San José, 19 de mayo del 2022.

Criterio N° DJ-AJ-C-212-2022

Máster Roxana Arrieta Meléndez
Directora de Gestión Humana

Estimada señora:

En atención al oficio **N° PJ-DGH-SGD-145-2021** de 26 de octubre del 2021 de la Dirección de Gestión Humana, y recibido el 18 de noviembre en curso en esta Dirección Jurídica, le remito el informe solicitado.

I. Antecedente de la gestión:

Mediante oficio **N° PJ-DGH-SGD-145-2021** de 26 de octubre del 2021 de la Dirección de Gestión Humana, se realizó la solicitud que se transcribe literalmente a continuación:

> "Con ocasión de los resultados de la población judicial, durante el periodo de evaluación 2020, se acude a su despacho, con el propósito de disponer de un criterio jurídico respecto de la determinación de si la información que conforma el comprobante del resultado final de la evaluación, en particular las justificaciones del resultado otorgado por la persona evaluadora en el apartado de competencias, es considerado de naturaleza sensible, para la privacidad de la persona objeto de la evaluación del desempeño, esto por cuanto, a excepción de instancias de control, como la Inspección Judicial o una autoridad penal, se han presentado solicitudes para uso de la información contenida en el comprobante del resultado final por parte de otros subprocesos de la Dirección de Gestión Humana, pero no se dispone de un criterio para determinar cuáles de los apartados que conforman dicho comprobante podrían considerarse como públicos o sensibles, teniendo presente que el mismo Reglamento, en su artículo 21, dispone:
>
> "-Custodia de los resultados.
> Los resultados del S.I.E.D. obtenidos por cada persona evaluada serán enviados al expediente electrónico, que administra la Dirección de Gestión Humana; y se considerarán públicos, salvo aquellos datos cuya confidencialidad debe ser resguardada de acuerdo con la Ley de protección de la persona frente al tratamiento de sus datos personales…"
>
> La anterior solicitud, se requiere para evitar el riesgo de posibles demandas por compartir las justificaciones que haya dispuesto la persona evaluadora para la persona

evaluada, dentro del ámbito de la confianza entre ambas partes." (El subrayado no es del original)

II. Análisis:

De previo a la exposición del criterio, se estima oportuno señalar que, en aplicación de lo dispuesto en el Reglamento de la Dirección Jurídica del Poder Judicial, contenido en la circular 251-2017, aprobado por la Corte Plena de la Corte Suprema de Justicia en el artículo XXXIII de la sesión número 47-14, celebrada el día 06 de octubre de 2014, debe entenderse que esta Dirección cumple funciones de asesoría jurídica en términos generales respecto de los alcances de la legislación vigente y no sustituye la valoración de cada caso concreto que legalmente compete al órgano administrativo decisor consultante, en virtud de lo cual, este acto constituye una orientación jurídica general sobre la base de la información y solicitud que plantea ese órgano colegiado, sin que se prejuzgue o sustituya la capacidad de toma de decisiones que le compete a ese órgano consultante, como órgano administrativo superior del Poder Judicial.

Es así como frente a la presente solicitud de criterio, hay que recordar que la labor de la asesoría legal en materia de criterios jurídicos, es orientar en los alcances legales del ejercicio administrativo, pero un límite legal y ético de quienes ejercen una adecuada asesoría jurídica, es no sustituir a los órganos competentes en el ejercicio de su decisión, sino tan solo ofrecer elementos para su valoración o de lo contrario, los órganos de decisión quedarían vaciados de su autoridad, sus competencias y responsabilidades y quedarían tan solo como simples repetidores o ejecutores de lo que el abogado diga, lo que haría que, en la práctica, sea el asesor jurídico quien ostente el poder institucional, a contrapelo de la decisión de la sociedad expresada en la legislación que otorga y deslinda las competencias públicas.

La gestión que se remite a esta Dirección Jurídica pretende determinar si la información que conforma el comprobante del resultado final de las evaluaciones del desempeño, en

particular las justificaciones del resultado otorgado por la persona evaluadora en el apartado de competencias, es considerada **datos de naturaleza sensible**, esto porque se han presentado solicitudes para uso de dicha información por parte de otros subprocesos de la Dirección de Gestión Humana.

Al respecto, es importante señalar que el artículo 24 de la **Constitución Política**, garantiza los derechos fundamentales a la intimidad, la inviolabilidad de los documentos privados, el secreto de las comunicaciones y el derecho de la autodeterminación informativa.

Debe considerarse que la protección de personas físicas en relación con el tratamiento de sus datos personales es un derecho fundamental que se encuentra reconocido con rango máximo en la mayoría de las Constituciones Políticas de los Estados Iberoamericanos, bajo la forma del **derecho de protección de datos personales o habeas data**, cuyo objeto es el de salvaguardar el poder de disposición y control que tiene toda persona física con respecto a la información que le concierne en contra de intrusiones ilegales o arbitrarias, fundamentalmente en atención al empleo de las tecnologías de la información y las comunicaciones que evolucionan vertiginosamente y cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana, siendo esto un gran desafío para la protección de este derecho.

Incluso es importante mencionar que, en algunos países Iberoamericanos, el Derecho a la protección de datos personales ha sido conceptualizado legislativa y jurisprudencialmente como un derecho de naturaleza distinta a los derechos a la vida privada y familiar, a la intimidad, al honor, al buen nombre y otros derechos similares, que en su conjunto garantizan el libre desarrollo de la personalidad de la persona física, hasta conformarse en un derecho autónomo, con características y dinámicas propias; no obstante, en nuestro país, aún sigue siendo un derecho derivado del Derecho a la Intimidad establecido en el artículo 24 de la Constitución Política.

Ahora bien, junto al derecho de protección de datos personales también podemos encontrar el **derecho de autodeterminación informativa**, el cual se puede definir como

aquella potestad que es inherente al ser humano, para ejercer el control sobre su información personal, en aquellos casos en que se pretenda ser compartida o publicada, siendo esta facultad un derecho fundamental que debe respetarse.

