

**San José, 02 de setiembre de 2024.  
Criterio N° DJ-C-499-2024.  
Cualquier consulta referirse a este oficio.**

**Señora  
MBA. Ana Eugenia Romero Jenkins  
Directora Ejecutiva  
S.D.**

**Estimada señora**

Mediante oficio N° 1265-DE-2024, de 16 de abril de 2024, la Dirección Ejecutiva solicita criterio jurídico sobre el tratamiento que esa oficina debe brindar a los datos personales consignados en los documentos remitidos por las oficinas judiciales y las autoridades jurisdiccionales para publicar en el Boletín Judicial. A continuación, se atiende el requerimiento.

**Criterio.**

### **1. Antecedentes.**

En el oficio citado Dirección Ejecutiva expone el caso de una persona usuaria que planteó un reclamo por la consignación de información personal en un edicto publicado en el Boletín Judicial. En virtud de esa circunstancia, esa oficina consulta lo siguiente:

1. Cuando corresponda, cuál sería la instancia que debe valorar el contenido de las publicaciones, bajo el contexto de la Ley de Protección de Datos. Cabe señalar que esta Dirección Ejecutiva no tiene competencia ni recurso humano para modificar el contenido de las publicaciones, ya que responden a una orden de la Autoridad Judicial.
2. ¿Es necesario que en este tipo de publicaciones del Boletín Judicial se despersonalicen los textos por parte de las Autoridades Judiciales? Debe tomarse en cuenta que, de suprimirse datos como nombre o calidades, podría no lograrse el cometido de la publicación al impedirse la identificación de la persona a la que refiere la publicación.
3. Debería considerarse por parte de las instancias que remiten los textos a publicar el principio de minimización de datos.
4. En este supuesto de despersonalización, cuál sería la función de la Dirección Ejecutiva, pues se trata de temas jurisdiccionales sobre los cuales no se tiene competencia ni conocimiento.

Con la intención de atender la consulta remitida, seguidamente, se analizan los temas relacionados con la situación expuesta por la Dirección Ejecutiva y, luego, se responde en forma específica cada una de las preguntas referidas.

## **2. Generalidades sobre la protección y tratamiento de datos personales.**

En nuestro país, la recopilación, la protección y el tratamiento de datos personales almacenados en bases de datos comerciales o accesibles a terceros, así como el derecho a la autodeterminación informativa, se encuentran regulados en la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, Ley N° 8968, de 7 de julio de 2011 (en adelante Ley de protección de la persona y sus datos personales o Ley N° 8968). El artículo 1 de esa ley establece que ese cuerpo normativo es de orden público.

### **Artículo 1. Objetivo y fin.**

Esta ley es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

Las leyes de orden público constituyen elementos normativos vertebradores del ordenamiento jurídico, cuyas disposiciones se caracterizan por ser generales y abstractas. Su contenido es de aplicación general y acatamiento obligatorio, dentro de su ámbito de cobertura. En las resoluciones número 2009-013606, de las catorce horas y cincuenta y siete minutos del 26 de agosto de 2009, y 001441-1992, de las quince horas y cuarenta y cinco minutos del 2 de junio de 1992, la Sala Constitucional define las leyes de orden público en los siguientes términos:

Por otra parte, y relación con el tema de las leyes de orden público, en la sentencia 1441-92 la Sala señaló:

“I ) El artículo 129 de la Constitución Política dispone, entre otras cosas, que "no tiene eficacia la renuncia de las leyes en general, ni la especial de interés público", de tal suerte que "los actos y convenios contra las leyes prohibitivas serán nulos, si las mismas leyes no disponen otra cosa". El concepto incluido por el constituyente de 1949 "leyes de interés público", corresponde a lo que en doctrina se conoce como de "orden público", es decir, aquéllas mediante las que interviene el Estado a fin de asegurar en la sociedad, su organización moral, política, social y económica” (el subrayado es agregado).

Acorde con las características atribuidas a las leyes de orden público, la Ley N° 8968 regula en forma general la recolección, el uso y el tratamiento de la información personal almacenada en bases de datos automatizadas o manuales, de carácter público o privado, constituidas con la finalidad de comercializar, distribuir o difundir la información.

Importante advertir desde ahora que, se encuentran excluidas del ámbito de aplicación de la ley, las bases de datos personales, públicas o privadas, constituidas para uso interno, personal o doméstico<sup>1</sup>, mientras la información no sea comercializada, distribuida o difundida.

### **Artículo 2. Ámbito de aplicación.**

Esta ley será de aplicación a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos.

El régimen de protección de los datos de carácter personal que se establece en esta ley no será de aplicación a las bases de datos mantenidas por personas físicas o jurídicas con fines exclusivamente internos, personales o domésticos, siempre y cuando estas no sean vendidas o de cualquier otra manera comercializadas.

Para dimensionar apropiadamente el ámbito de cobertura de la Ley de Protección de la Persona y sus Datos Personales, conviene tomar en cuenta las definiciones incluidas en su articulado y reglamento, todas ellas relativas a las cuestiones que pretende resguardar esa legislación.

Empecemos por comprender que debe entenderse por *datos personales*. Según el artículo 3 del cuerpo normativo en estudio, se consideran *datos personales* las informaciones referidas en forma específica a una persona física identificada o identificable<sup>2</sup>.

### **Artículo 3. Definiciones.**

Para los efectos de la presente ley se define lo siguiente:

---

<sup>1</sup> **Reglamento a la Ley de protección de la persona frente al tratamiento de sus datos personales. Artículo 2. Definiciones, siglas y acrónimos.** (...) c) Base de datos interna, personal o doméstica: Se considerará como base de datos personal o doméstica, cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales restringidos o de acceso irrestricto, mantenidos por personas físicas, siempre y cuando las bases de datos o su contenido no sea comercializado, distribuido o difundido. Se considerará como base de datos interna cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales mantenidos por personas jurídicas, públicas o privadas, siempre y cuando las bases de datos o su contenido no sea comercializado, distribuido o difundido. Conservarán la calidad de base de datos interna, aquellas bases de datos que sean compartidas dentro de un mismo grupo de interés económico ya sea local o con presencia internacional siempre que no medie difusión o distribución a terceros, venta o comercialización de cualquier naturaleza.

<sup>2</sup> **Reglamento a la Ley de protección de la persona frente al tratamiento de sus datos personales. Artículo 2. Definiciones, siglas y acrónimos.** (...) q) Persona física identificable: Persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad anatómica, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionadas.

