Estudio Centroamericano de Protección de Datos,

COSTA RICA

Mauricio París Cruz

Diagramación: Isabel Valladares
Edición: Raúl Altamar
Coordinación: Sara Fratti
Autoría: Mauricio París Cruz

Enero 2019.

IPANDETEC
INSTITUTO PANAMEÑO DE DERECHO Y NUEVAS TECNOLOGÍAS

Instituto Panameño de Derecho y Nuevas Tecnologías -IPANDETEC- es una organización sin fines de lucro basada en la Ciudad de Panamá, que promueve el uso y regulación de las TIC y la defensa de los Derechos Humanos en el entorno digital, a través de la incidencia, investigación, monitoreo y seguimiento legislativo de Políticas Públicas de Internet en Centroamérica.

1. Marco jurídico constitucional

Las garantías constitucionales que conforman el conjunto de derechos relacionados con la intimidad en Costa Rica son los artículos 23, 24 y 28 de la Constitución Política, que son a su vez el fundamento del derecho a la protección de los datos personales.

ARTÍCULO 23.- “El domicilio y todo otro recinto privado de los habitantes de la República son inviolables. No obstante, pueden ser allanados por orden escrita de juez competente, o para impedir la comisión o impunidad de delitos, o evitar daños graves a las personas o a la propiedad, con sujeción a lo que prescribe la ley”.

ARTÍCULO 24.- “Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones”.

Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República. Sin embargo, la ley, cuya aprobación y reforma requerirá los votos de dos tercios de los Diputados de la Asamblea Legislativa, fijará en qué casos podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento.

Igualmente, la ley determinará en cuáles casos podrán los Tribunales de Justicia ordenar que se intervenga cualquier tipo de comunicación, e indicará los delitos en cuya investigación podrá autorizarse el uso de esta potestad excepcional y durante cuánto tiempo. Asimismo, señalará las responsabilidades y sanciones en que incurrirán los funcionarios que apliquen ilegalmente esta excepción. Las resoluciones judiciales amparadas a esta norma deberán ser razonadas y podrán ejecutarse de inmediato. Su aplicación y control serán responsabilidad indelegable de la autoridad judicial.

La ley fijará los casos en que los funcionarios competentes del Ministerio de Hacienda y de la Contraloría General de la República podrán revisar los libros de contabilidad y sus anexos para fines tributarios y para fiscalizar la correcta utilización de los fondos públicos. Una ley especial, aprobada por dos tercios del total de los Diputados, determinará cuáles otros órganos de la Administración Pública podrán revisar los documentos que esa ley señale en relación con el cumplimiento de sus competencias de regulación y vigilancia para conseguir fines públicos. Asimismo, indicará en qué casos procede esa

revisión. No producirán efectos legales, la correspondencia que fuere sustraída ni la información obtenida como resultado de la intervención ilegal de cualquier comunicación."

ARTÍCULO 28.- "Nadie puede ser inquietado ni perseguido por la manifestación de sus opiniones ni por acto alguno que no infrinja la ley. Las acciones privadas que no dañen la moral o el orden públicos, o que no perjudiquen a tercero, están fuera de la acción de la ley. No se podrá, sin embargo, hacer en forma alguna propaganda política por clérigos o seglares invocando motivos de religión o valiéndose, como medio, de creencias religiosas".

Por otra parte, el Hábeas Data no está regulado como tal en nuestro ordenamiento jurídico. No obstante, la Sala Constitucional lo ha admitido en su jurisprudencia como una modalidad del recurso de amparo: "IV.- La Sala Constitucional se refirió por primera vez al concepto 'hábeas data' como instrumento de tutela del derecho a la autodeterminación informativa en la sentencia N° 4154-97 de las 19:30 horas del 16 de julio de 1997, en los siguientes términos: (...). El recurso de amparo, en la modalidad de hábeas data, tutela el derecho de una persona de conocer o rectificar toda la información pública o privada que exista sobre ella, incluso la que no haya sido utilizada ni haya de serlo en su perjuicio (...). Es importante señalar que, en esta resolución, la Sala aceptó la existencia del hábeas data como una modalidad del recurso de amparo...". Voto 08369-2003

No obstante lo anterior, a partir de la entrada en vigencia de la Ley pero en especial de la entrada en funciones de la Agencia de Protección de Datos de los Habitantes, la Sala Constitucional ha establecido:

