ASOCIACIÓN LATINOAMERICANA DE INTERNET

Bogotá, 10 de noviembre de 2023

Honorable Representante
OSCAR HERNÁN SÁNCHEZ LEÓN
Presidente
Comisión Primera Constitucional Permanente
Cámara de Representantes
La ciudad

Asunto: Comentarios al Proyecto de Ley 156/2023 Cámara *"Por la cual se dictan disposiciones para el régimen general de protección de datos personales"*.

Respetado Presidente,

Le saludo en nombre de la Asociación Latinoamericana de Internet (ALAI), organización regional sin fines de lucro que trabaja por el desarrollo digital de América Latina, representando la perspectiva de la industria de Internet. ALAI promueve el desarrollo inclusivo de la economía digital mediante el fortalecimiento del Internet abierto y respalda políticas que favorezcan el respeto y ejercicio de los derechos humanos, el emprendimiento y la innovación.

Inspirados en el bienestar colectivo, la democracia participativa y la búsqueda del máximo desarrollo y beneficio social para los colombianos, nos dirigimos a Usted para expresar nuestras observaciones con respecto al proyecto de ley referido en el asunto y contribuir así en su proceso de formulación.

Estamos totalmente de acuerdo en la importancia de implementar soluciones integrales que salvaguarden la privacidad de los ciudadanos en los diversos entornos digitales. Asimismo, creemos que el uso responsable de los datos es crucial para impulsar la innovación y la productividad de las sociedades.

Con base en estas premisas, estamos firmemente convencidos de que los enfoques intermedios, que buscan objetivos de política como la protección de los datos al mismo tiempo que facilitan su uso innovador y su transferencia transfronteriza, constituyen el punto de partida óptimo para la formulación de políticas públicas adecuadas y efectivas sobre la privacidad en Internet.

Aunque, en términos generales, el proyecto de ley persigue fines bienintencionados, nuestras sugerencias buscan mejorar la iniciativa al evitar la imposición de cargas excesivas que desincentivan el desarrollo de la digitalización en Colombia, la cual, ha

contribuido al crecimiento acumulado del PIB en 6,12%, siendo el más alto de América Latina[1].

De igual modo, buscamos promover la adaptación de las normativas a las tecnologías actuales, sin perjudicar el flujo natural y progresivo de la innovación tecnológica, como tampoco la seguridad jurídica del ecosistema digital.

La iniciativa, tal como está planteada, aplica cargas desproporcionadas que exceden las obligaciones de los responsables del tratamiento de datos. Además, exige intervenciones humanas innecesarias, desconociendo el funcionamiento y aporte de tecnologías actuales como la Inteligencia Artificial (IA), generando altos costos en perjuicio de la economía digital, la competitividad y la productividad. Esta preocupación se vuelve especialmente relevante en el contexto colombiano, dado que la contribución de la productividad al crecimiento promedio del PIB se sitúa en un modesto 1.4% (32% del total)[2], lo cual, ha llevado a organizaciones como el *McKinsey Global Institute* a prever que, si no se mejora la productividad, la tasa de crecimiento promedio del PIB para Colombia entre 2015 y 2030 sería de 2.1%, cifra que marca una reducción del 50% en relación con la tasa de crecimiento promedio que el país experimentó entre 2000 y 2015.

Por otro lado, el proyecto de ley no establece de manera clara los requisitos y procedimientos de las denuncias de los usuarios ante las autoridades e ignora los sistemas actuales para el tratamiento de datos, imponiendo medidas técnicas que, de manera inmediata, implicaría costos excesivos a los responsables. Cargas similares se evidencian en el requisito de designar un representante legal o sucursal en Colombia para empresas extranjeras o en la reducción de 15 días hábiles a 72 horas, del plazo de notificación de incidentes de seguridad de datos personales.

A su vez, existen oportunidades de mejora en cuanto a la definición de algunos conceptos como el referente a los tratamientos de datos de "alto riesgo", con el fin de proteger la seguridad jurídica de los responsables del manejo de datos. La falta de claridad también se percibe en las reglas impuestas a los responsables que realizan el tratamiento de datos y no están domiciliados en Colombia.

Hacemos un llamado a la reflexión sobre los contenidos que pretenden limitar el desarrollo de la Inteligencia Artificial (IA) en Colombia, socavando el principio de neutralidad tecnológica y restringiendo el potencial económico de esta tecnología para el país. Vale la pena recordar que al 2030, se espera que el crecimiento económico mundial, proporcionado por la IA, sea de 15,7 billones de dólares[3]. Las oportunidades para

---

[1]Katz, Raul (2015) "El Ecosistema y la Economía Digital en América Latina en 2015". Comisión Económica para América Latina y el Caribe (CEPAL), CAF –banco de desarrollo de América Latina, Centro de Estudios de Telecomunicaciones de América Latina (cet.la), Fundación Telefónica realizaron.

[2] Rescatado de McKinsey Global Institute – MGI. (2017). Where will Latin America´s Growth Come From?

[3] Recuperado de "AI Index Report", Stanford University, 2022, https://aiindex.stanford.edu/wp-content/uploads/2022/03/2022-AI-Index-Report_Master.pdf

Colombia son inmejorables, teniendo en cuenta que el país es uno de los más preparado en la región para la adopción de este tipo de tecnologías emergentes, destacándose a nivel internacional por su Estrategia de IA y su visión en el desarrollo de un marco regulatorio, ético y de gobernanza de avanzada[4].