Por otro lado, el Derecho de toda persona a tener acceso a la información de interés público o incluso privado de ésta, que se encuentre en poder de la Administración, se encuentra consagrado constitucionalmente en nuestro ordenamiento jurídico. La norma que resulta aplicable es el artículo 30 **Constitucional**, la cual establece "*Se garantiza el libre acceso a los departamentos administrativos con propósitos de información sobre asuntos de interés público. Quedan a salvo los secretos de Estado.*"

En un estudio especial elaborado por la Organización de Estados Americanos, sobre el derecho de acceso a la información (2007), se indicó que "*El acceso a la información constituye una herramienta esencial para combatir la corrupción, hacer realidad el principio de transparencia en la gestión pública y mejorar la calidad de nuestras democracias, caracterizadas por una cultura de secretismo y por organismos públicos cuyas políticas y prácticas de manejo de la información no necesariamente están orientadas a facilitar su acceso a las personas (…)*"[1]

Es ese sentido, el efectivo acceso a la información permitirá exigir al Estado una adecuada prestación de los servicios públicos esenciales y con ello, mejorar la calidad de vida de los habitantes.

Es así como una de las funciones más importantes del Estado moderno es la del correcto manejo de la información que recibe y produce de la interacción con los administrados y, en ese sentido, el **Estado se constituye en un custodio y no el dueño** de esa información, razón por la cual, en materia de acceso a la información, más que derechos, los entes públicos tienen una

- [1] OEA, Estudio Especial Derecho de Acceso a la Información (2007), citado por MARÍN JIMÉNEZ (Jaínse), **Derecho de Acceso a la Información: alcances, límites y responsabilidades asociadas**, Arisol Consultores- Poder Judicial, capacitación realizada 9 y 10 de diciembre del 2014, página 7.

serie de deberes, obligaciones y responsabilidades muy amplias. En este sentido se ha señalado lo siguiente:

> "(…) El derecho a la información está en el corazón de la democracia. Sólo una ciudadanía bien informada puede contribuir de forma efectiva al proceso de toma de decisiones. La **participación democrática** depende de la posibilidad de los ciudadanos de acceder a la información que necesitan. El derecho a la información permite un diálogo entre el público y sus gobernantes, **cultiva la buena gobernanza y promueve la rendición de cuentas** al empoderar a los ciudadanos, los periodistas y la sociedad civil en general con la información que requieren para luchar contra la corrupción y actuar como vigilantes contra abusos por parte de las autoridades (…)
>
> (…) democratizar el acceso a la información, en particular la información en manos de entidades públicas, fomenta un clima político de apertura, transparencia y participación ciudadana. El derecho a la información se basa en que las **autoridades son simplemente los guardianes de la misma para la sociedad** pues la información es propiedad de esta última. Cuando la transparencia reemplaza los secretos y el poder se expone al escrutinio público, los abusos se pueden frenar, la opinión pública se puede incorporar y el Estado puede rendirle cuentas al interés público (…)".[2]

Por un lado, nos encontramos con importantes Principios como el de Publicidad, Transparencia y Rendición de Cuentas que condicionan el accionar del Estado; pero, por otro lado, nos encontramos que el derecho de acceso a la información no es absoluto sino relativo, pues **junto al acceso convive la obligación de guardar reserva, de proteger datos o informaciones sensibles de terceros, a fin de tutelar sus derechos**.

El acceso a la información y a la protección y resguardo de datos sensibles no son conceptos opuestos, es decir, no son excluyentes, sino que son dos obligaciones que se deben cumplir de manera simultánea y armónica.

---

[2] Toby Mendel, El Derecho a la información en América Latina, comparación Jurídica, UNESCO, 2009, oficina de Quito, citado por MARÍN JIMÉNEZ (Jaínse), Derecho de Acceso a la Información: alcances, límites y responsabilidades asociadas, Arisol Consultores- Poder Judicial, capacitación realizada 9 y 10 de diciembre del 2014, filminas 7/259 y 8/259.

La **Sala Constitucional** en reiteradas sentencias ha tratado el tema de la protección de datos resaltando el derecho consagrado en el artículo 24 de la **Constitución Política** que protege la intimidad de las personas. En la resolución N° 8672-2010 de las 9:36 horas del 14 de mayo de 2010, expone que los datos sensibles o nominativos que posea un órgano público no pueden ser de acceso irrestricto para terceras personas. Al respecto dijo:

> "El artículo 24 de la Constitución Política le garantiza a todas las personas una esfera de intimidad intangible para el resto de los sujetos de derecho, de tal forma que aquellos datos íntimos, sensibles o nominativos que un ente u órgano público ha recolectado, procesado y almacenado, por constar en sus archivos, registros y expedientes físicos o automatizados, no pueden ser accedidos por ninguna persona por suponer ello una intromisión o injerencia externa e inconstitucional. Obviamente, lo anterior resulta de mayor aplicación cuando el propio administrado ha puesto en conocimiento de una administración pública información confidencial, por ser requerida, con el propósito de obtener un resultado determinado o beneficio. En realidad, esta limitación está íntimamente ligada al primer límite intrínseco indicado, puesto que, muy, probablemente, en tal supuesto la información pretendida no recae sobre asuntos de interés público sino privado". (Énfasis suplido).

A mayor abundamiento, la **Sala Constitucional**, en la resolución N° 11.338-2003 de las 9:50 horas del 3 de octubre del 2003 reiteró la tesis expuesta en la resolución N° 4.847 de las 16:27 horas del 22 de junio de 1999, que en lo que interesa, señaló:

> "(…) *Es obvio, que el* ***acceso a la información*** *es un poderoso instrumento de progreso individual, y para el ejercicio de los derechos políticos y sociales. Pero también debe reconocerse que el progreso no significa que los ciudadanos deban quedar en situación de desventaja frente al Estado o a los particulares.* El nuevo derecho a la intimidad debe ponderar los intereses en relación, entre el legítimo interés de la sociedad a desarrollarse utilizando la información, como la también necesidad de proteger a la persona frente al uso arbitrario de sus datos personales. *La tutela a la intimidad implica, la posibilidad real y efectiva para el ciudadano de saber cuáles datos suyos están siendo tratados, con qué fines, por cuáles personas, bajo qué circunstancias, para que pueda ejercer el control correspondiente sobre la información que se distribuye y que lo afecta (arts. 24 de la Constitución y 13 inciso 1, de la Convención Americana de Derechos Humanos).* (…)" (Énfasis suplido)

Es decir, el Estado debe procurar colocar a disposición del público la información de la manera más actual y completa posible; sin embargo, debe observar límites como el resguardo de datos privados recopilados por la Administración conforme a la **Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales**, N° 8968 de 7 de julio del 2011.

En ese sentido, los artículos 1, 2, 3, 4, 5, 6, 8, 9, 10, 14, 30 y 31 de la **Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales**, establecen lo siguiente:

> ***"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."*
>
> ***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.*
>
> *[…]*
>
> **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.
>
> **b)** Datos personales: cualquier dato relativo a una persona física identificada o identificable.
>
> **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.