"Esta Sala, bajo una mejor ponderación estima que ahora los habitantes cuentan con un mecanismo celero, oportuno y especializado para garantizar su derecho a la autodeterminación informativa en relación con su vida o actividades privadas 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. Así las cosas, en tesis de principio, esta Sala remite a esa instancia administrativa los asuntos en donde se alegue la violación del derecho de comentario, reservándose el conocimiento, únicamente, de aquellos asuntos en los que habiendo acudido ante la Agencia de Protección de Datos de los Habitantes, no se haya encontrado amparo a ese derecho". 2015-002279

En algunos casos la Sala Constitucional sigue arrogándose el conocimiento de casos que entran dentro del ámbito de aplicación de la Ley, siendo el análisis de competencia muy casuístico.

2. Marco jurídico ordinario

La Ley de Protección de la persona frente al tratamiento de sus datos personales es la Ley N. 8968 del 7 de julio del 2011, publicada en la Gaceta N. 170 del 5 de setiembre de 2011 con su Reglamento establecido por el Decreto Ejecutivo No. 37554-JP.

3. Definición de datos personales y datos sensibles

Contenida en el Art. 3 de la Ley. 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”.

Establece este inciso que para que un dato sea considerado de acceso irrestricto así debe disponerse en una ley especial. A la fecha no se ha promulgado legislación que expresamente delimite cuáles datos personales tienen esta condición. Consideramos que este es un doble error legislativo: a) Por una parte, pareciera innecesario hacer reserva de ley para un tema tan puntual, y debería permitirse que la condición de datos irrestrictos se realizara mediante un decreto ejecutivo, lo cual debería ser la forma también en la que se creen bases de datos en las instituciones del Estado; y b) Si se consideraba que la reserva de ley era necesaria o conveniente, por economía procesal el legislador debió incluir en esta misma Ley cuáles son las bases de datos que contarían con esta condición, en vez de hacer referencia a una legislación futura e incierta.

Pese a no existir ley especial, entendemos que dentro de los supuestos de esta norma se encontrarían, por ejemplo, a los datos de nacimiento, defunción, estado civil o domicilio electoral contenidos en el Registro Civil, el registro de morosidad patronal de la Caja Costarricense del Seguro Social, o los diversos Registros que componen el Registro de la Propiedad. El hecho de que para acceder a estos datos se pueda requerir la creación de un usuario y contraseña no es un elemento relevante, siempre y cuando cualquier persona pueda obtener una cuenta con el fin de acceder a datos personales. Habría sido deseable que la Ley o el Reglamento enlistaran cuáles de las bases de datos que hoy, de facto, son de acceso irrestricto mantendrían dicha condición una vez promulgada la Ley.

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".

Como ejemplo podría pensarse en las declaraciones de impuestos, o las planillas que se reportan a la Caja Costarricense del Seguro Social, así como la información que se encuentra bajo custodia del Archivo Judicial.

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".

Entrarían en esta definición registros tales como los expedientes médicos, los registros de afiliación a partidos políticos o a sindicatos, o incluso los registros mantenidos por organizaciones religiosas, tal como el registro de bautismo de la Iglesia Católica, entre otros.

4. Principios de tratamiento de datos personales

A. Legalidad: El tratamiento de los datos personales de los ciudadanos debe realizarse de conformidad con el marco legal existente en el país para tales efectos, en especial la Constitución Política y la Ley No. 8968 y su Reglamento.

B. Calidad: El Art. 6 de la Ley establece el Principio de Calidad de la información en estos términos: "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".

C. Transparencia: Es el equivalente al principio de acceso a la información en el tanto todo titular tiene derecho a acceder a sus datos personales, conocer el fin para el que se utilizan y el responsable de la base de datos.

D. Finalidad: Previo a recolectar datos personales el fin con el cuál se realiza dicha recolección debe ser determinado y manifestado al titular de los datos personales.

E. Exactitud: Los datos de carácter personal deberán ser exactos. La persona responsable de la base de datos tomará las medidas necesarias para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados. Si los datos de carácter personal registrados resultan ser inexactos en todo o en parte, o incompletos, serán eliminados o sustituidos de oficio por la persona responsable de la base de datos, por los correspondientes datos rectificados, actualizados o complementados.