Además, invitamos a la prudencia al abordar temas que aún están en una etapa inicial de discusión a nivel global, como es el caso de los neuroderechos. Dado que este asunto se encuentra en una fase temprana de desarrollo, todavía no hay un consenso definitivo entre académicos, sociedad civil, gobiernos y tecnólogos sobre sus verdaderos alcances, lo cual, podría conducir a decisiones que, en lugar de proteger al consumidor, tengan impactos negativos en el acceso a neurotecnologías por parte de poblaciones vulnerables que podrían beneficiarse de los avances de las neurociencias.

Por último, instamos a la preservación de los principios constitucionales al designar las autoridades responsables de las decisiones en los casos de indemnización y responsabilidad. También solicitamos amablemente, avanzar de manera conjunta en una definición clara sobre quiénes serían los sujetos afectados por las multas calculadas como porcentaje de utilidades, ya que el proyecto de ley no especifica de manera precisa a quiénes se aplicaría este tipo de sanciones.

En vista de lo expresado, a continuación, detallamos nuestras observaciones frente a los artículos de interés, a fin de contribuir al proceso de formulación del proyecto de ley:

1. **Artículo 3. Ámbito territorial**

La propuesta contraría el principio de aplicación territorial de la ley. La Corte Constitucional ha determinado que la ley colombiana es mandatoria para todos **los residentes del país,** tanto nacionales como extranjeros. Asimismo, en sentencia C-249 de 2004, la Corte señaló que *"Con fundamento en el artículo 4 superior los nacionales y extranjeros deben someterse a la Constitución, a la ley y a las autoridades. Las leyes obligan a todos los habitantes del país, incluyendo a los extranjeros domiciliados o transeúntes, salvo lo previsto para éstos en tratados públicos" (subrayas fuera de texto).*

Este principio de territorialidad de la ley, se ampara además en el derecho internacional público, que establece que **la ley colombiana aplica a los nacionales y a los extranjeros que se encuentren en el territorio nacional** y constituye *"el fundamento esencial de la soberanía, conforme al cual cada Estado puede prescribir y aplicar normas dentro de su respectivo territorio, dado que este es su alcance espacial natural"*[5].

Por lo anterior, la norma de protección de datos personales debe aplicar a quienes tratan

[4] Recuperado de Oxford "Goverment AI Readiness Index" 2022.
[5] Corte Constitucional, sentencia C-1189 de 2000.

datos personales en el territorio nacional, ya sean nacionales o extranjeros. Cualquier otra aplicación sería contraria al principio de aplicación territorial de la ley constitucionalmente reconocido.

Por otro lado, se estima que el ámbito de aplicación extraterritorial propuesto para actividades de tratamiento de datos personales relacionados con la (i) la oferta de bienes o servicios a titulares en Colombia, y de (ii) el control de su comportamiento, resultan criterios supremamente indeterminados que generan inseguridad jurídica. Hoy en día, en un mundo globalizado, en el que es posible ofrecer servicios a cualquier parte del mundo, pretender que todos aquellos que se ofrecen en Colombia deban cumplir con estas disposiciones es un desincentivo para que efectivamente estén disponibles en Colombia una diversidad de servicios digitales, como educativos, de ocio, profesionales, entre otros.

2. **Artículo 6. Principios relativos al tratamiento.**

Sugerimos amablemente la eliminación del literal h) «Principio de integridad» por la dificultad técnica de monitorear la fragmentación de los datos personales, así como la imposibilidad de anonimizar datos.

3. **Artículo 9. Consentimiento de niños, niñas y adolescentes.**

El numeral tercero indica que el responsable del tratamiento de datos deberá tomar todas las medidas razonables para verificar el consentimiento otorgado o autorizado por el representante legal de los menores de edad, cuando se les ofrezcan directamente servicios de la sociedad de la información.

Establecer con certeza si una persona es efectivamente el representante legal de un menor no debe ser una facultad de los particulares responsables del tratamiento de datos personales. En esa medida, y de conformidad con la buena fe, debería presumirse cierto que las personas que dicen ser representantes legales de un menor efectivamente lo son. Establecer en cabeza de los responsables del tratamiento de datos personales la obligación de verificar que efectivamente es un representante legal de un menor quien dice serlo, es una carga desproporcionada para un particular.

4. **Artículo 14. Condiciones para el tratamiento necesario para la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero.**

Solicitamos amablemente que se revisen los criterios propuestos para que el tratamiento de datos personales pueda estar basado en un interés legítimo, toda vez que la disposición propuesta contiene un gran número de requisitos que dificultarían la aplicación del interés legítimo en el tratamiento de datos personales. Algunos requisitos carecen de definición clara, lo que complicaría la implementación de esta disposición, como el término "relación pertinente y apropiada entre el titular y el responsable", incluido en el inciso b del numeral primero.