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.

f) Deber de confidencialidad: obligación de los responsables de bases de datos, personal a su cargo y del personal de la Agencia de Protección de Datos de los Habitantes (Prodhab), de guardar la confidencialidad con ocasión del ejercicio de las facultades dadas por esta ley, principalmente cuando se acceda a información sobre datos personales y sensibles. Esta obligación perdurará aun después de finalizada la relación con la base de datos.

g) Interesado: persona física, titular de los datos que sean objeto del tratamiento automatizado o manual.

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 registrase y qué tipo de tratamiento se les aplicarán.

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.

Artículo 4.- Autodeterminación informativa

Toda persona tiene derecho a la autodeterminación informativa, la cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales reconocidos en esta sección.

Se reconoce también la autodeterminación informativa como un derecho fundamental, con el objeto de controlar el flujo de informaciones que conciernen a cada persona, derivado del derecho a la privacidad, evitando que se propicien acciones discriminatorias.

Artículo 5.- Principio de consentimiento informado

1.- Obligación de informar

Cuando se soliciten datos de carácter personal será necesario informar de previo a las personas titulares o a sus representantes, de modo expreso, preciso e inequívoco:

a) De la existencia de una base de datos de carácter personal.

b) De los fines que se persiguen con la recolección de estos datos.

c) De los destinatarios de la información, así como de quiénes podrán consultarla.

d) Del carácter obligatorio o facultativo de sus respuestas a las preguntas que se le formulen durante la recolección de los datos.

e) Del tratamiento que se dará a los datos solicitados.

f) De las consecuencias de la negativa a suministrar los datos.

g) De la posibilidad de ejercer los derechos que le asisten.

h) De la identidad y dirección del responsable de la base de datos.

Cuando se utilicen cuestionarios u otros medios para la recolección de datos personales figurarán estas advertencias en forma claramente legible.

2.- Otorgamiento del consentimiento

Quien recopile datos personales deberá obtener el consentimiento expreso de la persona titular de los datos o de su representante. Este consentimiento deberá constar por escrito, ya sea en un documento físico o electrónico, el cual podrá ser revocado de la misma forma, sin efecto retroactivo.

No será necesario el consentimiento expreso cuando:

a) Exista orden fundamentada, dictada por autoridad judicial competente o acuerdo adoptado por una comisión especial de investigación de la Asamblea Legislativa en el ejercicio de su cargo.

b) Se trate de datos personales de acceso irrestricto, obtenidos de fuentes de acceso público general.

c) Los datos deban ser entregados por disposición constitucional o legal.

Se prohíbe el acopio de datos sin el consentimiento informado de la persona, o bien, adquiridos por medios fraudulentos, desleales o ilícitos.

Artículo 6.- Principio de calidad de la información. Solo podrán ser recolectados, almacenados o empleados datos de carácter personal para su tratamiento automatizado o manual, cuando tales datos sean actuales, veraces, exactos y adecuados al fin para el que fueron recolectados.

[…]

4.- Adecuación al fin. Los datos de carácter personal serán recopilados con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines. No se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando se establezcan las garantías oportunas para salvaguardar los derechos contemplados en esta ley. Las bases de datos no pueden tener finalidades contrarias a las leyes ni a la moral 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.

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.

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.

[…]

Artículo 10.- Seguridad de los datos

El responsable de la base de datos deberá adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a esta ley.

Dichas medidas deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual, para garantizar la protección de la información almacenada.

No se registrarán datos personales en bases de datos que no reúnan las condiciones que garanticen plenamente su seguridad e integridad, así como la de los centros de tratamiento, equipos, sistemas y programas.

Por vía de reglamento se establecerán los requisitos y las condiciones que deban reunir las bases de datos automatizadas y manuales, y de las personas que intervengan en el acopio, almacenamiento y uso de los datos.

Artículo 14.- Transferencia de datos personales, regla general

Los responsables de las bases de datos, públicas o privadas, solo podrán transferir datos contenidos en ellas cuando el titular del derecho haya autorizado expresa y válidamente tal transferencia y se haga sin vulnerar los principios y derechos reconocidos en esta ley.

Artículo 30.- Faltas graves

Serán consideradas faltas graves, para los efectos de esta ley:

a) Recolectar, almacenar, transmitir o de cualquier otra forma emplear datos personales sin el consentimiento informado y expreso del titular de los datos, con arreglo a las disposiciones de esta ley.

[…]

c) Recolectar, almacenar, transmitir o de cualquier otro modo emplear datos personales para una finalidad distinta de la autorizada por el titular de la información.

[…]

Artículo 31.- Faltas gravísimas

Serán consideradas faltas gravísimas, para los efectos de esta ley:

a) Recolectar, almacenar, transmitir o de cualquier otra forma emplear, por parte de personas físicas o jurídicas privadas, datos sensibles, según la definición prevista en el artículo 3 de esta ley.

[…]

c) Revelar información registrada en una base de datos personales cuyo secreto esté obligado a guardar conforme la ley.

[…]"

Como puede observarse de la normativa antes transcrita, el objetivo de dicha ley es asegurar en todo momento el respeto al **derecho fundamental de autodeterminación informativa** derivado del derecho a la intimidad (artículo 24 de la **Constitución Política**), el

cual garantiza un trato legítimo y un estricto control sobre el flujo de informaciones concernientes a una persona, cubriendo bases de datos que mantienen los entes públicos y los sujetos privados. Es decir, el derecho de autodeterminación informativa forma parte de las garantías a la personalidad (intimidad, petición y acceso a la información).

La autodeterminación informativa, consiste en el derecho que tiene toda persona física a conocer lo que conste sobre ella en cualquier base de datos pública o privada, el fin para el cual está siendo utilizada o si está siendo empleada para un fin distinto del autorizado o del que legalmente puede cumplir.

Uno de los más importantes principios del derecho a la autodeterminación es el **Principio de Consentimiento Informado**, el cual consiste en la necesidad de informar previamente a las personas titulares, cuando se les soliciten datos de carácter personal, de forma expresa, precisa e inequívoca, de la existencia de la base de datos, cuáles son los fines que se persiguen con su recolección, los destinatarios y quiénes podrían consultar esa información, sobre el carácter obligatorio o facultativo de las respuestas a las preguntas que se formulen durante la recolección de los datos y del tratamiento que se le dará a esa información, de las consecuencias de la negativa de brindar los datos, también sobre la posibilidad de ejercer los derechos que le asisten al interesado, así como de la identidad y dirección del responsable de la base de datos.