F. Limitación al plazo de conservación: El Derecho al Olvido está consagrado en el artículo 11 del Reglamento, y especifica de manera clara que se entenderá como "Derecho al olvido, la conservación de los datos personales, que puedan afectar a su titular, pero que no podrán exceder el plazo diez años; esto desde la fecha de ocurrencia de los hechos registrados, salvo disposición normativa especial que establezca otro plazo o porque el acuerdo de las partes haya establecido un plazo menor. Nuevamente se indica que en caso de que sea necesaria su conservación, más allá del plazo estipulado, deberán ser desasociados los datos personales de su titular".

G. Confidencialidad: La fidelidad, la discreción y el deber de secreto de todos aquellos que intervengan en las fases del tratamiento de datos son especialmente importantes. El Art. 11 de la Ley establece: "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".

5. Derechos ARCO

A. Acceso: A través del ejercicio de este derecho el titular de los datos personales puede verificar si existen datos personales suyos en una base de datos, qué datos de carácter personal están siendo tratados por parte de terceros, la finalidad de ese tratamiento, el origen de los citados datos, la forma en la cual se almacenan y si se han transferido o se van transferir a un tercero.

B. Rectificación: Es la posibilidad del titular de los datos personales de modificar aquellos datos que sean inexactos o incompletos, debiendo en la solicitud de rectificación indicar qué datos desea que se modifiquen.

C. Cancelación: Toda persona puede solicitar y obtener del responsable del manejo de los datos personales la eliminación de su información privada, en cualquier momento y circunstancia. Dentro de este derecho se incluye el derecho al olvido, el cual consiste en la obligación que tiene todo responsable de una base de datos personales de suprimir los aquellos que le puedan afectar a su titular por un plazo máximo de 10 años. Lo anterior implica que este tipo de datos debe ser eliminada por su almacenador, aún no medie solicitud del titular de estos.

D. Oposición: Aunque no está expresamente incorporado como tal, se entiende como un derivado del derecho de autodeterminación informativa que se garantiza como un derecho fundamental, con el objeto de controlar el flujo de informaciones que conciernen a cada persona en los términos del artículo 4 de la Ley.

6. Consentimiento

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".

El consentimiento es el principio básico para el tratamiento de los datos personales. Ahora bien, el derecho fundamental a la protección de datos no es de carácter absoluto, sino que debe ponderarse junto con otros derechos fundamentales tales como el derecho a la información, protección de la salud, seguridad nacional u otros intereses públicos.

Dado que el deber de información es uno de los principios que fundamentan la protección de datos en Costa Rica, este establece un derecho del titular de los datos de ser informado, y al mismo tiempo un deber del responsable de la base de datos de informar tales aspectos, recayendo en este último la carga de la prueba de haber informado oportunamente al titular de todo lo indicado en este artículo.

Es importante aclarar que la información debe entregarse al titular de los datos o a su representante, lo cual implica que en casos de datos personales de menores de edad o incapaces, dicha comunicación debe ser realizada a sus padres, tutores o representantes, según sea el caso.

El Art. 5 del Reglamento establece "formalidades del consentimiento", y señala que debe ser otorgado en un documento físico o electrónico, que debe ser de fácil compresión, gratuito y debidamente identificado.

Los artículos 7, 8 y 9 del Reglamento desarrollan la revocación del consentimiento, fijando el Art. 8 un plazo de 5 días hábiles a partir de su recepción para que el responsable de la base de datos proceda conforme a su aplicación.

7. Sujetos obligados

Encargado: Toda persona física o jurídica, entidad pública o privada, o cualquier otro organismo que da tratamiento a los datos personales por cuenta del responsable de la base de datos.

Responsable: Toda persona física o jurídica, pública o privada, que administre o, gerencie o, se encargue o, sea propietario, de una o más bases de datos públicas o privadas, 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 les aplicarán.

Intermediario tecnológico o proveedor de servicios: Persona física o jurídica, pública o privada que brinde servicios de infraestructura, plataforma, software u otros servicios.

8. Transferencia y cesión de datos

Determinar si existen disposiciones sobre la transferencia y cesión de datos, qué condiciones se establecen.

El Art. 2 de la Ley define transferencia como “Acción mediante la cual se trasladan datos personales, a un responsable de Base de Datos Personales o un tercero”.

