

## COLEGIO DE ABOGADOS Y ABOGADAS DE COSTA RICA

### COMISIÓN AD HOC PARA EL ANÁLISIS SOBRE LA CREACIÓN DE LA UNIDAD PRESIDENCIAL SOBRE ANÁLISIS DE DATOS

#### INFORME TÉCNICO

**ANTECEDENTES:** A petición de la Defensoría de los Habitantes se pide la colaboración al Colegio de Abogados y Abogadas de Costa Rica para el análisis técnico jurídico del Decreto Ejecutivo No.41996 de 14 de octubre de 2019, denominado “*Creación de la Unidad Presidencial de Análisis de Datos*”, publicado en el Diario Oficial La Gaceta No.31, Alcance 24, de 17 de febrero de 2020, y posteriormente derogado mediante Decreto Ejecutivo No.42216 de 21 de febrero de 2020. La Junta Directiva del Colegio de Abogados y Abogadas de Costa Rica rinde el presente informe, producto del análisis jurídico del documento sometido a estudio, del cual se extraen una serie de observaciones y recomendaciones, confrontando el contenido del decreto ejecutivo con otras normas que regulan la temática referente a los derechos de intimidad, privacidad, protección de las comunicaciones y documentos privados, y muy especialmente la protección de datos personales.

#### UNIDAD PRESIDENCIAL DE ANÁLISIS DE DATOS.


El día 14 de octubre del dos mil diecinueve, el Ministro de la Presidencia y el Ministro A.I de Planificación Nacional y Política Económica, firmaron, junto con el Presidente de la República, el decreto N° 41996-MP-MIDEPLAN, invocando las facultades otorgadas por la Constitución Política, la Ley General de Administración Pública No.6227 de 4 de mayo de 1978 y la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales No.8968 de 7 de julio de 2011, para crear la Unidad Presidencial de Análisis de Datos (UPAD).

El decreto tenía por objeto crear la Unidad Presidencial de Análisis de Datos (UPAD) y reglamentar su organización y funcionamiento.

La UPAD sería una unidad “*de tipo político-estratégico adscrita a la Presidencia de la República*”, con el fin de asesorar de manera permanente al Presidente de la República, fortaleciendo un enfoque de toma de decisiones de política pública, fundamentadas en la evidencia que aporta el análisis de los datos.

El decreto, en el numeral 4, inciso 4, establecía que UPAD se regiría por el deber de confidencialidad acerca de la información confidencial que obtenga:

“4. *Deber de confidencialidad: dicha obligación se extenderá a las personas funcionarias de la UPAD sobre la información confidencial que les sea compartida o suministrada bajo ese carácter por parte de las instituciones públicas. Esta obligación perdurará aún después de finalizada la relación con la UPAD.*”



Dentro de los objetivos enumerados para la UPAD destacaban el numeral 5º, incisos 6) y 7):

*“6. Realizar análisis sobre distintos fenómenos de la realidad costarricense que permitan la detección oportuna de problemas y oportunidades para proponer al Presidente de la República alternativas de toma de decisión política más certeras y dirigidas a generar el mayor impacto positivo para el país.*

*7. Monitorear y evaluar el impacto de las decisiones del Presidente de la República, tomadas sobre la base de las recomendaciones de la UPAD.”*

De acuerdo con el artículo 6º, se enumeraban las funciones de la UPAD, dentro de las que destacaban las siguientes:

*“3. Garantizar un adecuado resguardo y confidencialidad durante la gestión de los datos institucionales cuando así se requiera, de forma que se utilicen únicamente con fines de apoyo a la toma de decisiones de política pública que favorezcan al bienestar de las personas; cumpliendo con los principios éticos, las normativas de acceso y uso de información pública.*

*4. Monitoreo y evaluación del impacto de las decisiones del Presidente de la República, tomadas sobre la base de las recomendaciones de la UPAD.*

(...)

