procedibilidad establecido en el numeral 3 del presente artículo, y; f) Los demás documentos que se quiera hacer valer en el trámite administrativo. 3. El titular o quien represente sus intereses solo podrá elevar queja ante la Autoridad de Control una vez que haya agotado el requisito de procedibilidad, esto es, la presentación de **un reclamo previo**, con ejercicio de derechos, ante el responsable o el encargado según sea el caso siempre que, habiendo

	caso siempre que, habiendo transcurrido el término establecido en esta ley para la solución del reclamo previo, el sujeto obligado no se hubiese pronunciado o, de existir respuesta, esta no satisfaga los intereses del titular de la información. 4. La Autoridad de Control tendrá la obligación de examinar integralmente la petición, y en ningún caso, podrá estimarla como incompleta por falta de requisitos o documentos que no se encuentren dentro del marco jurídico vigente, que no sean necesarios para resolverla o que se encuentren dentro de sus archivos. Si el reclamo resulta incompleto, se requerirá al titular dentro de los diez (10) días siguientes a la fecha de radicación de la queja para que la complete, otorgándole al solicitante el término de un (1) mes para ello. Transcurrido el término		transcurrido el término establecido en esta ley para la solución del reclamo previo, el sujeto obligado no se hubiese pronunciado o, de no existir respuesta, esta no satisfaga los intereses del titular de la información. 4. La Autoridad de Control tendrá la obligación de examinar integralmente la **queja**, y en ningún caso, podrá estimarla como incompleta por falta de requisitos o documentos que no se encuentren dentro del marco jurídico vigente, que no sean necesarios para resolverla o que se encuentren dentro de sus archivos. Si **la queja** resulta incompleto, se requerirá al titular dentro de los diez (10) días siguientes a la fecha de radicación de la queja para que la complete, otorgándole al

certicámara.

	de un (1) mes desde la fecha del requerimiento sin que el solicitante presente la información requerida, se entenderá que ha desistido de su queja, salvo que antes del vencimiento de dicho plazo éste solicite prórroga hasta por un término igual. 5. La autoridad de control ante la que se haya presentado la queja informará a solicitud del reclamante sobre el curso del trámite administrativo y en cualquier caso sobre las etapas que la normativa procesal así determine como obligatorias.		solicitante el término de un (1) mes para ello. Transcurrido el término de un (1) mes desde la fecha **de la presentación de la queja** sin que el solicitante presente la información requerida, se entenderá que ha desistido de su queja, salvo que antes del vencimiento de dicho plazo éste solicite prórroga hasta por un término igual. 5. La autoridad de control ante la que se haya presentado la queja informará a solicitud del titular o **de la persona que represente sus intereses** sobre el curso del trámite administrativo y en cualquier caso sobre las etapas que la normativa procesal así determine como obligatorias.
37.4	4. El responsable del tratamiento deberá actualizar la información, comunicando de forma oportuna al encargado	Respecto al numeral 4, consideramos oportuno aclarar, ¿qué se debe entender por novedad?.	

certicámara.

	del tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas técnicas y organizativas apropiadas para que la información suministrada a este, se mantenga actualizada.	En caso de que se refiera a incidentes, es ideal que el responsable tenga la oportunidad de realizar la investigación pertinente, en un tiempo definido e informar el detalle de lo sucedido con los hechos y datos investigados.	
40.	**Artículo 40. Representantes de responsables o encargados del tratamiento con domicilio fuera del territorio Nacional.** 1. Cuando sea de aplicación el artículo 3 numeral 2, el responsable o el encargado del tratamiento designará por escrito un representante legal y/o sucursal en Colombia. 2. La obligación establecida en el numeral 1 del presente artículo no será aplicable: a) Al tratamiento de datos que sea ocasional, que no incluyan el manejo a gran escala de	Solicitamos se aclare en el texto, ¿cuál es el alcance, las calidades y facultades que deberán tener los representantes de responsables o encargados del tratamiento con domicilio fuera del territorio Nacional?	