En ese sentido, quien recopile los datos personales deberá obtener obligatoriamente el consentimiento expreso de la persona titular, siendo prohibida la recolección de datos sin el consentimiento informado de la persona titular. El consentimiento debe constar por escrito.

De esta manera, la institución se encuentra legitimada a tratar datos personales en su posesión, en el tanto cuente con el consentimiento del titular.

No obstante, dicha normativa señala que no será necesario el consentimiento expreso cuando exista una orden dictada por la autoridad judicial competente, o se trate de datos

personales de acceso irrestricto, o bien, los datos deban ser entregados por disposición constitucional o legal.

También, de acuerdo con el **Principio de Calidad de Información**, solamente pueden ser recolectados, empleados o almacenados datos de carácter personal para su tratamiento automatizado o manual, adecuados al fin para el que fueron recolectados, sin poder ser tratados después, de manera incompatible con los fines.

Asimismo, en el artículo 8 de dicha Ley, claramente se definen las **excepciones** a la citada **autodeterminación informativa**, excepciones que están limitadas de manera justa, razonable y acorde con el Principio de Transparencia Administrativa, en los siguientes casos: Cuando los fines persigan la seguridad del Estado, la seguridad y el ejercicio de la autoridad pública, la prevención, persecución, investigación, detención y represión de las infracciones penales, el funcionamiento de bases de datos con fines estadísticos, históricos o de investigación científica, siempre que no exista el riesgo de que las personas sean identificadas, la adecuada prestación de servicios públicos y la eficaz actividad ordinaria de la Administración.

Por otro lado, dicha ley hace una categorización particular o especial en el tratamiento de los datos, estableciendo que **datos sensibles** son aquellos 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 de la persona, entre otros, es decir, información relativa al fuero íntimo de la persona, por lo que ninguna persona estará obligada a suministrar este tipo de datos, salvo que el tratamiento de los datos sea necesario para salvaguardar el interés vital de la persona interesada, sea realizado en el curso de sus actividades legítimas y con las debidas garantías y que no se comuniquen a terceros sin el consentimiento, o que la persona los haya hecho públicos voluntariamente, o que resulte necesario para el diagnóstico médico, siempre sujeto al secreto profesional.

Por su parte, los **datos personales de acceso restringido** son aquellos que, si bien forman parte de registros de acceso público, tienen acceso restringido por ser los datos de interés solamente para el titular o para la Administración Pública.

Mientras que los **datos de acceso irrestricto** son los contenidos en bases de datos públicas de acceso general, según lo dispuesto por leyes especiales y conforme a la finalidad para la cual fueron recabados. Sin embargo, la norma es enfática en que, no se considerarán contemplados en esta categoría: la dirección exacta de la residencia, la fotografía, los números de teléfono privados y otros datos de igual naturaleza, **cuyo tratamiento pueda generar condiciones injustas o discriminatorias o afectar los derechos y los intereses de la persona titular**.

En el tema de la seguridad de los datos, se señala que el responsable de la base de datos debe adoptar las medidas técnicas y de organización necesarias para garantizar la seguridad de los datos que son de carácter personal y evitar así su tratamiento o acceso no autorizado, siendo parte de esa seguridad el deber de confidencialidad cuando se acceda a información sobre datos personales y sensibles, por lo que para poder transferir datos personales, la regla general es que solo se podrán transferir la información contenida en las bases de datos, cuando el titular del derecho haya autorizado de forma expresa y válidamente ese traslado y se haga sin vulnerar los principios y derechos reconocidos en la ley.

En ese sentido es importante señalar que la norma advierte con toda claridad que, constituye una falta grave, recolectar, almacenar, transmitir o de cualquier otra forma emplear datos personales sin el consentimiento informado y expreso del titular de los datos, o que se utilicen para una finalidad distinta de la autorizada por el titular, considerándose falta gravísima estas mismas acciones cuando se trate de datos sensibles.

Por su parte, también debe tomarse en consideración que el ***"Reglamento de actuación de la Ley de Protección de la persona frente al tratamiento de sus datos personales en el Poder Judicial"***[3], establece en los artículos 1, 2, 3, 4, 5, 6, 8, 9, 11, 12, 13, 18 y 25 lo siguiente:

> *"***Artículo 1: Fundamento normativo**
>
> En aplicación de la Ley N° 8968, el Poder Judicial debe establecer los pasos a seguir para la recolección, almacenamiento, tratamiento y manejo de los datos personales incluidos en resoluciones o documentos judiciales, que contengan **datos sensibles**, de conformidad con los artículos previstos en dicha Ley.
>
> **Artículo 2: Finalidad**
>
> Este reglamento tiene como objeto definir los lineamientos Institucionales en relación con el tratamiento que deberá aplicarse a la información originada en el Poder Judicial previo a su publicación en Internet o por cualquier medio con acceso a terceras personas, de forma tal que **se garantice el derecho al acceso a la información pública de carácter judicial, en equilibrio del derecho a la autodeterminación informativa, evitando que se propicien acciones discriminatorias.**
>
> **Artículo 3: Definiciones**
>
> Para la aplicación de este reglamento, se deben considerar las siguientes definiciones:
>
> ***a) Autodeterminación Informativa:*** Derecho fundamental que tiene como objeto controlar el flujo de información que concierne a cada persona, derivado del derecho a la privacidad, evitando que se propicien acciones discriminatorias.
>
> ***b) Datos personales:*** Cualquier dato relativo a una persona física identificada o identificable, tal como el nombre, número de cédula, dirección domiciliaria, entre otros.
>
> ***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.

[3] Aprobado por la Corte Plena en la sesión N° 1-16 celebrada el 11 de enero del 2016, artículo XXXVI y comunicado mediante Circular N° 88-2016 del 3 de junio del 2016.

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.

e) Datos sensibles: Toda aquella información que pueda ser utilizada contra una o varias personas físicas, para discriminarlas o excluirlas, en relación con su fuero íntimo, por ejemplo por su origen racial o étnico, por sus opiniones políticas, convicciones religiosas, espirituales o filosóficas; así como la relativa a información biomédica, vida, salud y orientación sexual, entre otros.