5. **Artículos 16. Tratamiento de datos personales relativos a delitos y condenas penales; artículo 17. Tratamiento de datos relativos a infracciones y sanciones administrativas.**

Estimamos respetuosamente que los artículos en comento vulneran el derecho fundamental a la libre expresión y al acceso a la información. Al respecto, la Corte Constitucional en Sentencia T-098 de 2017 estableció que:

> *"pretender que la circulación restringida del dato negativo implique que los medios de comunicación no puedan hacer mención o referenciar un hecho cierto y verificable, como fue la decisión judicial de condenar al accionante por los delitos cometidos, no tiene protección dentro del marco constitucional.* ***La circulación restringida del dato negativo tiene una finalidad precisa, pero en ningún momento podrá extenderse hasta el punto de prohibir que la sociedad pueda informarse sobre un hecho cierto y objetivo,*** *como lo es una condena penal, lo cual atentaría contra el núcleo esencial de la libertad de expresión, pues siguiendo dicha argumentación, el cumplimiento de una condena penal contemplaría no sólo la extinción de la pena, sino el hecho mismo, y en esa medida, eliminaría el dato histórico sobre la ocurrencia de un conjunto de acciones que condujeron a una condena penal, así como hacer público dicho hecho y la posibilidad de que la sociedad sea informada al respecto. Como ya lo ha reiterado la Corte en decisiones precedentes, el dato negativo de la condena penal sigue cumpliendo importantes funciones constitucionales"* (negrita fuera del texto).

Por otro lado, estas disposiciones crearían una carga burocrática desproporcionada al determinar que la verificación de los antecedentes penales de una persona deberán llevarse a cabo bajo la supervisión de las autoridades públicas, limitando el proceso obligatorio de realizar verificaciones sobre las contrapartes a través de mecanismos implementados por las compañías como el Sistema de Autocontrol y Gestión del Riesgo Integral de Lavado de Activos, Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva (SAGRILAFT). Lo anterior podría generar una desincentivo en las compañías que pretendan contratar sin realizar esta verificación.

6. **Artículo 19. Transparencia e información al titular.**

El proyecto de ley remite a la actual Ley 1581 de 2012, que establece un plazo genérico de diez días hábiles contados a partir de la fecha de recibo de la misma.

El proyecto establece que en los supuestos en los que no es posible para el responsable atender al reclamo del titular en los términos previstos, deberá informar al titular los motivos de su demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho días hábiles siguientes al vencimiento del primer término. Además,

se dispone de un plazo de tres días hábiles siguientes a su recepción para dar respuesta al derecho de rectificación en medios de comunicación.

Ni siquiera en los reglamentos de datos más restrictivos se dispone de plazos tan estrictos. Por ejemplo, el Reglamento General de Protección de Datos de la Unión Europea establece un plazo de un mes prorrogable por otro mes.

Esto responde a que las organizaciones gestionan una gran cantidad de datos, lo que dificulta el procesamiento de las solicitudes de los titulares y la verificación de su identidad en plazos tan escuetos, especialmente en casos como el derecho de acceso o portabilidad. Adicionalmente, la complejidad aumenta cuando los datos han sido transferidos a un encargado del tratamiento, ya que esto implica la participación de otro sujeto en la gestión de la petición.

Por lo tanto, sugerimos que se amplíe el plazo de respuesta a un mes a partir de la recepción de la solicitud. Además, debería concederse la posibilidad de prórroga para los casos en los que sea necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable debería informar al titular de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación.

Este ajuste permitiría un manejo más efectivo y cuidadoso de las solicitudes, garantizando tanto la protección de datos como el derecho legítimo de los titulares a acceder a su información.

7. **Artículo 23. Disposiciones generales sobre ejercicio de los derechos.**

El numeral 6 del artículo establece que, en cualquier caso, los padres o representantes legales pueden ejercer los derechos de acceso, rectificación, cancelación y oposición en nombre de los menores de edad.

Teniendo en cuenta la edad de consentimiento propuesta (14 años), la inclusión de este punto puede resultar problemática, ya que los padres o representantes legales pueden ejercer estos derechos incluso en casos en los que los menores tienen más de 14 años.

8. **Artículo 26. Derecho de rectificación en medios de comunicación.**

Se sugiere eliminar el numeral 6, toda vez que se estaría imponiendo una obligación que traslada la responsabilidad del contenido que se publica a las plataformas y responsables de redes sociales. Es claro que toda persona tiene derecho a recibir rectificaciones de contenidos que atenten contra su buen nombre o contra el principio de exactitud en Internet. No obstante, los administradores de redes sociales no deben responder por lo que en ellas se publica, ni adoptar posturas más allá de su neutralidad en la prestación de sus servicios.

Adicionalmente, el artículo no establece criterios para la adopción de protocolos ni para definir cuándo deben operar ni cuando se entiende cumplida esta obligación. Esta norma impone una carga innecesaria, injustificada y que no se compadece de la realidad actual ni del funcionamiento de este tipo de espacios.

Aunado a lo anterior, estimamos que el artículo incumple con el principio de unidad de materia en tanto no contempla el derecho de rectificación de datos personales, sino de información supuestamente inexacta publicada por medios de comunicación.

9. **Artículos 28. Derecho al olvido en búsquedas de Internet; y artículo 29. Derecho al olvido en servicios de redes sociales y servicios equivalentes.**

El derecho al olvido podría vulnerar el derecho a la libre expresión y es contrario al sistema interamericano de derechos humanos, conforme a lo establecido por la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH), y la Declaración Conjunta sobre Libertad de Expresión e Internet, adoptada por el Relator Especial de Naciones Unidas para la Libertad de Opinión y de Expresión, y la Relatora Especial de la Organización de Estados Americanos para la Libertad de Expresión.

Esta última contiene el principio de neutralidad de la red y la responsabilidad limitada de los intermediarios de internet. Es este sistema, aplicable en países como Perú, el que impide que pueda aplicar el derecho al olvido y que se expidan sentencias como la del Caso Costeja v. AEPD, resuelto por el Tribunal de Justicia de la Unión Europea (sentencia que reconoce el derecho al olvido en la Unión Europea).