	categorías especiales de datos indicadas en el artículo 15 numeral 1, o de datos personales relativos a delitos y condenas penales a que se refiere el artículo 16, y que sea improbable que entrañe un riesgo para los derechos y garantías de las personas naturales, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento, o; b) A las autoridades u organismos públicos. 3. El responsable o el encargado del tratamiento encomendará al representante las facultades necesarias a fin de garantizar el cumplimiento de lo dispuesto en la presente ley. 4. La designación de un representante por el responsable o el encargado del tratamiento se entenderá sin perjuicio de las acciones que pudieran emprenderse		

certicámara.

	contra el propio responsable o encargado.		
41.1	1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable, éste elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos de la presente ley y garantice la protección de los derechos del titular.	Respecto al numeral 1, sugerimos eliminar la palabra "únicamente." A nuestro juicio esta norma desconoce que puede existir multiplicidad de tratamientos para los cuales se requieran diferentes encargados con el fin de garantizar la protección de los derechos de los titulares de la información. Agradecemos tener en cuenta que la norma impone una restricción innecesaria e injustificada.	1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable, éste elegirá **a** un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos de la presente ley y garantice la protección de los derechos del titular.
49.	**Artículo 49. Notificación de un Incidente de seguridad de los datos personales a la autoridad de control.** 1. En caso de Incidente de seguridad de los datos personales, el responsable del tratamiento lo notificará a la Superintendencia de	Se sugiere modificar el término para la notificación de incidentes de seguridad de los datos personales. Se recomienda mantener el estándar actual. El proyecto de ley eleva el estándar de forma desproporcionada, pasando de 15 días hábiles en la actualidad a 72 horas. Esto representa grandes retos e impactos para	

	Industria y Comercio de conformidad con el artículo 73 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicho Incidente de seguridad constituya un riesgo para los derechos y las garantías de las personas naturales. Si la notificación a la Superintendencia de Industria y Comercio no tiene lugar en el plazo de 72 horas, deberá ir acompañada de los motivos que expliquen la dilación. 2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento los incidentes de seguridad de los datos personales de las que tenga conocimiento. 3. La notificación contemplada en el numeral 1 deberá, como mínimo:	las empresas, particularmente las pequeñas y medianas que no tienen las capacidad administrativas ni operativas para afrontar este tipo de situaciones de manera ágil y eficiente, nuevamente destacamos la importancia de valorar este tipo de impactos. Sumado a lo anterior, es importante considerar que se requiere de 72 horas para la contención, erradicación e investigación del incidente de seguridad. Por lo cual, notificar a las 72 horas podría dar lugar a imprecisiones en la información entregada, o a la generación de alertas innecesarias, se sugiere ampliar el término.	

certicámara.

	a) Describir la naturaleza de la Incidente de seguridad de los datos personales y, cuando sea posible, el número aproximado y tipo de titulares afectados, las categorías de datos y el número aproximado de registros de datos personales afectados; b) Comunicar el nombre y los datos de contacto del oficial de protección de datos o de otro punto de contacto en el que pueda obtenerse más información; c) Describir las posibles consecuencias del Incidente de seguridad de los datos personales; d) Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio al Incidente de seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos. 4. Si no fuera posible facilitar la información		

	descrita en el numeral 3 del presente artículo simultáneamente con la notificación de un incidente de seguridad, y en la medida que esta condición persista, la información se facilitará de manera gradual sin dilación indebida. 5. El responsable del tratamiento documentará cualquier Incidente de seguridad de los datos personales, incluidos los hechos relacionados con este, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo. 6. Los datos personales contenidos en la notificación de una Incidente de seguridad y que fueron comunicados a la Superintendencia de Industria y Comercio, proveedores de tecnologías y servicios de seguridad, podrán ser tratados exclusivamente		

certicámara.