Esta definición se ve precisada en el Reglamento que la define 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”.

El Art. 14 de la Ley establece “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”.

En efecto, el Art. 40 del Reglamento establece que no se considera trasferencia el traslado de datos personales del responsable de una base de datos a un encargado, proveedor de servicios o intermediario tecnológico o las empresas del mismo grupo de interés económico.

Asimismo, ese mismo artículo establece que la transferencia requerirá siempre el consentimiento inequívoco 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 Reglamento disponen. El Art. 41 del Reglamento también estipula que la transferencia debe realizarse bajo fiel cumplimiento de los protocolos mínimos de actuación debidamente inscritos ante Prodhab. La carga de la prueba sobre la legalidad de la transferencia recae sobre el responsable (Art. 42 del Reglamento), y deberá estar respaldada en un contrato con el responsable receptor en el que se prevean al menos las mismas obligaciones a las que se encuentra sujeto el responsable de la transferencia de los datos (Art. 43 del Reglamento).

9. Autoridad competente

La Agencia de Protección de Datos de los Habitantes (Prodhab) es el órgano de desconcentración máxima adscrito al Ministerio de Justicia y Paz. Tiene personalidad jurídica instrumental propia en el desempeño de las funciones que le asigna la ley, además de la administración de sus recursos y presupuesto, así como para suscribir los contratos y convenios que requiera para el cumplimiento de sus funciones. La Agencia goza de independencia de criterio.

La Dirección de la Prodhab está a cargo de un director o una directora nacional, quien deberá contar, al menos, con el grado académico de licenciatura en una materia afín al objeto de su función y ser de reconocida solvencia profesional y moral.

No podrá ser nombrado director o directora nacional quien sea propietario, accionista, miembro de la junta directiva, gerente, asesor, representante legal o empleado de una empresa dedicada a la recolección o el almacenamiento de datos personales. Dicha prohibición persistirá hasta por dos años después de haber cesado sus funciones o vínculo empresarial. Estará igualmente impedido quien sea cónyuge o pariente hasta el tercer grado de consanguinidad o afinidad de una persona que esté en alguno de los supuestos mencionados anteriormente.

10. La computación en la nube y los servicios financieros

En Costa Rica, el manejo de datos personales referentes al comportamiento crediticio se rige por las normas que regulan el Sistema Financiero Nacional. Lo anterior se encuentra contemplado en el artículo 9.4 de la Ley, el cual que hace una advertencia: “dicha normativa debe garantizar un grado de riesgo aceptable por parte de las entidades financieras, sin limitar el pleno ejercicio del derecho a la autodeterminación informativa ni exceder los límites de la Ley”.

Por lo tanto, la Ley establece los parámetros mínimos al manejo de datos personales en los servicios financieros. Además de estos parámetros mínimos, existe una serie de Reglamentos que regula la protección de datos personales en esta materia, así como el uso de herramientas en la nube por las entidades bancarias, entre los cuales destaca el Reglamento General de Gestión de la Tecnología de Información, del Consejo Nacional de Supervisión del Sistema Financiero.

De acuerdo al artículo 1 de este Reglamento, el objeto de la norma es establecer los requerimientos mínimos para la gestión de la tecnología de información que deben acatar las entidades supervisadas y reguladas del Sistema Financiero costarricense. El Reglamento contiene regulaciones relacionadas a: (i) la organización de las tecnologías de información; y (ii) la supervisión y auditoría externa de las tecnologías de información. Asimismo, esta norma se complementa con los Lineamientos Generales al Reglamento General de Gestión de la Tecnología de Información, que servirá para determinar la forma de aplicar el Reglamento.

Del Reglamento destaca la regulación sobre el manejo de las bases de datos, contenido en el artículo 19, el cual establece que todas las bases de datos deben estar accesibles al ente supervisor correspondiente, sin ningún tipo de restricción o condición. Por otra parte, en caso de que el control de la base de datos esté encargado a un tercero, exige que exista un contrato entre la entidad y el proveedor, que deberá respetar las disposiciones de la Ley.

Finalmente, dicho numeral permite que el procesamiento y acceso a las bases de datos se dé a través de servicios de computación en la nube, siempre y cuando se cumpla con los requisitos legales, de seguridad y de acceso del supervisor. En este último caso, se entiende que el uso de herramientas en la nube deberá respetar todos los derechos contemplados en la Ley.