La Corte Constitucional colombiana ha dicho que no podría aplicar el derecho al olvido por *"la necesidad de garantizar el derecho a la libertad de expresión en internet, que se encuentra atado al principio de neutralidad de la red. Como quedó expuesto, este último se orienta a garantizar el acceso a internet en condiciones de igualdad para todas las personas que se valen de este medio para expresar sus ideas y opiniones. Lo anterior demanda evitar situaciones de bloqueo, interferencia o filtración, que puedan llegar a implicar tratamientos diferenciales entre quienes pretenden hacer uso de la red. Esto a su vez, implica la eliminación de controles previos o de cualquier tipo de censura, salvo en aquellos supuestos específicos contemplados en la ley, por ejemplo, para evitar la difusión de pornografía infantil, entre otros. (...)*

No existe duda que la neutralidad de Internet, así como sus principios básicos de funcionamiento, se encuentran protegidos por el derecho a la libertad de expresión e información, a su vez ***consagrados en tratados internacionales sobre derechos humanos*** *y normas constitucionales como aquella contemplada en el art. 20 de la Carta Política. De lo anterior se colige que una afectación de la neutralidad de la red implica a su vez una*

intromisión con el derecho fundamental a la libertad de expresión e información de todos los usuarios de la red que, por lo tanto, ha de estar sujeta a la prueba tripartita antes mencionada. (...)

Una solución como la adoptada por el Tribunal de Justicia de la Unión Europea en el caso Costeja v. AEPD, si bien representa un mecanismo de garantía del derecho al buen nombre de la persona afectada por la difusión de la noticia, implica a la vez un sacrificio innecesario del principio de neutralidad de internet y, con ello, de las libertades de expresión e información".[6]

Por lo tanto, invitamos a un diálogo mesurado sobre este asunto con el fin de crear un marco legal que proteja tanto la privacidad individual como la libertad de expresión en el entorno digital.

10. Artículo 33. Derecho de oposición.

El numeral 1 establece que el titular podrá oponerse al tratamiento de sus datos personales si la finalidad es, entre otras, la elaboración de perfiles. Esta disposición impactaría a una gran parte de la industria tecnológica que requiere del uso de cierta información del titular para el desarrollo de su objeto social. Si se concede al titular el derecho de oposición en estos casos, podría generar cargas innecesarias o incluso hacer que las empresas no puedan proporcionar servicios diferenciados a los titulares que expresen su objeción.

Adicionalmente el numeral 2 del artículo establece el derecho del titular de datos personales a oponerse en cualquier momento al tratamiento de sus datos para fines de marketing y publicidad directa.

Es relevante que el proyecto de ley indique que, de darse esta oposición, el responsable no será obligado a seguir proveyendo servicios al titular. También se estima relevante que el proyecto de ley otorgue la posibilidad a los responsables de responder a los titulares este tipo de oposiciones.

11. Artículo 34. Decisiones individuales automatizadas, incluida la elaboración de perfiles.

Este artículo se refiere a las decisiones individuales automatizadas, incluida la elaboración de perfiles. En virtud del artículo, los titulares tienen derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, en los que no medie

---

[6] Sentencia T-277/15. Rescatado de: www.corteconstitucional.gov.co/relatoria/2015/t-277-15.htm)

intervención humana alguna, incluida la elaboración de perfiles, que le produzca efectos jurídicos o le afecte significativamente de modo similar.

Esta regla no aplica cuando ese tipo de decisiones son necesarias para la celebración o ejecución de un contrato o se basa en el consentimiento explícito del titular.

No obstante, en esos casos el responsable del tratamiento debe adoptar las medidas adecuadas para salvaguardar los derechos y garantías fundamentales del titular, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista, a recibir una explicación de la decisión y a impugnar la decisión.

Imponer esta condición no tiene en consideración el funcionamiento y la tecnología actual en materia de uso de Inteligencias Artificiales o decisiones individuales automatizadas. Exigir intervención humana implica gastos administrativos y operativos desproporcionados para los responsables. Por esa razón, se sugiere la eliminación del numeral 3 del artículo.

12. Artículo 36. Derecho a presentar una denuncia ante la Autoridad de Control.

El artículo 36 establece el derecho a presentar una denuncia ante la Autoridad de Control. No obstante, no se definen los requisitos que debe cumplir la denuncia, el procedimiento que debe surtir y los resultados que puede conllevar. Esto genera inseguridad jurídica para los responsables y encargados del tratamiento de datos personales que pueden ser sujeto de este tipo de denuncias.

Se recomienda reformular la redacción del artículo con el objetivo de indicar los requisitos que debe cumplir la denuncia, el procedimiento que debe surtir y los resultados que puede conllevar.

13. Artículo 37. Obligaciones del responsable del tratamiento.

Por técnica legislativa, el contenido del numeral 3 debería contemplarse en un parágrafo, debido a que no es propiamente una obligación. Así, incluirlo donde está puede prestarse para malas interpretaciones y la posible situación de incumplimiento de una obligación por parte de los responsables.