	durante el tiempo y alcance necesario para su análisis, detección protección y respuesta ante el incidente y adoptando medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado		
50.	**Artículo 50. Comunicación de un Incidente de seguridad de los datos personales al titular.** 1. Cuando sea probable que el Incidente de seguridad de los datos personales entrañe un alto riesgo para los derechos y garantías de las personas naturales, el responsable del tratamiento lo comunicará al titular sin dilación indebida. 2. La comunicación al titular contemplada en el numeral 1 del presente artículo deberá describir en un lenguaje claro y sencillo la naturaleza del Incidente de seguridad de los datos personales y contendrá como mínimo la información y las	Solicitamos se aclare qué factores determinan que un incidente de seguridad constituya un alto riesgo para los derechos y garantías de los titulares. Lo anterior, teniendo en cuenta que en la práctica, no tiene utilidad informar todo tipo de incidentes al titular de los datos, por el contrario, esto podría generar pánico masivo, debido a que hay incidentes que no generan un perjuicio o afectación al titular.	

	medidas a que se refiere el artículo 49, numeral 3, literales b), c) y d). 3. La comunicación al titular a la que se refiere el numeral 1 no será necesaria si se cumple alguna de las condiciones siguientes: a) El responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por el Incidente de seguridad, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado; b) El responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y garantías del titular a que se refiere el numeral 1;		

certicámara.

	4. Cuando la comunicación a los titulares suponga un esfuerzo desproporcionado para el responsable del tratamiento, éste podrá optar por una comunicación pública o una medida de difusión semejante por la que se informe de manera igualmente efectiva a los titulares. 5. Cuando el responsable no haya comunicado al titular el Incidente de seguridad de los datos personales, la Superintendencia de Industria y Comercio, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo comunique o podrá confirmar que se cumple alguna de las condiciones mencionadas en el numeral 3.		
52	**Artículo 52. Consulta previa.**	Solicitamos amablemente, indicar ¿cuáles son los criterios con base en los cuales se determine el “alto riesgo” en la	

	1. El responsable del tratamiento consultará ante la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio antes de llevar a cabo un tratamiento cuando, de la evaluación de impacto de que trata del artículo 51, se concluya que dicho tratamiento supondría un alto riesgo para los derechos y garantías de los titulares. 2. Cuando la Delegatura para la Protección de Datos Personales considere que el tratamiento previsto en el numeral 1 suponga un alto riesgo para los derechos y garantías de los titulares, asesorará por escrito al responsable, y en su caso al encargado, entre otras cosas respecto de las medidas técnicas y organizativas que se deberán adoptar previo al tratamiento de los datos. La Delegatura para la Protección de Datos	garantía de los derechos de los titulares.	

	Personales deberá, en un plazo de 3 meses contados a partir de la fecha en que el responsable, o en su caso el encargado, acude ante ella, emitir un concepto. Este plazo podrá prorrogarse, en función de la complejidad del tratamiento, por única vez, por un periodo igual a la inicial, informando al responsable y, en su caso, al encargado del tratamiento de tal prórroga, indicando los motivos de la dilación. 3. El escrito que el responsable del tratamiento allegue a la Superintendencia de Industria y Comercio deberá contener como mínimo la siguiente información: a) En caso de ser procedente, las responsabilidades respectivas del responsable, y los encargados implicados en el tratamiento, en particular en caso de		

certicámara.

	tratamiento dentro de un grupo empresarial; b) Los fines y medios del tratamiento previsto; c) Las medidas establecidas para proteger los derechos y garantías de los titulares de conformidad con la presente Ley; d) En su caso, los datos de contacto del oficial de protección de datos; e) La evaluación de impacto relativa a la protección de datos establecida en el artículo 51 de esta ley; f) Cualquier otra información que solicite la autoridad nacional de protección de datos. Parágrafo: Cuando la Superintendencia de Industria y Comercio deba requerir información y/o documentación adicional, los términos establecidos en el numeral 2 del presente artículo se suspenderán hasta que la información		

certicámara.