(...)

b) Datos personales: cualquier dato relativo a una persona física identificada o identificable.

(...)

Adicionalmente, la Ley N° 8968 subdivide los datos personales en (1) sensibles, (2) de acceso restringido, (3) de acceso irrestricto y (4) referentes al comportamiento crediticio. Conforme a los artículos 3 y 9 de ese cuerpo normativo, son *datos sensibles* aquellos que relatan aspectos intrínsecos y reservados (privados) de las creencias y condiciones de una persona o, como los describe la ley, aquellos relativos al fuero íntimo de la persona.

### **Artículo 3. Definiciones.**

Para los efectos de la presente ley se define lo siguiente:

(...)

e) Datos sensibles: información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros.

(...)

-0-

### **Artículo 9. Categorías particulares de los datos.**

Además de las reglas generales establecidas en esta ley, para el tratamiento de los datos personales, las categorías particulares de los datos que se mencionarán, se regirán por las siguientes disposiciones:

#### **1.- Datos sensibles.**

Ninguna persona estará obligada a suministrar datos sensibles. Se prohíbe el tratamiento de datos de carácter personal que revelen el origen racial o étnico, opiniones políticas, convicciones religiosas, espirituales o filosóficas, así como los relativos a la salud, la vida y la orientación sexual, entre otros.

(...)

De acuerdo con los numerales 3 y 9 de la ley en estudio, son *datos personales de acceso irrestricto* los almacenados en bases de datos públicas de acceso general, por así disponerlo una ley especial y por la finalidad del almacenamiento de esos datos. En tanto que, se consideran *datos personales de acceso restringido*, aquellos que interesan únicamente a su titular o a la Administración Pública, aunque se encuentren en bases de datos de acceso público.

### **Artículo 3. Definiciones.**

Para los efectos de la presente ley se define lo siguiente:

(...)

c) Datos personales de acceso irrestricto: los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.

d) Datos personales de acceso restringido: los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública.

(...)

-0-

#### **Artículo 9.- Categorías particulares de los datos.**

Además de las reglas generales establecidas en esta ley, para el tratamiento de los datos personales, las categorías particulares de los datos que se mencionarán, se regirán por las siguientes disposiciones:

(...)

##### **2.- Datos personales de acceso restringido**

Datos personales de acceso restringido son los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública. Su tratamiento será permitido únicamente para fines públicos o si se cuenta con el consentimiento expreso del titular.

##### **3.- Datos personales de acceso irrestricto**

Datos personales de acceso irrestricto son los contenidos en bases de datos públicas de acceso general, según lo dispongan las leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.

No se considerarán contemplados en esta categoría: la dirección exacta de la residencia, excepto si su uso es producto de un mandato, citación o notificación administrativa o judicial, o bien, de una operación bancaria o financiera, la fotografía, los números de teléfono privados y otros de igual naturaleza cuyo tratamiento pueda afectar los derechos y los intereses de la persona titular.

(...)

Atendiendo el contenido del ordinal 9 del decreto legislativo analizado, también se considera información personal los datos atinentes al comportamiento crediticio de las personas, cuyo contenido se regirá por las normas del Sistema Financiero Nacional, sin perjuicio del ejercicio del derecho a la autodeterminación informativa.

#### **Artículo 9. Categorías particulares de los datos.**

Además de las reglas generales establecidas en esta ley, para el tratamiento de los datos personales, las categorías particulares de los datos que se mencionarán, se regirán por las siguientes disposiciones:

(...)

##### **4.- Datos referentes al comportamiento crediticio.**

Los datos referentes al comportamiento crediticio se regirán por las normas que regulan el Sistema Financiero Nacional, de modo que permitan garantizar un grado de riesgo aceptable por parte de las entidades financieras, sin impedir el pleno ejercicio del derecho a la autodeterminación informativa ni exceder los límites de esta ley.

Ahora bien, como se dijo anteriormente, la Ley N° 8968 regula el uso y tratamiento de datos personales cuando éstos se encuentren almacenados en bases informativas destinadas

a la comercialización, distribución o difusión de la información. Para esos efectos, según la ley de marras y su reglamento, se considera base de datos la recopilación organizada de datos personales, destinada a ser utilizada en diversas actividades, tales como registro, organización, conservación, consulta, modificación, comunicación, intercambio, cotejo y comercialización de la información. El artículo 3 de la ley define la base de datos en los siguientes términos:

### **Artículo 3. Definiciones.**

Para los efectos de la presente ley se define lo siguiente:

a) Base de datos: cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales, que sean objeto de tratamiento o procesamiento, automatizado o manuales, cualquiera que sea la modalidad de su elaboración, organización o acceso.

El artículo 2 del Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, Decreto Ejecutivo N° 37554-JP (en adelante Reglamento N° 37554-JP o simplemente Reglamento) define la base de datos en términos similares a los utilizados por la ley, agregando que esa recopilación puede encontrarse en un sitio físico o en la internet y debe contar con la dirección de una persona responsable, concepto este último que ya se encontraba previsto en la ley, en el aparatado de definiciones<sup>3</sup>.

**Artículo 2. Definiciones, siglas y acrónimos.** Además de las definiciones establecidas en la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, para los efectos del presente Reglamento se entenderá por:

(...)

b) Base de datos: Cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales públicos o privados, que sean objeto de tratamiento, automatizado o manual, en el sitio o en la nube, bajo control o dirección de un responsable, cualquiera que sea la modalidad de su elaboración, organización o acceso.

En cuanto a la materia protegida, tanto la Ley N° 8968, como su Reglamento, definen el (uso y) tratamiento de datos personales como el conjunto de operaciones destinadas a facilitar el acceso a la información recopilada. En cuanto a este tema, el Reglamento es más amplio que la Ley, porque propone definiciones para las nociones de *comercializar, consultar,*

---

<sup>3</sup> **Ley de protección de la persona frente al tratamiento de sus datos personales. Artículo 3. Definiciones.** (...) h) Responsable de la base de datos: persona física o jurídica que administre, gerencie o se encargue de la base de datos, ya sea esta una entidad pública o privada, competente, con arreglo a la ley, para decidir cuál es la finalidad de la base de datos, cuáles categorías de datos de carácter personal deberán registrarse y qué tipo de tratamiento se les aplicarán.