[…]

g) Persona Interesada: Persona física, titular de los datos que sean objeto del tratamiento automatizado o manual.

h) **Persona identificada o identificable:** Toda persona cuya identidad pueda determinarse, directa o indirectamente, por ejemplo, mediante un número de identificación o uno o varios elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

[…]

k) Persona Responsable de la protección de datos: Persona o Despacho que tiene a su cargo la emisión, administración, tratamiento o publicación de información sujeta a la protección de datos personales.

l) Persona Encargada de la protección de datos: Persona o despacho encargado de analizar e implementar la protección de datos personales.

[…]

Artículo 4: Ámbito de aplicación

Estos artículos deberán ser aplicados por los despachos u oficinas judiciales, independientemente de la materia que se trate, en aquellos documentos, resoluciones escritas o información que emitan y que deba ser difundida, publicada o puesta a disposición de terceras personas que no forman parte del proceso.

También deberán protegerse, cuando contengan datos sensibles y previo a su publicación, difusión o puesta a disposición de terceras personas, aquellos fallos emitidos oralmente, sea en audio o video. No obstante, hasta tanto no se cuente con herramientas y plataforma tecnológica que permita dicha protección, no podrán ser publicados.

Artículo 5: Documentos de acceso público en las bases de datos del Poder Judicial a terceras personas

Son de acceso público en las bases de datos oficiales del Poder Judicial, las resoluciones emitidas por los Tribunales Superiores que se encuentren en firme, y las de las Salas de la Corte Suprema de Justicia. **No podrá publicitarse aquella información que no haya sido protegida según lo dispuesto en la Ley No. 8968.**

Artículo 6: Personas Responsables de la protección de datos

Serán responsables de la protección de datos:

· Los funcionarios o funcionarias judiciales responsables de identificar los datos sensibles en las resoluciones a despersonalizar, quienes generan la alerta conforme a los procedimientos establecidos institucionalmente y con base en un razonamiento jurídico adecuado.

· La persona designada en cada despacho u oficina judicial, responsables de remitir la información a los encargados de la protección de los datos.

· La Dirección de Tecnología de la Información, quien deberá proporcionar a los funcionarios y funcionarias, las herramientas tecnológicas que faciliten la protección de datos, así como establecer las medidas de seguridad que garanticen la confidencialidad, disponibilidad e integridad de la información que custodia el Poder Judicial.

[…]

Artículo 8: Obligaciones de la persona responsable de la protección de los datos

La persona, oficina o despacho responsable de la protección de datos deberá:

a) Cumplir las políticas y temas estratégicos institucionales, para la implementación de este reglamento.

b) Identificar y transferir a las personas encargadas, los documentos o resoluciones objeto de protección, mediante el procedimiento que se implemente.

c) Velar por el cumplimiento de este reglamento y demás normas relacionadas.

Artículo 9: Obligaciones de las personas encargadas de la protección de datos

Son obligaciones de las personas encargadas de la protección de datos:

a) Implementar las medidas de seguridad que correspondan y cumplir con lo dispuesto en la Ley No.8968, en el reglamento institucional y demás disposiciones aplicables.

b) Analizar si procede la despersonalización de la información en las resoluciones o documentos que se le han remitido para estudio.

c) Proceder a despersonalizar los datos personales de acceso restringido y de carácter sensible, de conformidad con los dispuesto en la Ley No. 8968 y este reglamento.

[…]

Artículo 11: Otras obligaciones de las personas encargadas y responsables de la protección de datos.

Las personas encargadas y responsables de la protección de datos deberán:

a) Abstenerse de usar los datos sensibles para fines distintos a los autorizados.

b) Guardar confidencialidad respecto de los datos sensibles tratados.

c) Abstenerse de transferir o difundir los datos sensibles de acuerdo con la Ley No.8968.

Artículo 12: Datos que deben protegerse

Para efectos de publicitar la información deberán ocultarse o eliminarse los datos personales contenidos en una resolución o sentencia, que permitan identificar a una persona, cuando se haga alusión a datos sensibles o de acceso restringido.

No podrá divulgarse bajo ninguna circunstancia, la información personal relativa a personas menores de edad, personas mentalmente incapaces, víctimas de acoso, de delitos sexuales y de violencia doméstica. De igual manera no se podrán publicar en ningún caso, la dirección de la residencia, fotografías, número de teléfonos privados y otros de igual naturaleza cuyo tratamiento pueda afectar los derechos y los intereses de la persona titular.

Artículo 13: Reemplazo de Datos Sensibles

Los datos que serán objeto de protección serán los datos personales. En relación con los datos sensibles estos se conservarán con el fin de mantener la historia y estadística para rescatar temas de interés relacionados con derechos humanos, género, violencia doméstica, accesibilidad, entre otros.

Artículo 18: Bases de Datos

Se mantendrán dos tipos de bases de datos:

Base de Datos de acceso restringido: Contendrá toda la información en forma íntegra, sin ningún tratamiento de despersonalización y será conservada para su consulta interna, mediante los procedimientos y sistemas informáticos establecidos por el Digesto de Jurisprudencia y los Centros de Jurisprudencia, en coordinación con la Dirección Jurídica del Poder Judicial.

Base de Datos Pública: En cuanto a la información que deberá ser publicada en Internet o de acceso a terceras personas, se mantendrá una base de datos "pública", que contendrá la información despersonalizada conforme a este reglamento y normativa relacionada. […].

[…]

Artículo 25: Aplicación de este Reglamento

Este reglamento será de acatamiento obligatorio para todas las personas redactoras, despachos y oficinas judiciales, a partir de su aprobación y publicación. En caso de incumplimiento se aplicarán las medidas sancionatorias correspondientes.*"*

En ese sentido tanto la Ley 8968 como el ***"Reglamento de actuación de la Ley de Protección de la persona frente al tratamiento de sus datos personales en el Poder Judicial"***, aseguran el Derecho Fundamental de Autodeterminación Informativa, al regular el flujo de información que atañe a cada persona y establece el camino que se debe seguir para el adecuado tratamiento y manejo de los datos o la información que se origina en el Poder Judicial. Por supuesto que, esta normativa es de acatamiento obligatorio, especialmente por todas aquellas oficinas o despachos que recopilen datos personales.

También es importante señalar que, con respecto a los **datos sensibles**, los "**Estándares de Protección de Datos Personales**"[4], los define de la siguiente manera:

[4] Aprobados en el XV Encuentro Iberoamericano de Protección de Datos, celebrado del 20 al 22 de junio del 2017 en Santiago de Chile. https://www.infoem.org.mx/doc/publicaciones/EPDPEI_2017.pdf

"**2. Definiciones**

2.1. Para los efectos de los presentes Estándares se entenderá por:

[…]

d. Datos personales sensibles: aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívLoca a una persona física."