*7. Establecimiento de alianzas de cooperación con instituciones públicas y académicas para garantizar que se incorporen en la gestión de trabajo de la UPAD tecnologías de vanguardia, así como la experiencia en análisis de datos para mejorar la gobernanza pública.”*

Con el fin de cumplir las atribuciones constitucionales y legales del Presidente de la República, los principios, objetivos y funciones de UPAD, en el numeral 7º se obligaba a todas las instituciones de la Administración Pública Central y Descentralizada a permitir el acceso a toda información que fuere requerida por parte de la UPAD, *“salvo aquellos casos particulares donde la información sea considerada como secreto de Estado”*. Adicionalmente, *“en cumplimiento de los incisos e) y f) del artículo 8º de la Ley de Protección de la Persona frente al tratamiento de sus datos personales, Ley N° 8968, se requerirá información de carácter confidencial con la que cuenten las instituciones públicas.”*

Según el texto literal del numeral 7º, la información transferida mantendría en todo momento su carácter confidencial y establecía que la UPAD suscribiría acuerdos de gobernanza con las instituciones para la transferencia de información, y así garantizar un uso responsable y coherente de los datos que beneficiaría a los ciudadanos y fortalecería la confianza pública.

Con el fin de asegurar la confidencialidad de los datos, la UPAD contaría con un Director, el cual se denominaba Director de Análisis de Datos el cual, de acuerdo con el decreto, es equivalente a un Director de Datos (Chief Data Officer) y respondería directamente al

Presidente de la República. Este director, debería contar con experiencia en análisis de datos para la toma de decisiones de política pública, *“con conocimiento tanto en el uso de técnicas de ciencia de datos como de ciencia política, administración pública u otras afines”*. No se menciona nada con respecto al apartado de Chief Data Officer, que es un perfil más dirigido a la protección de los datos personales.

El decreto, en su numeral 10º. declaraba de interés público las actividades de la UPAD.

De acuerdo con lo reportado por diferentes medios de comunicación, un grupo de personas ya habían venido ejerciendo de facto la función de esta unidad por unos dieciocho meses y habían solicitado la transferencia de datos personales, para ser utilizados en lo que el decreto llamó Unidad Presidencial de Análisis de Datos.

El decreto fue publicado en el diario oficial La Gaceta No.31, Alcance 24, de 17 de febrero de 2020, y posteriormente fue derogado mediante Decreto Ejecutivo No.42216 de 21 de febrero de 2020.

De igual manera, según lo reportado por diferentes medios de comunicación, se indica que pudo haber sido utilizada la plataforma [tableau.com](https://tableau.com), sin que se sepa la fecha, para publicar información que podría estar protegida, y haber sido obtenida de entes públicos. En el mismo sentido, la política de datos<sup>1</sup> de la plataforma Tableau Public no garantiza la confidencialidad de los contenidos.

En comunicado de prensa por parte de la Agencia de Protección de Datos Personales PRODHAB, autoridad competente para investigar cualquier incumplimiento de las disposiciones de la ley No. 8968 citada, consideró oportuno que se haya derogado el decreto. Sin embargo, aclaró que *“No existe una prohibición legal para que la información pueda ser compartida, siendo que la ley 8968 establece excepciones y una de ellas es la actividad ordinaria de la administración”*. Al mismo tiempo, recomendó que, cuando el decreto entre en vigencia, se suscriban convenios interinstitucionales donde se establezcan obligaciones, responsables y eventuales consecuencias de quienes incumplan las obligaciones de las partes; lo cual ya es algo que el decreto regulaba en el numeral 7º en su párrafo segundo al indicar que *“las instituciones deberán establecer acuerdos de gobernanza para garantizar un uso responsable y coherente de los datos que beneficie a los ciudadanos y fortalezca la confianza pública”*.

#### NORMATIVA APLICABLE:

1.- **Artículo 24 de la Constitución Política**, el cual garantiza la libertad, intimidad y la privacidad de los ciudadanos, en un amplio rango de valores que incluyen sus comunicaciones

<sup>1</sup> Política de datos. Recuperado 2 marzo, 2020, de <https://public.tableau.com/es-es/s/data-policy>

Handwritten signatures and initials in the bottom right corner of the page, including a large signature at the top, a signature below it, and initials 'LW' and another signature at the bottom.

y documentos privados, pero que también es el origen básico de la autodeterminación informativa como derecho fundamental.

Estas garantías y protecciones se encuentran también contempladas en normas de rango internacional, tales como el Pacto Internacional de Derechos Civiles y Políticos, aprobado mediante ley No.4229 de 11 de diciembre de 1958, así como en el artículo 12 de la Declaración Universal de Derechos Humanos y por el artículo 11 de la Convención Americana sobre Derechos Humanos.

**2.-Principio de Reserva de Ley**, en el tanto sólo la Asamblea Legislativa, mediante una norma debidamente aprobada en su seno, puede imponer límites a los derechos fundamentales de los ciudadanos. El derecho a la protección de datos personales se considera un principio fundamental, que a la vez tiene su asidero en el artículo 24 de la Constitución Política. No existe norma jurídica alguna que otorgue esa potestad a otro Poder de la República.