	y/o documentación se haya obtenido o hasta que el plazo otorgado para suministrarlos, se haya cumplido.		
103	**Artículo 103. Plazos para la implantación de las medidas de seguridad.** La implantación de las medidas de seguridad previstas en la presente ley deberá producirse con arreglo a las siguientes reglas: 1. Respecto de las bases de datos que existieran al momento de la entrada en vigencia de la presente ley se llevara a cabo de la siguiente manera: a) En el plazo máximo de dieciocho meses desde su entrada en vigencia, deberán implantarse las medidas de seguridad en bases de datos automatizadas. b) Respecto de las bases de datos no automatizadas que existieran al momento de la entrada en vigencia de la presente ley, en el plazo máximo de un año. 2. Las bases de datos, tanto automatizadas	Al ser un Proyecto de Ley que generará gran impacto en las empresas que manejan datos personales como encargados o responsables y en la ciudadanía en general. Consideramos importante que se establezcan rangos de cumplimiento en virtud del número de titulares que se manejen en cada empresa, se tenga un régimen de transición de mayor o menor término según sea el caso. Pues, resultan muy cortos los siguientes términos: • Consentimiento: solo será válido el consentimiento de los titulares recabados con anterioridad a la expedición de esta ley un **año posterior a la entrada en vigencia**, plazo en cuál el responsable del tratamiento deberá obtenerlos en las condiciones previstas en la presente ley o legitimar el tratamiento en otra base jurídica.	

	como no automatizadas, creadas con posterioridad a la fecha de entrada en vigencia de la presente ley deberán tener implantadas, desde el momento de su creación la totalidad de las medidas de seguridad reguladas en esta ley.
	Parágrafo: A requerimiento de la Superintendencia de Industria y Comercio el responsable de Tratamiento deberá demostrar que está llevando a cabo la implementación de las medidas de seguridad en las bases de datos existentes en el momento de la entrada en vigencia de la presente ley.
		• Bases de datos: existieran al momento de la entrada en vigencia de la presente ley se llevará a cabo de la siguiente manera;
		  • En el plazo **máximo de dieciocho meses desde su entrada en vigencia**, deberán implantarse las medidas de seguridad en base de datos automatizadas.
		  • Respectos de las bases de datos no automatizadas que existieran al momento de la entrada en vigencia de la presente ley, en el **plazo máximo de un año**.
		• Los contratos de encargado del tratamiento suscritos con anterioridad a esta ley serán válidos hasta **dieciocho meses después** de su entrada en vigencia. Durante dicho plazo cualquiera de las partes podrá exigir	

certicámara.

		a la otra modificación del contrato. Si bien, consideramos que los datos personales de los ciudadanos colombianos tienen que ser tratados de la mejor manera y bajo la urgencia correspondiente. Estos términos resultarán más difíciles para empresas que administran alto volumen de datos personales, por lo que sugerimos se evalúe términos distintos según el tamaño de la empresa el régimen de transición y se pueda dar un cumplimiento real y efectivo de las disposiciones que contiene este Proyecto de Ley. Lo anterior, contribuirá al correcto tratamiento de datos personales por parte de las empresas que son responsables o encargados de los datos de los ciudadanos, pues incluye la perspectiva de empresas que propenden por el buen manejo de datos personales.	

Agradecemos su atención a las observaciones anteriormente presentadas.

Cordialmente,

CERTICÁMARA S.A.

Etiquetado:	Externo

certicámara.

Carrera 7 No. 26 - 20 Piso 18 / Edificio Seguros Tequendama
www.certicamara.com
Ventas, servicio al cliente y soporte: (601) 744 2727
Línea administrativa: (601) 745 2141

H.R. Duvalier Sanchez Arango
Comisión Primera
Cámara de Representantes

Ref: Observaciones Audiencia Pública Proyecto de Ley 156/2023 Cámara "Por la cual se dictan disposiciones para el Régimen General de Protección de Datos Personales"

Cordial saludo,

En atención a la Audiencia Pública para la discusión del Proyecto de Ley 156/2023 Cámara "Por la cual se dictan disposiciones para el Régimen General de Protección de Datos Personales", Emmanuel Vargas Penagos, codirector de la organización El Veinte, envía las observaciones sobre las cuáles desarrollará su intervención. Puntualmente, se centrará en los artículos relativos al "derecho de rectificación" y "derecho de supresión (derecho al olvido)" y sus implicaciones para la libertad de expresión y el acceso a la información.