La **Sala Constitucional** en la resolución N° 5255-2007 de las 16:28 horas del 18 de abril del 2007 señaló que la información de interés público es "…aquella en la que la colectividad tiene interés por estar vinculada a la marcha de las instituciones estatales para permitir la fiscalización ciudadana, con la obligación correlativa del funcionario de brindarla de manera expedita".

Al respecto, es importante resaltar lo siguiente:

- No toda información en poder del Estado aún y cuando conste en un expediente administrativo puede ser dada a terceros.
- Únicamente aquella que sea de interés público o cuando así lo establezca la ley.
- Pueden existir supuestos en los que se debe guardar reserva a fin de tutelar los derechos de terceros.[5]

Dentro de la información de interés público debe considerarse la que está relacionada con el **uso y disposición de los fondos públicos**, así como, sobre el **desempeño y remuneraciones de los funcionarios públicos.** El fundamento legal de lo anterior es la

[5] Véase Jaínse Marín Jiménez, Derecho de acceso a la información: alcances, límites y responsabilidades asociadas, Arisol Consultores, curso impartido los días 9 y 10 de diciembre del 2014, filmina 151/259.

Ley contra la corrupción y el enriquecimiento ilícito en la Función Pública, la cual en el artículo 7 establece lo siguiente:

> "Artículo 7º-**Libre acceso a la información**. Es de interés público la información relacionada con el ingreso, la presupuestación, la custodia, la fiscalización, la administración, la inversión y el gasto de los fondos públicos, así como la información necesaria para asegurar la efectividad de la presente Ley, en relación con hechos y conductas de los funcionarios públicos.
>
> No obstante, la Contraloría General de la República solo podrá revisar documentos de carácter privado según lo dispuesto en el artículo 24 de la Constitución Política y en el artículo 11 de la presente Ley."

Al respecto, la **Sala Constitucional**, en la resolución N° 880-1990 de las 14:25 horas del 1 de agosto de 1990, señaló, en lo que interesa:

> (…) Para efectos de una correcta resolución, en el caso, cabe advertir que si bien las normas y principios constitucionales atinentes deben apreciarse en su conjunto- ante el planteamiento determinado- y no aisladamente, para su correcta aplicación debe estarse también a la calidad o no de funcionario público que la persona, de quien se solicita información, tenga. Así el derecho a la información sobre determinada actividad, ventaja o derecho que un particular ostente estarla vedado por lo dispuesto en el artículo 24 de la Constitución Política, cosa que no sucede en cuanto al funcionario público, por el evidente interés que para la comunidad representa el poder estar debidamente informada de su actividad, **del buen o mal desempeño en el ejercicio de su cargo,** de las ventajas o no que el nombramiento conlleva y de los derechos que como tal obtiene, fundamentalmente en cuanto éstos sean de índole económica -salarios, en dinero o en especie, pluses, dietas, etcétera- pues en tratándose de **fondos públicos** son los administrados en general -o como usuarios del servicio- los que los pagan con sus contribuciones y tienen el derecho de saber cómo se administran y se gastan éstos. **Toda la actividad del funcionario público es evidentemente de interés público** -no sólo en buena lógica- sino por propia definición del artículo 113 de la Ley General de la Administración Pública, ya que el desempeñó de sus funciones debe estar encaminado primordialmente a la satisfacción de aquél y en cuanto se separe de aquella finalidad -que le envuelve como tal- estaría faltando a lo que constituye la esencia de su función. Sería conveniente, tal vez, para algunos funcionarios que pasara inadvertida su actividad, para que ésta no pudiera ser calificada así por la colectividad, pero desde la aceptación del cargo ello no es posible pues sobre aquella conveniencia privan los valores de seguridad jurídica y de justicia, no sólo para la comunidad sino también para todos y cada uno de los individuos que la forman -que en todo caso deben ser considerados como

representantes de aquélla, de la que el funcionario depende- y acto de justicia es el derecho a saber cómo se emplean y el destino que se da a los recursos que esa colectividad aporta y que hacen posible la retribución por sus servicios al "servidor público". Conlleva pues, lo expuesto, el derecho que tiene todo administrado de obtener información en cuanto se refiera a la **actividad del funcionario en el desempeño de sus funciones,** de sus emolumentos y de la **forma en que se administran los fondos públicos** en general y la obligación del servidor público de rendirlos a la comunidad -y a cualquier ciudadano como representante de aquélla- de quien el funcionario depende, con la única salvedad de que se trate de un secreto de Estado o de información suministrada a la administración por particulares, para gestiones determinadas, **que conservarán siempre su confidencialidad siempre y cuando ésta esté constitucional o legalmente protegida**. […] (Énfasis suplido)

De manera que, lo anterior, puede resumirse en lo siguiente:

- Toda la información relacionada con el desempeño y las remuneraciones que perciben los funcionarios públicos es de **acceso público**.
- Salvo que se trate de información confidencial del funcionario (expediente médico del funcionario, razones por las cuales está incapacitado, etc.
- La regla es el acceso (el secreto la excepción).[6]

Ahora bien, debido a que el caso concreto se refiere a información relacionada con la evaluación del desempeño de las personas servidoras judiciales, debemos traer a colación los artículos 1, 2, 5, 8 y 21 del **Reglamento del Sistema Integrado de Evaluación del Desempeño**[7], que señalan lo siguiente:

"**Artículo 1.- Ámbito de aplicación y alcance.**
En concordancia con lo que regula la Constitución Política, Ley General de Administración Pública, el Estatuto de Servicio Judicial, la Ley de Salarios del Poder Judicial, Ley General de Control Interno y demás normas vigentes en la materia, este reglamento se establece con el fin de regular la evaluación del desempeño de todas

[6] Véase Jaínse Marín Jiménez, Derecho de acceso a la información: alcances, límites y responsabilidades asociadas, Arisol Consultores, curso impartido los días 9 y 10 de diciembre del 2014, filmina 175/259.
[7] Comunicado mediante Circular N° 204-2019 del 18 de noviembre del 2019 y publicada el 9 de enero del 2020.

las personas que tengan relación de servicio dentro de todos los ámbitos del Poder Judicial.