**3.- Principio de Legalidad.** En el sector público, el Principio de Legalidad se encuentra regulado en el artículo 11 de la Constitución Política, así como en el párrafo primero del artículo 11 de la Ley General de la Administración Pública No.6227 de 4 de mayo de 1978, el cual indica literalmente que *“La Administración Pública actuará sometida al ordenamiento jurídico y sólo podrá realizar aquellos actos o prestar aquellos servicios públicos que autorice dicho ordenamiento, según la escala jerárquica de sus fuentes.”*. Esta regla no admite excepciones, así que ningún órgano público puede llevar a cabo ninguna función que no le esté expresamente permitida por una disposición preexistente. Actualmente, ninguna norma jurídica permite la transferencia de información entre órganos públicos, o de datos personales de los ciudadanos sin el debido conocimiento informado y la autorización de los titulares de los derechos.

**4. Deber de probidad por parte de los funcionarios públicos:** los funcionarios públicos de todo nivel deben de respetar y aplicar las disposiciones contempladas en el artículo 3 de la Ley contra la Corrupción y el Enriquecimiento Ilícito en la Función Pública No.8422 de 6 de octubre de 2004, así como el contenido del decreto ejecutivo No.33146 de 24 de mayo de 2006, denominado “Principios Éticos de los Funcionarios Públicos” y sus reformas.

**5. Transferencia de datos personales.** El Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, N° 37554-JP de 30 de 9 octubre de 2012 y sus reformas define la transferencia de datos personales como *“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.”* Esta temática también se regula con claridad en el artículo 14 de la ley No. 8968, donde se señala la prohibición de compartirlos sin la autorización del titular. Por regla general, *“Los responsables de las bases de datos, públicas o privadas, sólo podrán transferir datos contenidos en ellas cuando el titular del derecho haya autorizado expresa y válidamente tal transferencia y se*

Handwritten signatures and initials in the right margin, including a large signature at the top, several smaller initials, and a signature at the bottom right.

*haga sin vulnerar los principios y derechos reconocidos en esta ley.*” (Los destacados no son del original). Por la naturaleza de esta información de carácter personal, se **impide su traslado a terceros sin la debida autorización del titular**, pues requiere el consentimiento inequívoco del titular de los datos, esto de acuerdo con lo establecido en el artículo de la ley ya indicado y en el numeral 40 de su reglamento: **“La transferencia requerirá siempre el consentimiento inequívoco del titular. La transferencia implica la cesión de datos personales por parte, única y exclusivamente, del responsable que transfiere al responsable receptor de los datos personales. Dicha transferencia de datos personales requerirá siempre del consentimiento informado del titular, salvo disposición legal en contrario, asimismo que los datos a transferir hayan sido recabados o recolectados de forma lícita y según los criterios que la Ley y el presente Reglamento dispone. (...)”** (Los destacados no son del original)

Por lo anterior, los convenios interinstitucionales que busquen la transferencia de datos personales, de un responsable de la base de datos a otro, dentro de la Administración Pública, central o descentralizada, requieren el consentimiento informado del titular, salvo que exista una ley que faculte dicha transferencia.

**6. Datos personales sensibles y de acceso restringido.** Los datos sensibles hacen referencia a toda información que aluda a fuero interno de la persona tales como creencias, ideología, religión, vida o preferencias sexuales, salud, hábitos de vida, consumos, origen racial, pensamientos y en general cualquier dato referente a la intimidad o privacidad del ciudadano. De igual forma, los datos de acceso restringido son aquellos en los cuales sólo puede tener interés el titular o la Administración Pública en los casos que la ley autorice su recopilación y tratamiento. No son de acceso libre, ni público o general. Cualquier dato que se considere confidencial por una ley, necesariamente será de tipo sensible o de acceso restringido. Precisamente por la naturaleza tan particular y delicada de esta información, su tratamiento (que involucra al menos dieciséis acciones diferentes, según el artículo 3 de ley No.8968) se encuentra, en principio, prohibido, salvo las excepciones puntuales que prevé la normativa. También, el artículo 196 bis del Código Penal sanciona como agravante el tratamiento no autorizado por el titular, en beneficio propio o de un tercero, de los datos sensibles. El axioma es la protección de la libertad y la esfera personal del individuo, misma que involucra también sus documentos privados, comunicaciones y en general cualquier otro elemento que se contemple en el respeto a la autonomía de la voluntad del ciudadano, misma en la que el Estado no debe tener injerencia. Esta afirmación se desprende del primer párrafo del artículo 24 de la Constitución Política y demás Acuerdos Internacionales ya citados. Es necesario insistir y tener presente que esos datos sensibles, al igual que los datos personales de acceso restringido, pertenecen a la persona y es ésta su único titular. Por lo tanto, es sólo con su autorización formal que se pueden recopilar y dar un tratamiento adecuado (su transferencia, entre otras muchas acciones) que no lesione la autodeterminación informativa.