En línea con lo anterior, proponemos el siguiente ajuste:

~~3. La adhesión a códigos de conducta aprobados en virtud del artículo 58 o a un mecanismo de certificación aprobado en virtud del artículo 60 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.~~

Parágrafo: La adhesión a códigos de conducta aprobados en virtud del artículo 58 o a un mecanismo de certificación aprobado en virtud del artículo 60 podrán ser utilizados como

elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

14. Artículo 38. Protección de datos desde el diseño y por defecto.

El numeral 2 del artículo, establece que el responsable del tratamiento de datos *"aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles".*

Esta disposición no tiene en consideración el estado de la técnica actual implementada por los responsables del tratamiento de datos y no contempla que existen sistemas previamente creados, adicionales a los dispuestos por las autoridades nacionales, para garantizar la confidencialidad y la seguridad de los datos personales, los cuales no se ajustan a lo dispuesto en esta nueva norma. De esa manera, se llevaría a los responsables a incurrir en costos desproporcionados para adoptar este tipo de medidas técnicas.

Se sugiere eliminar esta disposición o modificar su carácter imperativo, con el objetivo de promover que los responsables migren a este tipo de sistemas para lograr avances progresivos en materia de protección de los derechos de los titulares.

15. Artículo 40. Representantes de responsables o encargados del tratamiento con domicilio fuera del territorio Nacional.

Se sugiere eliminar el numeral 1, el cual establece que *"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".*

Esta es una carga injustificada que no corresponde con la realidad del mercado. Muchas compañías prestan servicios desde el exterior y hacen tratamiento de datos en Colombia. Esto las obligaría a designar representantes en Colombia sin que haya justificación, generando cargas y barreras para los responsables.

Además, la ley ya requiere que se proporcione a los titulares la información sobre los responsables y los canales para ejercer sus derechos. Por tanto, resulta difícil comprender por qué sería necesario establecer una representación en el país.

16. Artículo 41. Encargado del tratamiento.

El numeral 1 del artículo, establece que *"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" (Negrilla por fuera del texto original).

Se sugiere eliminar la palabra "únicamente", ya que esta disposición 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. Esta norma impone una restricción innecesaria e injustificada.

17. Artículo 43. Registro de las actividades de tratamiento.

Se sugiere eliminar el artículo, toda vez que este tipo de requisitos aumentan las cargas de cumplimiento de las empresas sin que exista justificación debida para ello. Adicionalmente, aumenta la discrecionalidad de la autoridad de control para exigir información que la norma no logra justificar como necesaria.

18. Artículo 45. Bloqueo de los datos.

El artículo impone la obligación de "bloquear" los datos durante el proceso de rectificación o supresión de los mismos. Esto impone una carga operativa excesiva para una solicitud que en todo caso debe ser tramitada en 15 días hábiles.

19. Artículo 49. Notificación de un Incidente de seguridad de los datos personales a la autoridad de control.

Se sugiere modificar el término para la notificación de incidentes de seguridad de los datos personales. Se recomiendo 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 para las empresas, particularmente las pequeñas y medianas que no tienen las capacidades administrativas y operativas para afrontar este tipo de situaciones de manera ágil y eficiente. Además, se recomienda especificar que el plazo debe comenzar a contar desde que el oficial de protección de datos tenga conocimiento del asunto.

20. Artículos 51. Evaluación de impacto relativa a la protección de datos; artículo 52. Consulta previa.

El proyecto establece que 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 garantías de las personas naturales, deberá realizarse una evaluación de impacto. En caso de concluir que en efecto supone un alto riesgo para los

derechos y garantías de los titulares, el responsable deberá consultar ante la Superintendencia de Industria y Comercio para proceder con el tratamiento.

No obstante, la ley no define lo que se debe entender por "alto riesgo", lo que deja el concepto al arbitrio de la autoridad. Esto vulnera la seguridad jurídica a la que tienen derecho los responsables y encargados del tratamiento de la información.

21. Artículo 52. Consulta Previa

Respetuosamente se sugiere la eliminación del artículo, toda vez que la consulta previa podría desincentivar el desarrollo de proyectos innovadores, incluso si dichas iniciativas tienen beneficios legítimos y protegen adecuadamente la privacidad de los titulares de datos. Además, se podrían generar costos adicionales para las organizaciones, especialmente las más pequeñas. En lugar de imponer consultas previas obligatorias, se sugiere promover pautas y mejores prácticas para permitir decisiones informadas sobre la protección de datos.

22. Artículos 53. Designación del Oficial de protección de datos; y artículo 54. Calidades del Oficial de protección de datos.

El artículo 53 incluye la figura del Oficial de protección de datos, sin diferencias sustanciales en cuanto al régimen previsto en el Régimen General de Protección de Datos de la Unión Europea. Sin embargo, los incisos c y d del numeral 2, agregan que el responsable y encargado deberán designar un Oficial cuando se trate de entidades que, entre otros:

> i) exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala; y
> ii) en el caso de prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

Estos supuestos no están previstos siquiera en el Régimen General de Protección de Datos de la Unión Europea, por consiguiente añadirían cargas burocráticas innecesarias que desincentivarían la dinámica y crecimiento del ecosistema.

Además, no se establecen las reglas para los responsables que realizan el tratamiento y no están domiciliados en Colombia, por lo que termina convirtiéndose en una carga para este tipo de responsables. La norma debería ser más clara al establecer este tipo de situaciones para garantizar el cumplimiento de las normas y evitar que los responsables incurran en sanciones.

Asimismo, el proyecto establece en el inciso 6 del artículo 54 que el responsable o encargado del tratamiento publicará los datos de contacto del Oficial a la Delegatura para la Protección de Datos Personales ("Delegatura") en un plazo de 15 días hábiles. Nuevamente, estas disposiciones resultan desproporcionadas y ni siquiera se contemplan en el Régimen General de Protección de Datos de la Unión Europea.