*distribuir y difundir, transferencia de datos personales y tratamiento de datos.* A continuación, se transcriben las definiciones aludidas.

**Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales.  
Artículo 3. Definiciones.**

Para los efectos de la presente ley se define lo siguiente:

(...)

**i)** Tratamiento de datos personales: cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros.

-0-

**Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales.**

**Artículo 2. Definiciones, siglas y acrónimos.** Además de las definiciones establecidas en la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, para los efectos del presente Reglamento se entenderá por:

(...)

**e)** Comercializar: Vender, transar, intercambiar o de cualquier manera enajenar o pignorar, con fines de lucro a favor de un tercero, una o más veces, aquellos datos personales que consten en bases de datos.

(...)

**g)** Consulta: Solicitud realizada a una base de datos, en la que se requiere información concreta en función de criterios de búsqueda definidos, siempre que dicha solicitud no resulte en una trasbase o réplica de la base de datos.

(...)

**j)** Distribución, difusión: Cualquier forma en la que se repartan o publiquen datos personales, a un tercero, por cualquier medio siempre que medie un fin de comercializar el dato o medie el lucro con la base de datos.

(...)

**w)** Transferencia de datos personales: Acción mediante la cual se trasladan datos personales del responsable de una base de datos personales a cualquier tercero distinto del propio responsable, de su grupo de interés económico, del encargado, proveedor de servicios o intermediario tecnológico, en estos casos siempre y cuando el receptor no use los datos para distribución, difusión o comercialización.

**x)** Tratamiento de datos: Cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión, distribución o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros.

**y)** Tratamiento de datos automatizado: Cualquier operación, conjunto de operaciones o procedimientos, aplicados a datos personales, efectuados mediante la utilización

de hardware, software, redes, servicios, aplicaciones, en el sitio o en la nube, o cualquier otra tecnología de la información que permitan la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión, distribución o cualquier otra forma que facilite el acceso a estos, el cotejo, o la interconexión, así como su bloqueo, supresión o destrucción, intercambio o digitalización de datos personales, entre otros.

(...)

Entonces, conforme a las consideraciones expuestas y las normas citadas, la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, y su reglamento, protegen la libertad y el derecho a la autodeterminación informativa, regulando el tratamiento de la información personal almacenada en bases de datos recopiladas para brindar acceso a terceras personas, asentando la responsabilidad por el uso y manejo de esos archivos en las personas responsables de esos bancos informativos.

Sin embargo, tal protección no brinda cobertura a todos los supuestos de hecho relacionados con el uso y tratamiento de información personal. La ley resulta inaplicable cuando no existe una base de datos personales destinada a la comercialización o difusión de su información. La implementación de las salvaguardas y los procedimientos establecidos en ese cuerpo normativo requieren la existencia de una base de datos personales. Ese banco informativo funciona como condición objetiva para aplicar la ley. Consecuentemente, ante la ausencia de un archivo de datos personales recopilados para compartir con terceros, la ley resulta inaplicable.

Conviene advertir que, en estos casos, aunque no opere la protección derivada de la Ley N° 8968, el ordenamiento jurídico ofrece múltiples herramientas legales para garantizar la privacidad de las personas y contrarrestar el uso abusivo, inapropiado e ilegal de la información personal.

Aparte de lo indicado, la ley prescribe tres supuestos en los que se excepciona su aplicación. El primero, genérico, contenido en el artículo 8, que permite limitar los principios, los derechos y las garantías previstas en esa normativa cuando concurra un interés público, como sucede en temas relacionados con la seguridad del Estado; la seguridad y el ejercicio de la autoridad pública; la prevención, persecución, investigación, detención y represión de actividades delictivas o contrarias a la ética profesional; la investigación estadística, histórica o científica, siempre que no se pueda identificar a las personas; la adecuada prestación de servicios públicos, y; la eficiencia de la actividad ordinaria de la Administración Pública.

**Artículo 8. Excepciones a la autodeterminación informativa del ciudadano.**

Los principios, los derechos y las garantías aquí establecidos podrán ser limitados de manera justa, razonable y acorde con el principio de transparencia administrativa, cuando se persigan los siguientes fines:

- a) La seguridad del Estado.
- b) La seguridad y el ejercicio de la autoridad pública.
- c) La prevención, persecución, investigación, detención y represión de las infracciones penales, o de las infracciones de la deontología en las profesiones.
- d) El funcionamiento de bases de datos que se utilicen con fines estadísticos, históricos o de investigación científica, cuando no exista riesgo de que las personas sean identificadas.
- e) La adecuada prestación de servicios públicos.
- f) La eficaz actividad ordinaria de la Administración, por parte de las autoridades oficiales.

El segundo, específico, se refiere a los datos sensibles. El apartado 1 del numeral 9 de la ley indica en forma expresa que ninguna persona estará obligada a suministrar ese tipo de datos, excepto que *a) El tratamiento de los datos sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que la persona interesada esté física o jurídicamente incapacitada para dar su consentimiento; b) El tratamiento de los datos sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo, por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de las personas interesadas; c) El tratamiento se refiera a datos que la persona interesada haya hecho públicos voluntariamente o sean necesarios para el reconocimiento, el ejercicio o la defensa de un derecho en un procedimiento judicial, y; d) El tratamiento de los datos resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un funcionario o funcionaria del área de la salud, sujeto al secreto profesional o propio de su función, o por otra persona sujeta, asimismo, a una obligación equivalente de secreto.*

El tercero, también específico, tiene que ver con los datos personales de acceso restringido. El apartado 2 del antes citado ordinal 9 establece que esa información puede ser objeto de tratamiento cuando medien fines públicos o se cuente con el consentimiento expreso del titular.

**Artículo 9. Categorías particulares de los datos.**

Además de las reglas generales establecidas en esta ley, para el tratamiento de los datos personales, las categorías particulares de los datos que se mencionarán, se regirán por las siguientes disposiciones:

**1.- Datos sensibles.**

Ninguna persona estará obligada a suministrar datos sensibles. Se prohíbe el tratamiento de datos de carácter personal que revelen el origen racial o étnico, opiniones políticas, convicciones religiosas, espirituales o filosóficas, así como los relativos a la salud, la vida y la orientación sexual, entre otros.