**7. Limitación al derecho de autodeterminación informativa.** Las excepciones a la autodeterminación informativa del ciudadano se encuentran contempladas en el artículo 8 de la citada ley No.8968. Sólo podrán ser limitados **“de manera justa, razonable y acorde con el principio de transparencia administrativa”**, cuando la Administración busque ciertos

Handwritten signatures and initials in the right margin, including a large signature at the top, a smaller one below it, and several initials and scribbles at the bottom right.

objetivos, tales como la seguridad del Estado; la seguridad y el ejercicio de la autoridad pública; la prevención, persecución, investigación, detención y represión de las infracciones penales, o de las infracciones de la deontología en las profesiones; 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 o hacerlas identificables; la adecuada prestación de servicios públicos; y la eficaz actividad ordinaria de la Administración, por parte de las autoridades oficiales.

Estas dos últimas excepciones han sido citadas en el decreto de creación de la UPAD para justificar sus actuaciones y obtener información confidencial sin el consentimiento de los titulares. No obstante, no comparte esta Comisión su aplicación para justificar el traslado de datos personales desde otras bases de datos que cumplen otras finalidades establecidas por ley, y que a la vez pueden contener información sensible o de acceso restringido. Las excepciones no pueden anular la regla principal declarada por el artículo 24 de la Constitución Política, ni los artículos 9 y 14 de la ley No.8968, sobre la prohibición del tratamiento de datos personales y las reglas aplicables para la transferencia de datos personales.

De igual manera, ese procedimiento de recabar información personal, sin verdadera autorización legal y sin indicar con claridad cuál es la finalidad concreta de una nueva base de datos, transgrede las disposiciones vistas sobre la prohibición de recopilar datos personales de manera ilícita, dar tratamiento a datos sensibles, así como prohibición de transferir datos personales; todo ello sin autorización de los titulares de la información. Apelar a los incisos e) y f) del artículo 8 de la ley No.8968 es insuficiente para justificar esas acciones que son manifiestamente contrarias a la ley pues dichos incisos, a pesar de contener términos indeterminados o poco claros, no pueden ser interpretados de manera amplia en contra de los derechos fundamentales de los ciudadanos, en tanto que están referidos a la posibilidad de preservar ciertos datos personales para cumplir un fin público de la institución que los recaba y les dará el tratamiento que autorice la ley, no para que sean transferidos y tratados en otra oficina gubernamental que no posee normativa clara ni es respetuosa del principio de legalidad.

**8. Funciones de la Agencia de Protección de Datos de los Habitantes.** - Las funciones que la ley ordena a la Agencia de Protección de Datos de los Habitantes - Prodhav - están reseñadas en el artículo 16 de la ley No.8968. Son bastante amplias y todas ellas están referidas al resguardo de los datos personales de los ciudadanos. Precisamente, el inciso a) establece la función de **“velar por el cumplimiento de la normativa en materia de protección de datos, tanto por parte de personas físicas o jurídicas privadas, como por entes y órganos públicos.”**

Debe llevar un registro de las bases de datos que deban estar inscrita de acuerdo con la ley, así como requerir, de quienes administren bases de datos, las informaciones necesarias para el ejercicio de su cargo, entre ellas, los protocolos utilizados.