Artículo 2.- Definiciones.

a) Evaluación del Desempeño: es el proceso de gestión de todas las personas trabajadoras judiciales basado en instrumentos y procedimientos con parámetros objetivos diseñados por la Dirección de Gestión Humana, que tiende a potenciar la mejora continua y rendición de cuentas de esas personas. Además, por medio de la observación y supervisión, permite valorar y apreciar el desempeño individual de la persona servidora judicial, en un determinado tiempo, para medir su aporte en el logro de las funciones, objetivos, actividades y responsabilidades que les competen según el Sistema de Clasificación y Valoración de Puestos. En términos de la eficiencia, eficacia, economía y calidad de los servicios que se prestan.

[…]

Artículo 5.- Principios.

La evaluación del desempeño se regirá por los siguientes principios:

[…]

j) Transparencia: la información que se genere como producto de la aplicación del SIED, deberá ser oportuna, exacta y a disposición de quién lo requiera, respetando las regulaciones en la protección de datos.

[…]

Artículo 8.- Responsabilidad de los otros órganos involucrados

a) La Dirección de Gestión Humana, por medio del **Subproceso de Gestión del Desempeño**, será el órgano asesor con carácter vinculante y obligatorio de los órganos que integran el S.I.E.D., para el desarrollo de las acciones administrativas, tales como: planificar, elaborar, administrar, facilitar y validar todo el proceso de evaluación del desempeño, así como el responsable de procesar información, generar resultados y presentar informes con el objeto de que se planifiquen las respectivas acciones de mejora.

[…]

Artículo 21. -Custodia de los resultados.

Los resultados del S.I.E.D. obtenidos por cada persona evaluada serán enviados al expediente electrónico, que administra la Dirección de Gestión Humana; y **se considerarán públicos**, salvo aquellos datos cuya confidencialidad debe ser resguardada de acuerdo con la Ley de protección de la persona frente al tratamiento de sus datos personales."

Obsérvese que uno de los principios en que se fundamenta dicho Reglamento del Sistema Integrado de Evaluación del Desempeño es la **transparencia**, en el sentido de que la información o los datos que se generen producto de la aplicación del SIED, debe estar a disposición de quien la requiera, siempre y cuando se respete las regulaciones en materia de protección de datos. Por otro lado, señala que los resultados obtenidos por cada persona evaluada son datos **públicos**, excepto aquellos cuya confidencialidad debe ser resguardada de acuerdo con la *Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales*.

En ese sentido debe entenderse que el alcance que tiene la aplicación del Sistema Integrado de Evaluación del Desempeño, tanto para el Poder Judicial como para las personas servidoras judiciales, es mejorar la calidad de sus servicios y contribuir con el valor público que el Estado requiere de todas las personas que lo integran, y que el fin específico de la información recopilada es precisamente medir el logro de las funciones, objetivos, actividades y responsabilidades que le competen a cada una de las personas que tengan relación de servicio dentro de todos los ámbitos del Poder Judicial, de acuerdo con lo establecido en los artículos 1 y 2 del citado Reglamento, todo esto en procura del bienestar de la sociedad costarricense; sin embargo, dicha normativa es enfática en señalar que toda la evaluación del desempeño, debe estar en línea con lo que dispone la **Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales y sus principios**.

De acuerdo con todo lo anteriormente analizado, esta Dirección Jurídica estima que si la información relativa a las justificaciones del resultado final de la evaluación del desempeño otorgado por la persona evaluadora en el apartado de competencias a determinada persona, revela 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 de la persona, entre otros, es decir, información relativa al fuero íntimo de la persona, se estaría en presencia de datos de naturaleza íntima o sensible y que, al constituirse en información confidencial, tendría que ser necesariamente protegida para poder ser transferida o compartida a terceros, por cuanto su tratamiento podría afectar los derechos e intereses de la persona titular.

En ese sentido, debe tomarse en consideración que de acuerdo con el artículo 8 del **Reglamento del Sistema Integrado de Evaluación del Desempeño**, el **Subproceso de Gestión de Desempeño** de la Dirección de Gestión Humana, además de ser el órgano asesor con carácter vinculante y obligatorio de los órganos que integran la SIED, también es la oficina responsable de procesar la información y generar los resultados; en consecuencia, al estar legitimada, le **corresponde garantizar un trato adecuado y brindar seguridad a la información que determine como sensible, íntima o nominativa**, evitando ser utilizada para fines distintos a los autorizados, contrario sensu se necesitaría obligatoriamente el consentimiento informado de las personas titulares de la información.

En todo caso, la regla general es que los despachos u oficinas judiciales, tienen la obligación de que las transferencias de datos se realicen sin quebrantar los principios y derechos mencionados en este informe; de lo contrario, la Administración se encontraría ante una falta gravísima al revelar información sensible o confidencial registrada en las bases de datos que se tienen al efecto, incurriendo además, en **delitos como el de abuso de autoridad, prevaricato y violación de datos personales.**

III. Conclusiones:

De conformidad con todo lo expuesto y con fundamento en los artículos 11, 24 y 30 de la Constitución Política, el artículo 11 (Principio de Legalidad Administrativa) de la Ley General de la Administración Pública, artículo 7 de la Ley contra la Corrupción y el enriquecimiento ilícito en la Función Pública, los artículos 1, 2, 3, 4, 5, 6, 8, 9, 10, 14, 30 y 31 de la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, los artículos 1, 2, 3, 4, 5, 6, 8, 9, 11, 12, 13, 18 y 25 del Reglamento de actuación de la Ley de Protección de la persona frente al tratamiento de sus datos personales en el Poder Judicial, los artículos 1, 2, 5, 8 y 21 del Reglamento del Sistema Integrado de Evaluación del Desempeño en el Poder Judicial, los Principios de Intimidad, de Autodeterminación Informativa, de Consentimiento Informado, de Calidad de la Información, de Transparencia y lo dispuesto por la Sala Constitucional, en la

resolución N° 2003-11338 de las 9:50 horas del 3 de octubre del 2003 y el voto 8672-2010 de las 9:36 horas del 14 de mayo de 2010, se concluye lo siguiente:

1. El Estado se constituye en un custodio y no en el dueño de la información que recibe y produce de la interacción con los administrados, razón por la cual, en materia de acceso a la información, más que derechos, los entes públicos tienen una serie de deberes, obligaciones y responsabilidades muy amplias.

2. El **derecho a la intimidad** debe ponderar los intereses en relación, entre el legítimo interés de la sociedad a desarrollarse utilizando la información, como también la necesidad de proteger a la persona frente al uso arbitrario de sus datos personales y, por ello, el progreso no significa que los ciudadanos deban quedar en una situación de desventaja frente al Estado.