Por lo tanto, sugerimos eliminar estas disposiciones con el fin de evitar obstáculos engorrosos para el desarrollo de la economía digital.

23. Artículo 66. Transferencias o comunicaciones no autorizadas por la Ley.

El artículo establece que cualquier sentencia de un órgano judicial o decisión de una autoridad administrativa de un tercer país que requiera que un responsable o encargado del tratamiento transfiera o comunique datos personales, sólo será reconocida o ejecutable si se fundamenta en un acuerdo internacional, como un tratado de asistencia jurídica mutua vigente entre el país requirente y Colombia.

Esta norma puede resultar en el incumplimiento de deberes legales de los responsables en terceros países.

El artículo podría ser más claro y establecer su aplicación únicamente a los casos en que se solicita información tratada exclusivamente en Colombia y que reposan en bases de datos ubicadas en el país.

24. Artículo 76. Poderes Investigativos.

No hace sentido que se faculte a la Superintendencia de Industria y Comercio para llevar a cabo visitas de inspección cuando los documentos esenciales para llevar a cabo investigaciones pueden ser proporcionados por los responsables y/o titulares que hayan presentado sus quejas ante dicha autoridad.

Las visitas de inspección pueden ser percibidas como redundantes y excesivamente invasivas. Los documentos y pruebas necesarias para llevar a cabo investigaciones, suministrados de manera voluntaria y transparente por los responsables y/o titulares, ofrecen una base sólida para las investigaciones sin necesidad de recurrir a visitas de inspección, las cuales podrían ser percibidas como una violación innecesaria de la privacidad y generar desconfianza entre las partes involucradas. Además, depender principalmente de la información proporcionada por los involucrados fomenta un clima de cooperación y confianza mutua, lo cual es esencial para un proceso de investigación justo y eficiente.

25. Artículo 77. Poderes correctivos y sancionatorios; y artículo 99.

A diferencia del Régimen General de Protección de Datos de la Unión Europea, el proyecto establece que la Superintendencia de Industria y Comercio, a través de la Delegatura de

Protección de Datos, dispondrá de poderes correctivos para imponer multas de carácter personal o institucional a los responsables y encargados. Sin embargo, no aclara bajo qué condiciones se aplicarán dichas multas de carácter personal.

La redacción del articulado brinda poca certeza y seguridad jurídica, ya que no aclara en qué supuestos se podrán imponer multas de carácter personal. En efecto, no resulta claro si se refiere a aquellos casos en que responsables y encargados actúen como personas físicas o naturales, o si por otro lado se aplicarán a integrantes de una organización. En cualquier caso, la falta de certeza podría resultar en un desincentivo para el tratamiento de datos personales en Colombia, considerando el monto de las multas.

Sugerimos eliminar la referencia a multas de carácter personal o aclarar de manera suficiente sin generar un desincentivo para el debido tratamiento de datos personales.

26. Artículo 89. Inteligencia artificial.

Se sugiere la eliminación del artículo ya que la medida va en contra de los postulados legales de Colombia que propenden por el desarrollo tecnológico del país y de la neutralidad tecnológica.

Por lo tanto, limitar el uso de la inteligencia artificial, por ejemplo, en la implementación de mecanismos de anonimización o disociación, implicaría una restricción injustificada de este tipo de herramientas y no permitiría su adecuado desarrollo y evolución. En contraste, la regulación debería concentrarse en la imposición de medidas de seguridad que garanticen la confidencialidad de los datos personales de los titulares.

Adicionalmente, somete a la discrecionalidad de la Superintendencia de Industria y Comercio (SIC), entidad que no es experta en materia de Inteligencia Artificial, la decisión de prohibir este tipo de tecnologías sin siquiera determinar un listado de requisitos o condiciones para el efecto. Incluso esta disposición contradice el principio de neutralidad de la red legal y constitucionalmente reconocido. Al respecto, los artículos 56 de la Ley 1450 de 2011 y el artículo 2.1.10.10 de la Resolución CRC 5050 de 2016, establecen que el estado les garantiza a los ciudadanos no restringir el acceso y uso a cualquier contenido y/o aplicación a través de internet.

El principio, de acuerdo con el Relator Especial de las Naciones Unidas (ONU) sobre la Promoción y Protección del derecho a la Libertad de Opinión y de Expresión, establece que: *"[e]l tratamiento de los datos y el tráfico de Internet no debe ser objeto de ningún tipo de discriminación en función de factores como dispositivos, contenido, autor, origen y/o destino del material, servicio o aplicación"*.

Lo que persigue tal principio es que la libertad de acceso y elección de los usuarios de utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal por medio de Internet no esté condicionada, direccionada o restringida, por medio de bloqueo,

filtración, o interferencia. Así las cosas, el principio se vulnera en la medida en que el artículo establece que la SIC podría prohibir acceso a tecnologías, sin que se cumplan de lleno los requisitos para que se permitan las excepciones al principio de neutralidad de la red.