También tiene la potestad de acceder a las bases de datos reguladas por la ley, a efectos de hacer cumplir efectivamente las normas sobre protección de datos personales. Esta atribución

Handwritten signatures and initials on the right side of the page, including a large signature at the top, a signature below it, and several initials (XV, LW, and others) further down.

se aplicará para los casos concretos presentados ante la Agencia y, excepcionalmente, cuando se tenga evidencia de un mal manejo generalizado de la base de datos o sistema de información. Debe resolver sobre los reclamos por infracción a las normas sobre protección de los datos personales, así como ordenar, de oficio o a petición de parte, la supresión, rectificación, adición o restricción en la circulación de las informaciones contenidas en los archivos y las bases de datos, cuando éstas contravengan las normas sobre protección de los datos personales. Tiene el deber de imponer las sanciones establecidas en la ley, a las personas físicas o jurídicas, públicas o privadas, que infrinjan las normas sobre protección de los datos personales, y dar traslado al Ministerio Público de las que puedan configurar delito. Debe promover y contribuir en la redacción de normativa tendiente a implementar las normas sobre protección de los datos personales, y dictar las directrices necesarias, las cuales deberán ser publicadas en el diario oficial La Gaceta, a efectos de que las instituciones públicas implementen los procedimientos adecuados respecto del manejo de los datos personales, respetando los diversos grados de autonomía administrativa e independencia funcional.

Finalmente, se le ordena fomentar entre los habitantes el conocimiento de los derechos concernientes al acopio, el almacenamiento, la transferencia y el uso de sus datos personales.

A pesar de que las funciones de la Prodhav son bastante claras, los criterios jurídicos emitidos por ese despacho no protegen los derechos de autodeterminación informativa, por lo que recomendamos que sean revisados para que se ajusten al bloque de constitucionalidad que hemos citado.

## ANÁLISIS JURÍDICO

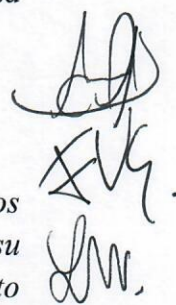
### Sobre la confidencialidad.

1. El decreto pretendía garantizar la confidencialidad de la información que se le transfiriera a la UPAD, pero no definía con detalle cómo se protegería esa información, quiénes serían los responsables de custodiarla y cuáles serían las consecuencias por violar ese deber de confidencialidad.

Una de las funciones de UPAD era resguardar la confidencialidad y se obligaba a los funcionarios a guardar ese deber, el cual se mantendría aún después de finalizada la relación con UPAD, lo que va en concordancia de lo contenido en el artículo 11 de la ley N° 8968, sobre el deber de confidencialidad de las personas que tengan acceso a los datos en razón de su función.

*“ARTÍCULO 11.- Deber de confidencialidad*

*La persona responsable y quienes intervengan en cualquier fase del tratamiento de datos personales están obligadas al secreto profesional o funcional, aun después de finalizada su relación con la base de datos. La persona obligada podrá ser relevado del deber de secreto por decisión judicial en lo estrictamente necesario y dentro de la causa que conoce.”*


El decreto no contiene ninguna referencia a normativa disciplinaria interna sobre las consecuencias en el caso de violación de dicho acuerdo de confidencialidad y con la información que tenemos disponible no es claro si a los funcionarios se les ha comunicado las consecuencias de la violación del deber de confidencialidad.

Con el fin de procurar un uso más seguro de los datos, el decreto establecía que se deberían elaborar “*acuerdos de gobernanza con las instituciones que les transfieran información, para garantizar así un uso responsable y coherente de los datos que beneficie a los ciudadanos y fortalezca la confianza pública*”. En este sentido, es importante que los órganos que están realizando investigación de este caso, exijan acuerdos para verificar que se está cumpliendo con este deber, en los casos en donde se encuentre ante transferencias en cumplimiento de la ley.

Se creó un cargo de Director de Análisis de Datos que, para efectos del posterior decreto, tendría equivalencia a la función que tiene un director de datos (“Chief Data Officer”); sin embargo, cuando en el artículo 10 detalló el perfil técnico, en ningún momento se mencionó la experiencia sobre protección en materia de datos personales, legal o informática, por lo que es difícil que en la práctica se pudieran cumplir las funciones, principios y objetivos vinculados con la confidencialidad mencionados en el decreto.

De acuerdo con el decreto, el director de UPAD era el encargado de hacer cumplir el marco jurídico sobre protección de datos personales, pues se indicaba que cumpliría la función de un “Chief Data Officer”.