Esta prohibición no se aplicará cuando:

- a) El tratamiento de los datos sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que la persona interesada esté física o jurídicamente incapacitada para dar su consentimiento.
- b) El tratamiento de los datos sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo, por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de las personas interesadas.
- c) El tratamiento se refiera a datos que la persona interesada haya hecho públicos voluntariamente o sean necesarios para el reconocimiento, el ejercicio o la defensa de un derecho en un procedimiento judicial.
- d) El tratamiento de los datos resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un funcionario o funcionaria del área de la salud, sujeto al secreto profesional o propio de su función, o por otra persona sujeta, asimismo, a una obligación equivalente de secreto.

**2.- Datos personales de acceso restringido.**

Datos personales de acceso restringido son los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública. Su tratamiento será permitido únicamente para fines públicos o si se cuenta con el consentimiento expreso del titular.

(...).

Lo expuesto significa que la Ley N° 8968 y su reglamento no aplican cuando concurre alguna de las circunstancias señaladas, a saber: **a.)** la ausencia de bases de datos personales o, aunque estas existan, cuando las mismas no estén destinadas a la comercialización o difusión de la información; **b.)** la concurrencia de un interés público que justifique soslayar la defensa del manejo de la información personal; **c.)** en cuanto a datos sensibles, cuando estos hayan sido publicados por la persona o su tratamiento sea necesario para (1) salvaguardar el interés vital de la persona o un tercero, (2) el desarrollo de actividades legítimas (siempre que los datos no se comuniquen a terceros sin el consentimiento de la persona), (3) el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, (4) la prevención, diagnóstico o tratamiento médico o sanitario, siempre que dicho servicio sea realizado por personal del área

de salud sujeto a secreto profesional o propio de su función, o por otras personas igualmente sujetos a una obligación de confidencialidad, y; **d.**) respecto a datos personales de acceso restringido, cuando su procesamiento sea para atender fines públicos o cuente con el consentimiento expreso de la persona interesada.

## **2.1. El Reglamento Para el Tratamiento de los Datos Personales Contenidos en las Bases de Datos de Acceso Público del Poder Judicial.**

Aparte de lo expuesto, para atender las consultas formuladas por la Dirección Ejecutiva debe tenerse presente el contenido del Reglamento ara el Tratamiento de los Datos Personales Contenidos en las Bases de Datos de Acceso Público del Poder Judicial (Circular N° 176-2024, publicada en el Boletín Judicial N° 161, del 02 de septiembre de 2024), que regula el uso y procesamiento de la información personal recopilada en las bases de datos de acceso público administradas por el Poder Judicial.

**Artículo 2.- Ámbito de aplicación.** Las normas contenidas en este reglamento se aplicarán al tratamiento que se dé a los datos personales que figuran en las bases de datos de acceso público del Poder Judicial, sin distinción de la materia y con independencia de si los respaldos son físicos o electrónicos, escritos u orales, de conformidad a lo establecido en la Ley de Protección de Datos vigente.

Las bases de datos internas o domésticas se registrarán por lo dispuesto en la normativa especial que las regule, sin perjuicio de la vinculación que para ellas pueda tener la ley N°8968 cuando fungen como respaldo de bases de datos de acceso público.

En el caso de las bases de datos que contienen información de uso exclusivo de personas funcionarias judiciales o las partes intervinientes en un proceso o trámite, pero que también contienen otra de naturaleza pública, deberá aplicarse lo dispuesto en este reglamento respecto al segundo tipo de información.

Según ese Reglamento, el Poder Judicial y su personal son responsables del almacenamiento y procesamiento de la información recibida por disposición constitucional o legal, así como de la información entregada por las personas usuarias del sistema de administración de justicia. El artículo 36 del reglamento citado establece que el Poder Judicial es el custodio de la información requerida a las personas usuarias y, a la vez, el responsable de guardar, reservar y proteger la información sensible, incluso cuando realice operaciones de tratamiento de datos, dentro de las que se encontraría la emisión de comunicados judiciales.

Además, agrega, toda persona servidora judicial es responsable por el tratamiento de los datos que deba gestionar en cumplimiento de sus funciones. Tal disposición impone a todas las oficinas judiciales y al funcionariado judicial el deber genérico de proteger la información

personal, sensible y de acceso restringido, que debe gestionar durante el ejercicio de sus funciones, independientemente de quien haya emitido o tratado previamente esos datos. Esta es la norma aplicable al caso de la Dirección Ejecutiva.

**Artículo 36. De la responsabilidad.** El Poder Judicial es custodio de la información que ha solicitado a las personas usuarias, por lo que, es responsable de guardar reserva, proteger datos o informaciones sensibles de terceros, a fin de tutelar los derechos de las personas usuarias de quienes recibe y produce información de la relación del servicio público justicia que brinda.

Asimismo, toda persona servidora judicial es responsable por el tratamiento que realice sobre los datos que, con ocasión de sus respectivas funciones, haga.

Como parte de los deberes derivados de la responsabilidad antes descrita, la institución, a través de su personal, debe proteger los datos personales contenidos en resoluciones judiciales o documentos administrativos que permitan identificar a una persona, cuando, sobre esa persona, consten datos de acceso restringido o datos sensibles.

**Artículo 25.- Datos que deben protegerse.** Deberán anonimizarse, previo a cualquier publicación, todos aquellos datos personales contenidos en resoluciones judiciales o documentos administrativos que permitan identificar a una persona sobre la que consten datos sensibles o de acceso restringido.

Los datos sensibles se conservarán con el fin de mantener la historia y facilitar la investigación jurídica, así como para rescatar temas relacionados con derechos humanos, género, violencia doméstica, accesibilidad, entre otros; no obstante, no se podrán revelar los datos personales que permitan identificar a los titulares de la información sensible.

Los datos de acceso restringido, tales como números de teléfono privados, correos electrónicos personales, dirección exacta del domicilio, cuentas bancarias y cualquier otro que la ley o disposiciones constitucionales cataloguen como tal, lo que se anonimizará será el dato restringido específico.

En aquellos casos en los que datos sensibles o de acceso restringido consten en imágenes insertadas en el documento o resolución, éstas deberán sustituirse a efectos de no vulnerar la autodeterminación informativa del titular de los datos.