La Relatoría Especial sobre Libertad de Expresión de la CIDH ha señalado tres excepciones al principio de neutralidad: (i) cuando sea necesario para mantener la seguridad y funcionamiento de Internet; (ii) con el fin de evitar transferencia de datos no queridos por el usuario y siempre que éste lo solicite de forma libre y expresa; (iii) para lidiar con problemas de congestión de Internet; y el artículo en comento no responde a algunas de las excepciones. De este modo, se ha reiterado en este informe de la Relatoría que: *"La neutralidad de la red se desprende del diseño original de Internet, el cual facilita el acceso y la difusión de contenidos, aplicaciones y servicios de manera libre y sin distinción alguna. Al mismo tiempo, la inexistencia de barreras desproporcionadas de entrada para ofrecer nuevos servicios y aplicaciones en Internet constituye un claro incentivo para la creatividad, la innovación y la competencia. (...) La protección de la neutralidad de la red es fundamental para garantizar la pluralidad y diversidad del flujo informativo".*

Por otro lado, el artículo es contraproducente desde el punto de vista técnico al indicar que quienes deben cumplir con las obligaciones sugeridas son quienes usan la inteligencia artificial. Meros usuarios de la inteligencia artificial no podrían tener injerencia sobre los datos personales objeto de tratamiento por la herramienta.

En todo caso, las medidas propuestas, de aplicarse a desarrolladores de la inteligencia artificial resultan negativas para el ecosistema digital y la innovación en Colombia. Cualquier regulación de la inteligencia artificial, de conformidad con recomendaciones de la OCDE, debe ser sectorial.

27. Artículo 90. Neurodoerechos

Este asunto se encuentra en una fase temprana de desarrollo, aún no existe un consenso definitivo entre académicos, sociedad civil, gobiernos y tecnólogos sobre sus verdaderos alcances. Esta falta de consenso podría llevar a decisiones que, en lugar de proteger al consumidor, tengan impactos negativos en el acceso de las poblaciones vulnerables a las neurotecnologías. Por lo tanto, se sugiere la eliminación del artículo.

28. Artículo 91. Tecnologías de rastreo.

El proyecto establece que es necesario obtener el consentimiento del usuario para utilizar las tecnologías de rastreo (ej. uso de cookies). Asimismo, se establecen las condiciones bajo las cuales se considerará prestado dicho consentimiento.

No obstante, ni siquiera el Régimen General de Protección de Datos de la Unión Europea regula explícitamente cómo debe ser el tratamiento de datos bajo tecnologías de rastreo. Por lo tanto, sugerimos que se recurra a sistemas más ágiles y simples para el tratamiento de datos bajo tecnologías de rastreo, como es el mecanismo del *"opt out"* (en reemplazo del *"opt in"*).

La dinámica propia de los negocios requiere de mecanismos flexibles y expeditos para el tratamiento de datos personales. Entendemos que el sistema *"opt out"* cumple esas premisas y, a su vez, concede una efectiva protección de los derechos de los titulares de los datos personales quienes pueden en todo momento ejercer la facultad de exigir que se deje de utilizar sus datos bajo este tipo de tecnologías. Inclusive los pedidos de consentimiento para el uso de datos con fines de rastreo electrónico, como el caso puntual de *cookies*, han sido cuestionados por los propios titulares de datos en el sentido de afectar la experiencia del usuario.

El sistema propuesto en el proyecto podría constituir un obstáculo para esta actividad específica, afectando la generación de nuevos negocios lícitos para las empresas y la experiencia para el usuario.

29. Artículo 92. Derecho a indemnización y responsabilidad.

Esta disposición, en su numeral 6, le otorga a la Superintendencia de Industria y Comercio la calidad de juez en materia de responsabilidad civil, lo que a nuestro juicio quebranta el principio de juez natural.

> *"El principio de juez natural se refiere de una parte a la especialidad, pues el legislador deberá consultar como principio de razón suficiente la naturaleza del órgano al que atribuye las funciones judiciales, y de otro lado, a la predeterminación legal del Juez que conocerá de determinados asuntos. Lo anterior supone: i) que el órgano judicial sea previamente creado por la ley; ii) que la competencia le haya sido atribuida previamente al hecho sometido a su decisión; iii) que no se trate de un juez por fuera de alguna estructura jurisdiccional (ex post) o establecido únicamente para el conocimiento de algún asunto (ad hoc); y iv) que no se someta un asunto a una jurisdicción especial cuando corresponde a la ordinaria o se desconozca la competencia que por fuero ha sido asignada a determinada autoridad judicial.*
>
> *Otro aspecto a considerar es que el juez natural es aquél a quien la Constitución o la ley le ha asignado el conocimiento de ciertos asuntos para su definición. En éste* (sic) *último caso, vale decir, cuando la competencia no ha sido fijada explícitamente en la Constitución, ha señalado la jurisprudencia constitucional, el legislador tiene libertad de configuración, siempre que no altere el marco funcional definido en la Constitución Política*[7]*".*

[7] Corte Constitucional. Sentencia T-916 de 2014. Disponible en: https://www.corteconstitucional.gov.co/relatoria/2014/T-916-14.htm#:~:text=El%20principio%20de%20juez%20natural,que%20conocer%C3%A1%20de%20determinados%20asuntos.

Además, el artículo plantea inquietudes considerables acerca del impacto de las acciones regulatorias en la supervisión de las normas de protección de datos. Existe la posibilidad real de que se debilite el papel de los reguladores en la aplicación de estas normas, siguiendo las prioridades que ellos mismos han establecido.

Por otro lado, aunque las acciones de los reguladores tienen el potencial de generar cambios positivos para todos los usuarios, permitir acciones privadas negociadas o acciones colectivas puede limitar estas mejoras a un subconjunto de usuarios.