3. El respeto al **derecho fundamental de autodeterminación informativa** derivado del derecho a la intimidad (artículo 24 de la **Constitución Política**), garantiza un trato legítimo y un control sobre el flujo de informaciones confidenciales concernientes a una persona, cubriendo las bases de datos que mantiene el Poder Judicial, de manera que, no pueden ser accedidos por ninguna persona, por suponer una intromisión o injerencia externa e inconstitucional.

4. Las **excepciones al Principio de Autodeterminación Informativa** están limitadas de manera justa, razonable y acorde con el Principio de Transparencia Administrativa, sin que el acceso a información íntima, sensible o nominativa que pueda estar incluida en las justificaciones del resultado final de la evaluación del desempeño de determinada persona, se encuentre asociado a alguna de ellas.

5. El **Principio de Consentimiento Informado**, consiste en la necesidad de informar previamente a las personas titulares, cuando se les soliciten datos de carácter personal, de forma expresa, precisa e inequívoca, de la existencia de la base de datos, cuáles son los fines que se persiguen con su recolección, los

destinatarios y quiénes podrían consultar esa información, sobre el carácter obligatorio o facultativo de las respuestas a las preguntas que se formulen durante la recolección de los datos y del tratamiento que se le dará a esa información, de las consecuencias de la negativa de brindar los datos, también sobre la posibilidad de ejercer los derechos que le asisten al interesado, así como de la identidad y dirección del responsable de la base de datos. De esta manera, quien recopile los datos personales deberá obtener obligatoriamente el consentimiento expreso de la persona titular, siendo prohibida la recolección de datos sin el consentimiento informado de la persona titular. El consentimiento debe constar por escrito.

6. El consentimiento expreso no es necesario cuando exista una orden dictada por la autoridad judicial competente, o se trate de datos personales de acceso irrestricto, o bien, los datos deban ser entregados por disposición constitucional o legal.

7. De acuerdo con el **Principio de Calidad de Información**, solamente pueden ser recolectados, empleados o almacenados datos de carácter personal para su tratamiento automatizado o manual, **adecuados al fin** para el que fueron recolectados, sin poder ser tratados después, de manera incompatible con los fines.

8. Conforme al **Principio de Transparencia**, la información o los datos que se generen producto de la aplicación del **Sistema Integrado de Evaluación del Desempeño** debe estar a disposición de quien la requiera, siempre y cuando se respete las regulaciones en materia de protección de datos anteriormente señaladas. Asimismo, los resultados obtenidos por cada persona evaluada son considerados públicos, excepto aquellos cuya confidencialidad debe ser resguardada de acuerdo con la **Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales**.

9. El **Subproceso de Gestión de Desempeño** de la Dirección de Gestión Humana, además de ser el órgano asesor con carácter vinculante y obligatorio de los órganos que integran la SIED, también es la oficina responsable de procesar la información y generar los resultados; en consecuencia, al estar legitimada, le corresponde **garantizar un trato adecuado y brindar seguridad a la información que determine como sensible, íntima o nominativa**, evitando ser utilizada para fines distintos a los autorizados, contrario sensu se necesitaría obligatoriamente el consentimiento informado de las personas titulares de la información. En consecuencia, si la información contenida en la casilla de justificaciones en la que se detalla el resultado final de la evaluación del desempeño consignado por la persona evaluadora en el apartado de *metas cuantitativas y competencias genéricas* a determinada persona, tuviera algún dato sensible, esa oficina deberá respetar y cumplir la protección legalmente establecida para ese tipo de información, a saber, 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 de la persona, entre otros, es decir, información relativa al fuero íntimo de la persona. De manera que, al constituirse en información confidencial, tendría que ser -necesariamente- protegida para poder ser transferida o compartida a terceros, por cuanto su tratamiento podría afectar los derechos e intereses de la persona titular.

10. La información suministrada con motivo de la evaluación realizada deberá ser empleada exclusivamente para los fines que fue requerida y los efectos de estos, salvo consentimiento del titular de la información.

11. Por regla general, los despachos u oficinas judiciales tienen la obligación de que las transferencias de datos se realicen sin quebrantar los principios y derechos mencionados en este informe; de lo contrario, la Administración se encontraría ante una falta gravísima al revelar información sensible o confidencial registrada en las bases de datos que se tienen al efecto, pudiendo incurrir, además, en

delitos como el de abuso de autoridad, prevaricato y violación de datos personales.

De esta manera, queda expuesto el panorama jurídico y regulatorio existente, a fin de que el órgano competente valore y decida lo que en Derecho proceda respecto del caso concreto.

Advertencias:

- Se les recuerda a los requirentes que los criterios de la Dirección Jurídica **no son vinculantes**.
- El presente criterio se funda en un razonamiento técnico jurídico con base en la aplicación del ordenamiento jurídico administrativo y el supletorio aplicable a la materia, cualquier valoración de oportunidad y conveniencia que sea necesario realizar, es competencia de las unidades decisoras y ejecutoras correspondientes.
- El presente criterio se emite con base en la información suministrada por la unidad requirente del mismo, mediante el oficio N° PJ-DGH-SGD-145-2021 de 26 de octubre del 2021 de la Dirección de Gestión Humana. Por lo anterior, no le corresponde a esta unidad asesora la responsabilidad por la veracidad de dicha información.
- Cualquier traslado del presente criterio a terceros no involucrados en los procesos de análisis y toma de decisiones con respecto al objeto del mismo, deberá ser realizado previa despersonalización de cualquier dato sensible que se haya consignado en dicho documento.
- No se advierte incompatibilidad o conflicto ético para la emisión del presente criterio, en tanto que los temas indicados no inciden en los derechos subjetivos de los suscribientes, ni hay vínculos de ningún tipo con la persona sobre la cual gira el análisis del informe.
- El presente criterio se emite con base a la consulta realizada, por lo que es responsabilidad de la unidad requirente precisar y delimitar la o las consultas formuladas a esta Dirección.

De usted atentamente,

Elaborado por: Lic. Manuel Araya Zúñiga
Asesor Jurídico 1 a. i.

Revisado por: Licda. Silvia Elena Calvo Solano
Coordinadora a. i. Área Análisis Jurídico

Autorizado por: M. Sc. Rodrigo Alberto Campos Hidalgo
Director Jurídico a. i.

Ref: 1518-21

MAZ