Dicha protección se extiende a las informaciones que, por su naturaleza u origen, requieren una protección especial. Se trata de datos de personas menores de edad, con discapacidad, víctimas de acoso sexual o laboral, víctimas de delitos sexuales o violencia doméstica, en condiciones de vulnerabilidad, con protección legal especial, así como personas actoras, demandadas, ofendidas, testigos o imputadas en procesos penales, penales juveniles, de familia, violencia doméstica y pensiones alimentarias. Además, debe protegerse el

almacenamiento y tratamiento de datos confidenciales, privados, referentes al domicilio de las personas y sus números telefónicos privados. También, debe brindarse protección a los datos de las personas indígenas o que involucren derechos colectivos de los pueblos indígenas que consten en peritajes antropológicos.

**Artículo 28.- Datos que requieren especial atención.** Además de lo dispuesto en este reglamento sobre datos sensibles y de acceso restringido, se deberá prestar especial atención y realizar la anonimización correspondiente cuando se trate de datos:

1. De personas menores de edad, incluyendo situaciones en las que la persona era menor de edad, aunque ya no lo sea.
2. De personas con discapacidad.
3. De víctimas de acoso sexual o laboral y víctimas de delitos sexuales o violencia doméstica.
4. De partes o intervinientes procesales que estén en condición de vulnerabilidad o que tengan una protección procesal especial derivada de una norma legal.
5. De partes o intervinientes procesales cuya divulgación de datos permita identificar a una persona respecto a la que se deban anonimizar datos.
6. Que, en virtud de disposiciones legales o de rango superior vinculantes, tengan carácter confidencial o privado.
7. Que revelen direcciones de residencia, números de teléfono privados y otros de igual naturaleza cuyo tratamiento pueda afectar los derechos y los intereses de la persona titular, así como las fotografías de personas.
8. No podrán publicarse datos que permitan identificar a las personas actoras, demandadas, ofendidas, testigos o imputadas, en procesos penales, penales juveniles, de familia, violencia doméstica y pensiones alimentarias. Cuando en resoluciones de materias distintas a las señaladas, se vincule a una persona con un proceso de esa naturaleza, se deberá aplicar la protección respecto a esa persona en particular.
9. Los datos de personas indígenas o que involucren derechos colectivos del pueblo indígena que consten en peritajes antropológicos.
10. Los datos agregados a bases de datos anonimizadas sobre poblaciones en condición de vulnerabilidad pueden ser tratadas y divulgadas, siempre y cuando, se establezcan las garantías oportunas para salvaguardar los derechos contemplados en la legislación.

De conformidad con el Reglamento en estudio, para implementar las garantías previstas en la Ley N° 8968 y su reglamento, así como el reglamento de protección de datos

emitido por el Poder Judicial, la institución debe contar con una Oficialía de Protección de Datos, encargada de velar por la implementación y cumplimiento de la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales y su reglamento, así como de la reglamentación acá analizada.

**Artículo 13.- Oficialía de Protección de Datos del Poder Judicial.** El Poder Judicial contará con una oficina encargada de velar por la implementación y cumplimiento efectivo de la normativa, políticas y procedimientos relacionados con la protección de datos.

Dicha oficina estará a cargo de un Oficial de Protección de Datos quien, además de las funciones que le atribuya la autoridad institucional competente, deberá:

- a) Brindar información y asesoramiento normativo sobre el tema de Protección de Datos.
- b) Supervisar el cumplimiento normativo, de políticas y procedimientos de tratamiento de datos personales en bases de datos de acceso público del Poder Judicial.
- c) Cooperar y ser el enlace con la autoridad de control de la Protección de Datos (PROHAB).
- d) Atender a las personas interesadas e intermediarias en casos de reclamación de la Protección de los Datos.
- e) Elaborar e implementar un programa de control de riesgos respecto al tratamiento de datos personales.
- f) Verificar la implementación transversal de las disposiciones de tratamiento de datos personales en el Poder Judicial.
- g) Promover una cultura institucional de protección de datos.
- h) Mantener un inventario de las distintas bases de datos de acceso público del Poder Judicial.
- i) Verificar que cada base de datos de acceso público tenga formalmente designadas tanto una persona responsable como a las personas encargadas, así como que estén ejerciendo sus funciones de manera activa.
- j) Cualquier otra función relacionada con la Protección de Datos que le designe la Corte Suprema de Justicia.

La Oficialía estará bajo la dirección del órgano que la Corte Suprema de Justicia designe y dependerá del Consejo Superior del Poder Judicial, para efectos de dirección y jerarquía en lo que corresponde a sus competencias.

En caso de no contar con presupuesto suficiente para implementar la oficina correspondiente, las competencias descritas en el presente artículo podrán asignarse temporalmente por la Corte Suprema de Justicia a un órgano existente al momento de vigencia del presente reglamento.

Además, la institución debe contar con personal dedicado a identificar y proteger datos. Respecto a la persona protectora de datos, el reglamento la define como aquella designada por los despachos y oficinas judiciales para realizar la protección material de datos, previo a su publicación o transmisión a terceras personas, anonimizando la información cuando consten datos sensibles o de acceso restringido.

**Artículo 10.- Persona protectora de datos.** Son personas responsables de proteger datos personales, aquellas encargadas de anonimizar datos cuando consten datos sensibles o de acceso restringido.

**Artículo 11.- Obligaciones de las personas protectoras de datos.**

Son obligaciones de las personas protectoras de datos, las siguientes:

a. Anonimizar los datos que le sean alertados por las personas identificadoras de conformidad con los lineamientos vigentes. No obstante, en aquellos casos que la persona protectora de datos detecte información que considera debe protegerse; sin embargo, no le fue así alertado, hará la observación a la persona identificadora correspondiente, para que analice nuevamente el tema y se pronuncie de forma definitiva en el plazo de dos días.

De no recibirse respuesta, la persona encargada de la anonimización aplicará su criterio, siempre en estricto apego de lo normado en este reglamento y demás instrumentos jurídicos, pero ello no relevará de la responsabilidad correspondiente a quien omitió identificar un dato y/o pronunciarse respecto a las observaciones hechas.

El procedimiento antes indicado no será necesario si la falta de alerta está relacionada con una causal de mera constatación, como lo es que consten datos de personas menores de edad, se trate de asuntos de familia o violencia doméstica, etc.; no obstante, cuando exista margen de interpretación o duda, deberá procederse según los términos indicados.

b. Remitir solicitud escrita a la Dirección de Tecnología de la Información y Comunicaciones cuando deba proteger los datos personales en la base de datos que el despacho u oficina tenga a su cargo y posterior a la modificación deberá verificar la correcta protección de la información.