El autor Daniel Trejos Medina, en su obra “[Big data, una oportunidad de mejora en las organizaciones](#)”, describe la función del Chief Data Officer de la siguiente manera:

*“El chief data officer tiene como función el unir la rendición de cuentas y **responsabilidad en lo que se refiere a protección, privacidad y gobierno de información, calidad de datos y gestión del ciclo de vida de los datos**<sup>2</sup>, para lograr que mediante la utilización de los activos de datos se pueda crear un valor para la organización. A diferencia del director de información, el chief data officer está vinculado con los riesgos, cumplimiento, gestión de políticas y funciones del negocio con origen en los datos. No es un sustituto o competidor del director de tecnología o información. El director de datos en las organizaciones donde existe, reporta al director general, es un rol similar al director de calidad, desde el punto de vista operativo pueden listarse cuatro áreas u objetivos en los cuales empoderar a su organización. Las cuales son: definir una estrategia, ejecutar una gobernanza o al menos un gobierno de datos, definir una arquitectura de datos y finalmente analizar los datos en beneficio de la organización.”* (TREJOS MEDINA, 2018)

#### **Datos confidenciales.**

<sup>2</sup> La negrita no corresponde a la fuente original.

Handwritten signatures and initials in the right margin, including a large scribble at the top, a signature below it, and several other initials and marks at the bottom right.



Es necesario aclarar que **los datos confidenciales o secretos pueden ser de tipo sensible o de acceso restringido**. En ninguno de los dos casos la ley permite su tratamiento salvo las excepciones que contempla la Ley de Defensa de la Persona frente al Tratamiento de su Datos Personales No.8968 de 7 de julio de 2011; que no se aplican dentro de los criterios definidos por el decreto ejecutivo en estudio.

Debemos recordar que los datos personales, como su nombre lo indica, pertenecen a la persona. Es la titular y propietaria de esos datos, no el Estado, ni un Ministerio, oficina, ni ningún organismo, Gobierno o institución pública o privada. Los datos de acceso restringido o confidencial que también se consideran contemplados en esta categoría son, entre otros, la dirección exacta de la residencia, 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, de acuerdo con la legislación correspondiente.

En caso de que la UPAD haya obtenido datos personales, es importante señalar que los principios de la autodeterminación informativa prohíben la recopilación o transferencia de datos de manera ilícita o fraudulenta, así como el acopio de datos sin el consentimiento informado de la persona, o bien, adquiridos por medios fraudulentos, desleales o ilícitos, todo ello de acuerdo con el artículo 5 de la ley No.8968 ya citada, además de las protecciones que se otorgan en el bloque de constitucionalidad visto antes.

No se indica en el decreto tampoco las maneras de procesamiento de la información, los algoritmos utilizados para cruzar la información, los programas utilizados ni la custodia de los datos confidenciales obtenidos de entes públicos.

Tampoco se definió por qué es necesario obtener información confidencial para elaborar políticas públicas, **si las estadísticas y datos públicos pueden ser empleados con ese propósito**, con la única limitación de que no pueda identificarse al individuo.

#### **Transferencia de datos personales entre instituciones públicas y protocolos de actuación.**

De acuerdo con la ley No 8968, en su artículo 3, inciso h), se define al responsable de la base de datos de la siguiente manera: "*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.*"

Por lo que, para nuestro legislador, cada entidad es responsable de sus bases de datos, las cuales deben estar adecuadas a un fin y la transferencia de datos personales; entre ellas deben contar con el consentimiento del titular, como se ha mencionado supra, o por una disposición legal que les permita realizar dicha transferencia.

Handwritten signatures and initials in the right margin, including a large scribble at the top, and several smaller signatures below it, including one that appears to be 'GW' and another that looks like 'García'.

En octubre del año del 2017, la Licda. Wendy Rivera Román, en su calidad de directora de la Agencia de Protección de Datos de los Habitantes (PRODHAB), emitió una opinión jurídica de carácter no vinculante, oficio APD-OJ-016-10-2017, dirigida al Lic. Wagner Granados Chaves, jefe a.i del departamento legal del Tribunal Supremo de Elecciones, con respecto a la transferencia de datos personales entre instituciones públicas:

*“Busca el legislador con esta norma que toda transferencia de datos se efectúe, cumpla con el respeto del derecho del titular de los mismos a brindar su consentimiento, siendo que es quien puede validar su transferencia. De igual forma, es mediante el Reglamento de Protección de la Persona Frente al Tratamiento de sus Datos personales, Decreto N° 37554-JP, en sus artículos 30, 31 y 32 que se establece las responsabilidades de los encargados de las bases de datos...”*

Ante el caso de UPAD, la actual directora nacional de PRODHAB, la señora Elizabeth Mora, manifiesta un cambio de criterio al emitir un comunicado de prensa, el cual posteriormente fue dejado sin efecto, con la siguiente explicación: «No existe una prohibición legal para que la información pueda ser compartida, siendo que la ley 8968 establece excepciones y una de ellas es la actividad ordinaria de la administración», lo cual es violatorio, de inicio, con el Principio de Legalidad.