Finalmente, la apertura a acciones privadas facilitaría prácticas abusivas y sobrecargaría a los responsables del tratamiento de datos, quienes deben defenderse contra estas acciones perjudiciales. Además, existe el riesgo de que surjan entidades oportunistas que prioricen sus intereses sobre la privacidad de las personas, amenazando la integridad del sistema de protección de datos.

Por lo anteriormente expuesto, sugerimos amablemente la eliminación del artículo.

30. **Artículo 97. Infracciones consideradas graves; y artículo 40. Representantes de responsables o encargados del tratamiento con domicilio fuera del territorio Nacional.**

El proyecto dispone que cuando se realice el tratamiento de datos personales de titulares que residan en territorio nacional por parte de un responsable o encargado no establecido en Colombia, el responsable o encargado del tratamiento designará por escrito a un representante legal y/o sucursal en Colombia, excepto en ciertos supuestos de excepción.

Sin embargo, según el proyecto, los representantes de los responsables o encargados de tratamiento se encuentran sujetos al régimen sancionador establecido en la ley. Esto se produciría bajo determinadas circunstancias, por ejemplo, ante la falta de atención por el representante de las solicitudes efectuadas por la autoridad de control o por los titulares.

Al respecto, se sugiere eliminar la figura del representante con el fin de evitar la creación de cargas burocráticas innecesarias. Incluso en el supuesto de que la decisión legislativa sea conservar este instituto, debería suprimirse la responsabilidad del representante. El establecimiento de posibles sanciones en cabeza del representante configuraría un elemento que desincentivaría el rol o incrementaría notablemente los costos de su designación para un responsable o encargado (ej.: contratación de seguro) si se toma en cuenta el riesgo que podría generar una sanción aplicable a su persona. Todo ello sin entrar en la consideración de la razonabilidad o equidad de la solución de derivar en el representante la responsabilidad del responsable o encargado.

31. Artículo 99. Sanciones

Las infracciones consideradas muy graves se sancionarán con multas de 2.000 salarios mínimos mensuales legales vigentes o tratándose de sujetos obligados al Registro de Bases de Datos, de una cuantía equivalente al 4% como máximo de las utilidades que genere el año fiscal anterior, optando por la de mayor cuantía.

Los montos de las sanciones deben ser razonables considerando el impacto que ello puede generar para la atracción de nuevos negocios e inversiones. Los rangos de las sanciones son elevados considerando que la sanción mínima tiene un monto de 1.000 salarios mínimos mensuales legales vigentes. En la actualidad las sanciones que impone la Superintendencia de Industria y Comercio tienen montos significativamente inferiores.

El proyecto de ley establece otra categoría de sanción que se calcula con base en el equivalente a un porcentaje de las utilidades generadas en el año fiscal anterior y que se optará por la de mayor cuantía. Al respecto deben hacerse dos comentarios:

En primer lugar, con este nuevo umbral se aumentan las cuantías de las sanciones porque el porcentaje de utilidades puede ser mucho mayor a los salarios mínimos definidos en cada caso concreto.

Por otro lado, la norma establece que esta sanción será aplicable a los sujetos obligados al Registro de Bases de Datos, pero en toda la ley no se hace referencia a esta obligación, por lo cual no es claro quiénes serían los posibles sujetos de estas eventuales sanciones.

32. Artículo 102. Condiciones del consentimiento.

La obligación de recabar nuevas autorizaciones durante el año siguiente a la expedición de la norma afectaría el activo principal de muchas empresas que es la cantidad de usuarios activos. En este sentido, el hecho de que se deban recabar nuevas autorizaciones para poder tratar sus datos personales crearía una carga desproporcionada a este tipo de empresas. Además, esta obligación podría resultar en inconvenientes significativos para los usuarios, incluyendo interrupciones en el servicio, pérdida de funcionalidades y complicaciones administrativas, lo que afectaría negativamente su experiencia con los servicios proporcionados.

33. Artículo 105. Contratos de encargados del tratamiento.

Los contratos de los encargados del tratamiento suscritos con anterioridad al proyecto, serán válidos hasta 18 meses 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 referente al "Encargado del tratamiento".

Los contratos firmados con posterioridad a la fecha de entrada en vigencia de la ley, deberán cumplir con los requisitos establecidos en la propia norma (artículo 41).

Consideramos que los plazos que contempla el proyecto son demasiado breves para que las partes adecuen sus contratos y, por ende, procedimientos y procesos. Consideramos más razonable ampliar el mismo a un período de dos años como incluso lo dispuso, en su momento, el Régimen General de Protección de Datos de la Unión Europea.

En estos términos, planteamos respetuosamente nuestros comentarios al proyecto de ley, no sin antes invitar a todos los actores interesados a unir fuerzas para forjar de manera colaborativa una visión regional de la privacidad en línea. A menudo, las autoridades de nuestro continente adoptan legislaciones de otras regiones que no responden a las realidades latinoamericanas donde la tecnología y las prácticas empresariales están en evolución constante. Por lo tanto, es crucial desarrollar una perspectiva latinoamericana que proteja los derechos fundamentales y promueva el uso responsable de los datos para el desarrollo sostenible de nuestras naciones.

Agradezco de antemano su tiempo y consideración.

Atentamente,

PABLO NIETO D.
Gerente Regional de Políticas Públicas Zona Andina
Asociación Latinoamericana de Internet (ALAI)
pablo@alati.lat