Implementar las medidas de seguridad y control interno que correspondan, así como, cumplir con lo dispuesto en la Ley de Protección de la Persona frente al Tratamiento de sus datos personales, el Reglamento institucional y demás disposiciones aplicables.

- c. Publicar las resoluciones judiciales y documentos administrativos, cuando corresponda.
- d. Guardar confidencialidad respecto de los datos personales tratados.
- e. Abstenerse de transferir, difundir o usar los datos sensibles o de acceso restringido para fines distintos a los autorizados.
- f. Velar por el cumplimiento de este reglamento y demás normas relacionadas.

Interesa ahondar en la figura de la persona identificadora de datos. Esta es aquella designada por los despachos y las oficinas judiciales para revisar los documentos emitidos o tratados por esas instancias, e identificar los datos que deban ser objeto de protección y, cuando corresponda, emitir las alertas correspondientes. Según el numeral 8 del reglamento examinado, son personas identificadoras de datos sensibles o de acceso restringido quienes emitan o traten resoluciones judiciales, documentos administrativos o cualquier otro conjunto estructurado de información que sea de acceso público.

Entre los deberes de esas personas destacan la identificación de datos sensibles o de acceso restringido presentes en los documentos bajo su gestión, así como la emisión de constancias (o alertas) sobre aquellos que deben ser anonimizados, indicado el motivo de su protección. Además, cuando detecten la concurrencia de datos que debían ser protegidos, pero no lo fueron, remitirán esos documentos al despacho o a la persona protectora de datos que corresponda, para su debido tratamiento y anonimización o etiquetado.

**Artículo 8.- Personas identificadoras de datos.** Son personas identificadoras de datos sensibles o de acceso restringido, todas las personas funcionarias que emitan resoluciones judiciales, documentos administrativos o cualquier otro conjunto estructurado de información que sea de acceso público, o bien, que sin ser quienes los emiten, sean designados formalmente por la coordinación o jefatura de un despacho u oficina en particular para efectuar la labor de identificación de datos.

**Artículo 9.- Obligaciones de las personas identificadoras de datos.**

Toda persona identificadora de datos deberá:

- a) Identificar si en las resoluciones judiciales (orales o escritas), documentos administrativos (documentos escritos, videos o audio) o cualquier otro conjunto estructurado de información a su cargo, existen datos sensibles o de acceso restringido que deban ser anonimizados de acuerdo con la normativa vigente.
- b) Dejar constancia de cuáles datos deben ser anonimizados y el motivo por el cual son objeto de protección. En casos donde el fundamento no se desprenda de este reglamento, indicar la norma jurídica que lo respalda. Lo anterior debe quedar por escrito en la casilla electrónica o archivo físico que a los efectos se disponga.

- c) Remitir los documentos al despacho o a la persona protectora de datos que realizará la protección material. En casos donde la persona identificadora sea la misma que la que debe realizar la protección material, igualmente se deberá dejar constancia del motivo que justifica la anonimización.
- d) Utilizar, de acuerdo con sus atribuciones, las herramientas tecnológicas que facilite la Dirección de Tecnologías de la Información y Comunicaciones, con la finalidad de establecer las medidas de seguridad que garanticen la confidencialidad, disponibilidad e integridad de la información que custodia el Poder Judicial.
- e) Guardar confidencialidad respecto de los datos personales tratados.
- f) Velar por el cumplimiento de este reglamento y demás normas relacionadas.

Acorde con la normativa referida, los despachos y las oficinas judiciales que participen en la recolección y tratamiento de datos personales deben contar con personas identificadoras y protectoras de datos, a efecto de revisar el contenido de los documentos que emiten o procesan, con la finalidad de garantizar el equilibrio necesario entre el ejercicio de la función judicial, el derecho de acceso a la información pública, el derecho a la autodeterminación informativa y la privacidad de las personas.

A partir de lo expuesto, le corresponde al aplicador del derecho o a la administración activa, analizar la situación de hecho sometida a su conocimiento, para determinar si se encuentra frente a una circunstancia que amerite aplicar las salvaguardas y procedimientos establecidos en la Ley para la Protección de la Persona Frente al Tratamiento de sus Datos Personales y sus distintas reglamentaciones o, si por el contrario, se encuentra ante una situación excepcionada en esos cuerpos normativos.

### **3. Las consultas formuladas por la Dirección Ejecutiva.**

Seguidamente se contesta en forma específica las preguntas formuladas por la Dirección Ejecutiva, exponiendo las consideraciones jurídicas correspondientes.

**3.1.** *Cuando corresponda, ¿cuál sería la instancia que debe valorar el contenido de las publicaciones, bajo el contexto de la Ley de Protección de Datos. Cabe señalar que esta Dirección Ejecutiva no tiene competencia ni recurso humano para modificar el contenido de las publicaciones, ya que responden a una orden de la Autoridad Judicial.*

Tal y como se expuso anteriormente, las salvaguardas y los procedimientos previstos en la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales y su reglamento, se aplican a la recolección, tratamiento y utilización de información personal compilada en bases de datos estructuradas y destinadas a la comercialización, difusión o distribución de esa información. Dentro de ese ámbito quedan incluidas la recopilación y tratamiento de datos personales de información constante en bases de datos de acceso público administradas por el Poder Judicial, según se desprende del artículo 2 del Reglamento para el Tratamiento de los Datos Personales Contenidos en las Bases de Datos de Acceso Público del Poder Judicial (Circular N° 176-2024, publicada en el Boletín Judicial N° 161, del 02 de septiembre de 2024).

Dicha normativa no puede implementarse en ausencia de una base de datos, ni cuando se está frente un archivo informativo de uso personal, doméstico o interno, es decir, en caso de existir una base de datos personales cuyo contenido no ha sido recopilado para la comercialización, difusión o distribución de la información.

Corresponde verificar si la información consignada en los comunicados judiciales se encuentra dentro de los supuestos cubiertos por la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales y sus reglamentaciones. Los comunicados judiciales son generados por los juzgados y tribunales del Poder Judicial, en el ejercicio de la función jurisdiccional. La información consignada en esos avisos es información personal e información de bienes materiales. Generalmente, dicha información se obtiene de las bases de datos administradas por el Poder Judicial, las cuales han sido conformadas con la información suministrada por las personas usuarias del sistema de administración de justicia, ya sea por disposición legal o por petición expresa de la autoridad judicial.