Esta Comisión considera que debe aplicarse el artículo 14 de la ley No.8968 sobre transferencia de datos, y no las excepciones previstas en el artículo 8, incisos e) y f).

Además, deben revisarse cuidadosamente los criterios jurídicos emitidos por la Prodhav pues en primera instancia aparece justificando el decreto de creación de la UPAD, apelando a razones jurídicas totalmente equivocadas, especialmente en lo que se refiere a la desaplicación del Principio de Legalidad, cuyo cumplimiento se ordena en el artículo 11 de la Constitución Política, así como en el numeral 11 de la Ley General de la Administración Pública No.6227 de 4 de mayo de 1978, según hemos citado.

Por lo anterior, se echa de menos la actuación que debió tener la Prodhav, toda vez que es función primordial de esta Agencia su actuación oficiosa en resguardo de los datos personales cuyos titulares son los ciudadanos, no el Estado.

Además, los criterios de la Prodhav muestran una preocupante confusión en cuanto a la naturaleza de los datos confidenciales, ya de por sí contemplados en la ley No.8968 como datos sensibles o datos de acceso restringido, al indicar que los datos confidenciales no se encuentran incluidos en la ley No.8968.

#### **ALOJAMIENTO DE DATOS PERSONALES EN SERVIDORES EN EL EXTRANJERO.**

Es por todos conocido que el gobierno de la República creó una cuenta en el sitio privado Tableau Public, en la dirección <https://public.tableau.com/profile/presidencia.costa.rica#!/>, y donde al menos un servidor que aloja el contenido se encuentra en Massachusetts, Estados

Unidos<sup>3</sup>. En la política de datos de dicho servicio se manifiesta lo siguiente:

*“No debe publicar datos confidenciales que no quiera divulgar, como el plan de ventas de una empresa o su información financiera personal. Una vez publicados, esos datos ya no serán privados”.*

Es preocupación de esta Comisión que dicho sitio Web haya sido alimentado con datos personales de los ciudadanos, y no solamente con datos estadísticos públicos que no tienen restricción alguna. Sin embargo, de haberse subido los datos personales en un servidor privado que está en el extranjero, sin autorización del titular y por vías que no aseguran su privacidad, se habría cometido una falta gravísima de acuerdo con el artículo 31, inciso f), y una falta leve de acuerdo con el artículo 29, inciso b), de la Ley.

Por lo tanto, es importante que el órgano competente para realizar esta investigación, la Prodhav, actúe de oficio. De igual manera, es importante que la Defensoría de los Habitantes utilice todos los mecanismos legales con los que cuenta para que la Prodhav cumpla las funciones que se le han otorgado en la ley.

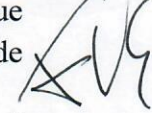
## **VIOLACIÓN DE DATOS PERSONALES**

Debido a la investigación penal que ha iniciado el Ministerio Público sobre este caso y la posibilidad de que las conductas encuadren dentro del tipo penal de violación de datos personales, no nos referiremos a este aspecto.

## **CONCLUSIONES.**

- 1.- La transferencia de datos personales, sean sensibles o de acceso restringido, requiere del consentimiento del titular de los datos o una norma legal expresa que faculte este tratamiento.
- 2.- Cualquier solicitud, recopilación o transferencia ilegal de datos personales debe ser investigada por la Agencia de Protección de Datos de los Habitantes, quien tiene la facultad legal de actuar de oficio.
- 3.- El alojamiento de datos personales en servidores privados que se encuentren en el extranjero requieren del consentimiento del titular de los datos.
- 4.- Esta Comisión considera que deben revisarse los criterios jurídicos emitidos por la Prodhav, relativos a la transferencia de datos personales con fundamento en las excepciones que contempla el artículo 8, incisos e) y f), porque considera que son contrarios al bloque de legalidad.