A finales de 2023 las organizaciones de la sociedad civil Karisma, Derechos Digitales, AccessNow, Fundación para la Libertad de Prensa y El Veinte, enviaron una carta a los representantes ponentes con el fin de señalar algunas anotaciones en relación con el proceso de redacción del proyecto de ley, así como algunas claves para la garantía de los derechos humanos en la esfera de la protección de datos. La carta no es aún visible en el micrositio de la Cámara de Representantes (cuando las intervenciones de otras organizaciones y gremios sí lo son), por tanto se anexa al final del presente escrito.

Para El Veinte los procesos de formulación de regulación en materia de protección de datos personales deben comprender tanto una participación comprensiva y plural de múltiples sectores de la sociedad, incluyendo a las organizaciones de la sociedad civil, como una cuidadosa revisión del respeto y garantía por los derechos fundamentales, como el derecho a la privacidad, a la intimidad, a la libertad de expresión y de prensa y al acceso a la información. Las normas relacionadas con los desarrollos tecnológicos que contempla el Proyecto de Ley no deben perder de vista la observancia por los derechos humanos que, incluso con anterioridad, se ha consagrado en el ordenamiento jurídico colombiano.

A partir de estas consideraciones y de los comentarios anexos enviados en la comunicación conjunta, se desarrollará la intervención del suscrito y en particular, como se mencionó, en relación con las implicaciones para la libertad de expresión y el acceso a la información.
En todo caso, de requerirse información adicional o al finalizar la Audiencia Pública y una vez reunidas las intervenciones registradas podrán allegarse las comunicaciones y comentarios adicionales correspondientes.

Agradezco su atención y el espacio de participación abierta para la ciudadanía.

Emmanuel Vargas
direccion@elveinte.org
Codirector, El Veinte

Anexo: Carta PL Habeas Data

Bogotá, noviembre de 2023

H.R. Duvalier Sanchez Arango
H.R. Juan Carlos Wills Ospina
H.R. Adriana Carolina Arbeláez Giraldo
H.R. Carlos Felipe Quintero Ovalle
H.R. Hernán Darío Cadavid Márquez
H.R. Astrid Sánchez Montes De Oca
H.R. Diógenes Quintero Amaya
H.R. Jorge Alejandro Ocampo Giraldo
H.R. Luis Alberto Albán Urbano
H.R. Marelen Castillo Torres

Ref: Proyecto de Ley 156/2023 Cámara "Por la cual se dictan disposiciones para el Régimen General de Protección de Datos Personales"

Asunto: Comentarios de organizaciones de la sociedad civil en relación con el proyecto citado.

Honorables representantes ponentes,

Las organizaciones de la sociedad civil abajo firmantes hemos revisado con detenimiento el proyecto de Ley Estatutaria radicado el pasado 22 de agosto en la Cámara de Representantes y, como organizaciones que tenemos, entre otras, la misión de velar por la protección de los derechos humanos en la esfera digital, queremos manifestar las siguientes preocupaciones generales sobre el proceso de su elaboración:

1. **El proyecto debería haber sido construido de cero con la participación de las múltiples partes interesadas: academia, industrias, sociedad civil, autoridades de control, entre otros.**

Estamos de acuerdo con que urge adaptar el marco de protección de datos colombiano con los estándares interamericanos y las mejores prácticas reconocidas en la materia. Su actualización debería **armonizar el disperso marco normativo existente, así como integrarse con las reglas jurisprudenciales en materia constitucional.**

Para ello, creemos que la participación ciudadana en la redacción del proyecto es esencial para reflejar las preocupaciones e intereses de múltiples partes, así como para que el proyecto pueda reflejar y responder a las necesidades sociojurídicas del contexto colombiano. **La redacción actual del proyecto no refleja las necesidades, intereses, ni estado del arte de la última década sobre buenas prácticas, jurisprudencia y regulación dispersa sobre protección de datos en el país**. Y aunque en el apartado sobre el fundamento normativo que hace parte de la exposición de motivos del proyecto se recoge algo de la gran dispersión normativa y del desarrollo jurisprudencial posterior a la promulgación de la Ley 1581 de 2012, dicha revisión desconoce una parte importante de los demás temas relacionados con el habeas data como normas y fallos que han introducido una complejidad sustancial a este asunto.