En términos genéricos, lo expuesto evidencia que el Poder Judicial cuenta con recopilaciones de datos personales. Esas compilaciones pueden ser difundidas, distribuidas o comunicadas a terceros, por disposición legal u orden judicial, tal y como sucede en el caso de las publicaciones de comunicados judiciales (p.ej.: edictos y citaciones). Ello implica que la recopilación, el tratamiento y la utilización de la información personal recolectada por el Poder Judicial, así como las bases de datos administradas por la institución, deben respetar lo dispuesto en la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales y sus reglamentaciones; sin perjuicio de los establecido en los numerales 5 y 8 del decreto legislativo indicado, 5, 14 del Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, 4.a y 29 del Reglamento para el tratamiento de los datos personales contenidos en bases de datos de acceso público del Poder Judicial y la demás normativa aplicable al tratamiento de datos e informaciones personales, cuya aplicación

procurará garantizar el equilibrio del derecho a la autodeterminación informativa con el acceso a la información pública de carácter judicial.

Respecto a la persona(s) o instancia(s) responsable(s) de implementar el contenido de la Ley N° 8968 y sus reglamentaciones en el Poder Judicial, se debe retomar lo señalado en el Reglamento Para el Tratamiento de los Datos Personales Contenidos en las Bases de Datos de Acceso Público del Poder Judicial. En términos generales, el Poder Judicial es responsable de la información que recopila y procesa (artículo 36 del reglamento), y le corresponde a la Oficialía de Protección de Datos del Poder Judicial procurar la implementación y el cumplimiento efectivo de las políticas y la normativa referida a la protección de datos personales (artículos 3.N y 13 del reglamento).

Sin perjuicio de lo anterior, la aplicación práctica e inmediata de las normas referidas a la protección de datos personales le incumbe a todos los despachos y oficinas del Poder Judicial (párrafo primero del artículo 36 del reglamento), quienes deben actuar por medio de sus funcionarios y funcionarias (párrafo segundo del artículo 36 del reglamento), particularmente a través de quienes resulten designados como identificadores (artículos 3.T, 8 y 9 del reglamento) y protectores (artículos 3.W, 10 y 11 del reglamento) de datos.

Recordemos que el artículo 2 del reglamento indica que esa normativa (y la Ley N° 8968) debe ser aplicada por los despachos y oficinas judiciales, sobre las operaciones de tratamiento de datos personales que figuren en las bases de datos del Poder Judicial y que sean de acceso público.

Partiendo de lo expuesto, según la normativa analizada, se infiere que, en un primer momento, la instancia encargada de verificar el ajuste del contenido de los comunicados judiciales con lo dispuesto en la Ley N° 8968 y sus reglamentaciones, es la oficina judicial emitente del documento a publicar, por medio de su personal.

Sin menoscabo de lo dicho, aunque la labor realizada por la Dirección Ejecutiva sea recibir documentos debidamente autorizados por órganos jurisdiccionales y, posteriormente, publicarlos en el Boletín Judicial, lo cierto es que, de acuerdo con el artículo 36 del reglamento interno de protección de datos, esa oficina y su personal, en un segundo momento, también son responsables por el tratamiento de los datos personales recibidos en razón de sus funciones (como órgano Director y Coordinador del Boletín Judicial).

Cierto es que los comunicados judiciales no pueden ser alterados por el personal de la Dirección Ejecutiva, pues ello podría constituir una infracción al principio de independencia de la persona juzgadora, así como una actuación irregular, con consecuencias administrativas,

penales y civiles; sin embargo, en ejercicio de sus deberes como instancia encargada de procesar datos personales, la Dirección Ejecutiva deberá revisar el contenido de los documentos remitidos para ser publicados en el Boletín Judicial y, en caso de identificar datos que no fueron debidamente protegidos por sus emisores, generará las alertas correspondientes y aplicará el trámite previsto en el reglamento, devolviendo esos documentos a la oficina remitente, para que se aplique correctamente las reglas de protección de datos.

**3.2.** *¿Es necesario que en este tipo de publicaciones del Boletín Judicial se despersonalicen los textos por parte de las Autoridades Judiciales? Debe tomarse en cuenta que, de suprimirse datos como nombre o calidades, podría no lograrse el cometido de la publicación al impedirse la identificación de la persona a la que refiere la publicación.*

En atención a los principios y normas que rigen el ejercicio de la función jurisdiccional y la labor de las personas juzgadoras, esta Dirección estima inapropiado afirmar o negar que los despachos judiciales deban despersonalizar (anonimizar o etiquetar) los comunicados judiciales, antes de remitirlos a la Dirección Ejecutiva para su publicación en el Boletín Judicial.

Lo correcto es reiterar que, de conformidad con lo establecido en la normativa analizada, cuando la autoridad judicial lo estime pertinente, ella deberá adoptar las medidas pertinentes para dar cumplimiento a lo dispuesto en la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales y sus reglamentaciones, prestando especial atención al reglamento Para el Tratamiento de los Datos Personales Contenidos en las Bases de Datos de Acceso Público del Poder Judicial.

A lo anterior se debe adicionar que, en el ejercicio de sus funciones, los despachos judiciales y las personas juzgadoras tendrán que tomar en cuenta lo dispuesto en el artículo 36 del Reglamento para el tratamiento de los datos personales contenidos en bases de datos de acceso público del Poder Judicial, el cual responsabiliza a la institución por la gestión (en sentido amplio) de los datos que administra y a las personas servidoras judiciales por el tratamiento de los datos utilizados en el cumplimiento de sus deberes.

Asimismo, deberán considerar lo establecido en los artículos 8, 9, 10 y 11 del citado reglamento. Conforme a esas normas, las personas emisoras o procesadoras de resoluciones judiciales y documentos administrativos con informaciones personales tiene la obligación de identificar los datos sensibles o de acceso restringido que deban ser anonimizados de acuerdo con la normativa vigente. Además, deben dejar constancia de cuáles datos deben ser anonimizados y el motivo de esa protección. Adicionalmente, tienen que remitir los

documentos al despacho o a la persona protectora de datos, quien realizará la protección material de la información.

**3.3.** *Debería considerarse por parte de las instancias que remiten los textos a publicar el principio de minimización de datos.*

El principio aludido procura minimizar la recolección y el tratamiento de información personal, promoviendo medidas organizativas y técnicas tendientes a garantizar la recolección de los datos personales estrictamente necesarios para la finalidad atendida, así como el tratamiento mínimo de esa información, limitando su almacenamiento, conservación y accesibilidad.