<sup>3</sup> De acuerdo a consulta en Domain Tools, en página Whois Record para Tableau.com, obtenida el 2 de marzo, 2020 de <https://whois.domaintools.com/tableau.com>



## RECOMENDACIONES

### REFORMAS A LA CONSTITUCIÓN POLÍTICA Y A LAS LEYES SOBRE LA MATERIA.

- 1.- A pesar de ser un derecho ampliamente reconocido como derivado del artículo 24 de la Constitución Política, recomendamos su reforma para que se extienda el haz de protección constitucional del artículo a los datos personales de los ciudadanos en forma expresa.
- 2.- Igualmente, que la reforma a dicho artículo, abarque una aclaración en el sentido de que, cuando se hable de ley, se entienda que, en cualquier supuesto, esta deberá ser aprobada por mayoría de dos tercios de los diputados, y que su debida aplicación requerirá de la intervención de un juez.
- 3.- Recomendamos reformar el artículo 8 de esta ley 8968 con el propósito de suprimir la posibilidad de cualquier interpretación contraria al artículo 24 de la Constitución Política y a la ley 8968.
- 4.- Recomendamos revisar la legislación existente con el propósito de suprimir cualquier norma que atente contra la autodeterminación informativa, incluyendo la responsabilidad de los jefes de las instituciones que resguarden y/o den tratamiento a los datos personales de los ciudadanos.
- 5.- Recomendamos que los entes receptores de información confidencial, deban tener todos los protocolos, obligaciones y garantías en los sistemas y procedimientos para custodiar la información confidencial recibida o custodiada, de una manera tan estricta o más que el ente que la custodia y al que le ha sido solicitada.
- 6.- Recomendamos que la PROHAB, si no lo tiene, haga un inventario exhaustivo de los órganos o entes públicos que resguardan datos personales y analice la calidad de las medidas de protección, y analice las medidas para evitar la utilización de equipo personal.
- 7.- Analizar la posibilidad de trasladar la Agencia de Protección de Datos de los Habitantes - PRODHAB - fuera del Poder Ejecutivo.

### RECOMENDACIONES ESPECÍFICAS

#### PARA EL COLEGIO DE ABOGADOS Y ABOGADAS.

- 1.- A manera de urgencia, proponer a la Asamblea Legislativa, un proyecto de ley que garantice la independencia de la Agencia de Protección de Datos de los Habitantes PRODHAB para poder fiscalizar las infracciones a normativa de datos personales por parte del gobierno, tal y como en el caso UPAD.

Handwritten signatures and initials on the right side of the page, including a large signature at the top, several smaller initials in the middle, and a signature at the bottom right.

2.- Iniciar un proceso de discusión con la Asamblea legislativa, Gobierno y los diferentes sectores con el fin de crear una normativa robusta en protección de datos personales.

3.- Promover ante la Asamblea Legislativa la ratificación del Convenio 108 del Consejo de Europa sobre Protección de Datos Personales por parte de Costa Rica.

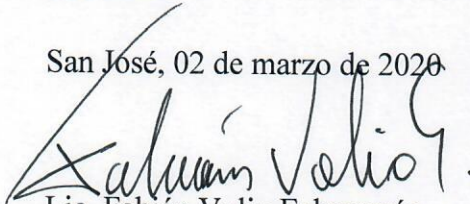
4.- Trabajar en conjunto con el gobierno en un compromiso en una moratoria en todos los proyectos que involucren reconocimiento facial y de datos personales en cámaras de videovigilancia, hasta que no se apruebe una ley sobre cómo deben regularse estos temas.

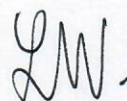
#### **PARA LA DEFENSORÍA DE LOS HABITANTES.**

1.- Iniciar una investigación sobre el posible incumplimiento de la PRODHAB de sus funciones y los cambios de criterio contrario a la legislación vigente y ponerlo en conocimiento de las autoridades que correspondan.

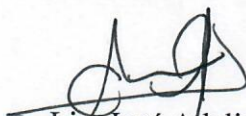
2.- Darle seguimiento a la investigación que deberá realizar la PRODHAB con respecto al caso de UPAD, con el fin de que haga cumplir la normativa vigente sobre protección de datos personales.

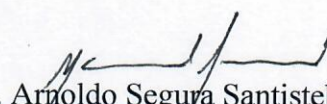
San José, 02 de marzo de 2020


  
Lic. Fabián Volio Echeverría

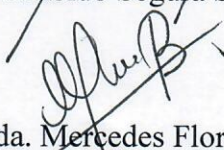


Lic. León Weinstok Mendelewicz

  
Lic. José Adalid Medrano Melara

  
Lic. Arnoldo Segura Santisteban

  
Lic. Álvaro Sánchez González

  
Licda. Mercedes Flores Badilla