Para solucionar esto, proponemos que el proceso de elaboración de esta iniciativa suceda en espacios de participación –presencial o virtual–, que permitan **abrir la discusión sobre** (i) el enfoque del nuevo marco normativo que se busca, (ii) las reglas que deben actualizarse, (iii) aquellas nuevas que quieren introducirse, y (iv) aquellas que definitivamente hay que derogar.

La **más amplia participación en la construcción de un marco normativo**, especialmente uno relacionado con un derecho fundamental central para la vida en sociedad actual, es enfatizado por la OCDE[1] como un pilar del Estado de Derecho y de los principios de Gobierno Abierto que Colombia suscribe. Además, redunda positivamente en múltiples aspectos: **una menor resistencia a su trámite y votación, así como un mayor respaldo por las partes interesadas**. Invitamos a que, en este sentido, se examine y sigan los procesos de participación amplia que sucedieron en Argentina y Brasil a propósito de la elaboración de los proyectos de ley de protección de datos en cada uno.

Creemos que es fundamental que la **participación suceda desde la fase cero**, y no cuando ya ha sido decidido y redactado su contenido. Las audiencias públicas deben tener lugar precisamente para decidir los temas, estructura y contenido del proyecto de ley, y no para comentar en escasos cinco minutos nuestro parecer sobre su contenido. Invitamos a los ponentes, así como a los autores de la iniciativa, a no apurar este proceso en perjuicio de su calidad normativa; estamos a tiempo de corregir el rumbo.

2. **La redacción del proyecto de ley de protección de datos debe integrarse de manera armónica y compatible con el ejercicio de otros derechos**

También nos genera preocupación que uno de los enfoques acogidos por la iniciativa, tal y como está redactada actualmente, sea el de **privilegiar de manera desproporcionada el ejercicio del derecho a la protección de datos por encima de otros derechos igualmente fundamentales**, como el derecho de acceso a la información y la libertad de expresión. De igual manera es indispensable garantizar que los estándares interamericanos que ya rigen esta materia sean atendidos. En concreto, múltiples artículos se oponen de manera directa a algunos de ellos y la interpretación que se ha hecho de ellos en la jurisprudencia constitucional.

Que se trate de una **norma estatutaria, que demanda el examen automático y único de parte de la Corte Constitucional, obliga a que la redacción, trámite y discusiones previas del contenido del proyecto sucedan de manera mucho más exhaustiva y meditada**. Para ello, la participación es esencial para que el proyecto resultante sea tal que refleje los más altos estándares y así pueda resistir y superar un análisis de constitucionalidad. Lo anterior también garantiza que no se requieran cambios o revisiones posteriores sobre un asunto que la Corte, tras su análisis, tomaría como cosa juzgada.

Por eso reiteramos la importancia de la participación ciudadana como un espacio útil para (i) identificar oportunidades de armonización legislativa también de cara al ejercicio de otros derechos, (ii) encontrar miradas alternativas que permitan compatibilizar la protección de datos de cara a los estándares interamericanos y aquellos otros fijados por la Corte Constitucional y (iii) para garantizar un texto que no pierda vigencia rápidamente.

---

[1] Alessandro Bellantoni, «Gobierno Abierto. Contexto mundial y el camino a seguir.» (OCDE, 2016), https://www.oecd.org/gov/Open-Government-Highlights-ESP.pdf.

De acuerdo con lo expuesto anteriormente, consideramos que el mejor curso de acción en este punto es **retirar el proyecto de manera que pueda llevarse a cabo un proceso amplio de consulta y participación respaldado por los distintos sectores**.

Agradecemos su atención y reiteramos nuestra apertura y disposición a la participación abierta y el diálogo

Un cordial saludo,

Fundación Karisma

Juan Diego Castañeda

juancastaneda@karisma.org.co

Fundación para la Libertad de Prensa

Jonathan Bock

director@flip.org.co

El Veinte

Emmanuel Vargas

direccion@elveinte.org

Derechos Digitales

Lucía Camacho

lucia.camacho@derechosdigitales.org

Access Now

Franco Giandana Gigena

franco@accessnow.org