Partiendo de lo anterior, resulta factible afirmar que las autoridades judiciales deberán tomar en cuenta los alcances del principio de minimización de datos para confeccionar los comunicados judiciales, siempre que dicha labor se realice en equilibrio con las exigencias legales impuestas para el trámite y resolución de los procesos judiciales.

**3.4.** *En este supuesto de despersonalización, cuál sería la función de la Dirección Ejecutiva, pues se trata de temas jurisdiccionales sobre los cuales no se tiene competencia ni conocimiento.*

Tal y como se dijo anteriormente, de conformidad con los artículos 8, 9 y 36 del Reglamento para el tratamiento de los datos personales contenidos en bases de datos de acceso público del Poder Judicial, en el caso de los comunicados judiciales remitidos para publicarse en el Boletín Judicial, la Dirección Ejecutiva deberá revisar su contenido, a fin de identificar datos sensibles, de acceso restringido o que por su naturaleza o características no puedan ser difundidos, y que no hayan sido despersonalizados, anonimizados o etiquetados.

En caso de identificar la existencia de datos que cumplan con las características apuntadas, la Dirección Ejecutiva levantará una constancia, en la que consignará los datos que estima deben ser protegidos, con la fundamentación correspondiente. Luego, comunicará esa circunstancia al despacho o a la oficina respectiva, para que esta última realice la protección efectiva de la información.

## **4. Conclusiones y recomendaciones.**

### **4.1 Conclusiones.**

De conformidad con lo expuesto y en atención a la consulta planteadas por la Dirección Ejecutiva, se concluye lo siguiente:

- 4.1.1** La recopilación, protección y el tratamiento de datos personales almacenados en bases de datos de acceso público del Poder Judicial se encuentran reguladas en la Ley de protección de la persona frente al tratamiento de sus datos personales (Ley N° 8968), el Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales (Decreto Ejecutivo N° 37554-JP) y el Reglamento Para el Tratamiento de los Datos Personales Contenidos en las Bases de Datos de Acceso Público del Poder Judicial (Circular N° 176-2024, publicada en el Boletín Judicial N° 161, del 02 de septiembre de 2024).
- 4.1.2** El artículo 2 del Reglamento Para el Tratamiento de los Datos Personales Contenidos en las Bases de Datos de Acceso Público del Poder Judicial establece que la normativa referida a la recopilación, protección y tratamiento de información personal debe ser aplicada por los despachos y oficinas judiciales, sobre las operaciones de tratamiento de datos personales que figuren en las bases de datos del Poder Judicial y que sean de acceso público.
- 4.1.3** El párrafo primero del numeral 36 del Reglamento Para el Tratamiento de los Datos Personales Contenidos en las Bases de Datos de Acceso Público del Poder Judicial indica que la institución es responsable de custodiar la información requerida a las personas usuarias; así como de proteger la información sensible, de acceso restringido o aquella que por sus características no pueda ser divulgada sin afectar la privacidad de la persona usuaria, incluso cuando realice operaciones de tratamiento de datos. Lo anterior, con las salvedades previstas en los artículos 5 y 8 de la Ley N° 8968, 5 y 14 del Decreto Ejecutivo N° 37554-JP, 4.a y 29 del Reglamento Para el Tratamiento de los Datos Personales Contenidos en las Bases de Datos de Acceso Público del Poder Judicial y otra normativa aplicable al tratamiento de datos e informaciones personales.
- 4.1.4** El párrafo segundo del ordinal 36 del Reglamento Para el Tratamiento de los Datos Personales Contenidos en las Bases de Datos de Acceso Público del Poder Judicial estipula que las personas servidoras judiciales son responsables por el tratamiento de los datos que deba gestionar en cumplimiento de sus funciones.
- 4.1.5** Los artículos 3.T, 8 y 9 del Para el Tratamiento de los Datos Personales Contenidos en las Bases de Datos de Acceso Público del Poder Judicial instituyen en el Poder Judicial la figura de la persona identificadora de datos, quien será la designada por los despachos y las oficinas judiciales para revisar los documentos emitidos o tratados por esas instancias, e identificar los datos que deban ser objeto de protección.

- 4.1.6** A la persona que ejerce la función de identificar de datos le corresponde alertar sobre la falta de protección de datos personales que debían ser resguardados y levantar la constancia correspondiente. Además, comunicar al despacho o a la oficina emitente (o remitente) la falta de protección de datos, para que esta segunda proceda a realizar la protección material de la información.
- 4.1.7** Conforme a lo expuesto, en el caso de los comunicados judiciales, dado que la Dirección Ejecutiva no los emite pero forma parte de la cadena de tratamiento de datos personales constantes en las bases informativas de los despachos y oficinas judiciales, le corresponde ejercer la función de identificar datos no protegidos y, cuando corresponda, comunicar la falta detectada a la oficina emitente del documento, para que esta última adopte las medidas necesarias para proteger la información como corresponda.

## **4.2. Recomendaciones.**

Con base en las consideraciones anteriores, esta oficina realiza las siguientes recomendaciones:

- 4.2.1.** Se recomienda a la Dirección Ejecutiva proponer al Consejo Superior que las comisiones jurisdiccionales coordinen con los despachos judiciales el estudio y la implementación de las regulaciones legales e infra legales de protección de datos personales, con énfasis en el Reglamento Para el Tratamiento de los Datos Personales Contenidos en las Bases de Datos de Acceso Público del Poder Judicial.
- 4.2.2.** En atención a la emisión del Reglamento Para el Tratamiento de los Datos Personales Contenidos en las Bases de Datos de Acceso Público del Poder Judicial se recomienda a la Dirección Ejecutiva coordinar con la Escuela Judicial (y demás instancias que corresponda), la elaboración de un curso dirigido al personal administrativo, que participa en el tratamiento y protección de datos, a fin de que pueda cumplir con las funciones que derivan de esa legislación; asimismo, la Dirección Ejecutiva deberá procurar que su personal realice y apruebe este curso.

Atentamente,

**Licda. Laura Moreira Barrantes**  
**Asesora Jurídica**

**Lic. Luis Abner Salas Muñoz**  
**Asesor Jurídico**

**MSc. Rodrigo Alberto Campos Hidalgo**



**Director Jurídico**

Ref. 1015-2024.-