El Reglamento del Centro de Información Crediticia resulta de importancia en el manejo de datos personales, pues regula el marco general del Centro de Información Crediticia. En este Reglamento se reconoce el derecho de autodeterminación informativa en esta materia, al establecer en su artículo 7 la necesidad de que haya autorización previa del titular de los datos para dar acceso a reportes individuales de información crediticia. Asimismo, se regula el procedimiento para revocar dicha autorización (art. 8), así como el derecho a obtener reportes sobre la información que el Centro de Información Crediticia almacena (art. 11) y solicitar su modificación (art. 12).

11. Agenda Digital

La Agenda Digital es una estrategia que adoptan los gobiernos de los países con el objetivo de desarrollar su economía y su sociedad digital, por la cual pasa todo lo relativo a inversiones, mejoras y desarrollos del sector de telecomunicaciones y de la Sociedad de la Información. En esta Agenda Digital los países se siguen un programa de objetivos e hitos concretos para la implementación y crecimiento de las tecnologías de la información y comunicación (TIC) en sus respectivas jurisdicciones.

El Gobierno de Costa Rica ha realizado múltiples esfuerzos en lograr alcanzar los objetivos de la Agenda Digital para América Latina y el Caribe eLAC2018, la cual fue aprobada en 2015 en México. Se trata de una estrategia regional de políticas digitales fijada con la mira en el año 2018. La Agenda Digital en mención contiene cinco áreas de acción, entre las cuales destacan las siguientes para efectos del presente reporte:

- **Economía digital, innovación y competitividad.** En esta sección la Agenda Digital señala cuatro objetivos entre los cuales destacan: (i) desarrollar y promover la industria de las TIC tradicional, como en sectores emergentes, para la producción de contenidos, bienes y servicios digitales; (ii) aumentar la productividad, el crecimiento y la innovación de los sectores productivos mediante el uso de las TIC; y (iii) potenciar la economía digital y el comercio electrónico a nivel nacional, adaptando las regulaciones de protección al consumidor y de protección de datos al entorno digital.

- **Gobernanza para la sociedad de la información.** Entre los cinco objetivos de esta sección resalta el hecho de que promover la seguridad y la confianza en el uso de Internet, garantizando el derecho a la privacidad y a la protección de los datos personales esté dentro de los objetivos de la Agenda Digital.

Por ende, se puede afirmar que los objetivos de la Agenda Digital están íntimamente relacionados con el derecho a la privacidad y a la protección de los datos personales, siendo estos temas clave para el crecimiento de los países en la utilización de las TIC. La existente legislación en materia de Protección de Datos no es un objetivo por sí misma, sino que la Agenda Digital considera que esta, adaptada al entorno digital, puede ser potenciadora de la economía digital y promueve la competitividad dentro del mercado nacional y regional.

Costa Rica, al contar con legislación sobre el tema, cumple con los objetivos de la Agenda Digital, aunque se afirma que esta no regula aspectos específicos del comercio electrónico, lo cual constituye una cuenta pendiente para el país.

Referencias

Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales. Ley No. 8968 del 7 de julio de 2011. Publicada en el Diario Oficial "La Gaceta" No. 170 del 5 de setiembre de 2011. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.

Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales. Decreto Ejecutivo No. 37554-JP de 30 de octubre de 2012. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.

Agenda Digital para América Latina y el Caribe (eLAC2018). Comisión Económica Para América Latina y el Caribe. Naciones Unidas. 7 de agosto de 2015. Disponible en: https://repositorio.cepal.org/bitstream/handle/11362/38886/S1500758_es.pdf?sequence=1&isAllowed=y

Monitoreo de la Agenda Digital para América Latina y el Caribe eLAC2018. Comisión Económica Para América Latina y el Caribe. Naciones Unidas. Abril de 2018. Disponible en: https://repositorio.cepal.org/bitstream/handle/11362/43444/1/S1800256_es.pdf

Reglamento General de Gestión de la Tecnología de Información. Consejo Nacional de Supervisión del Sistema Financiero. 17 de abril de 2017. Disponible en: https://www.sugef.fi.cr/normativa/normativa_vigente/documentos/SUGEF%2014-17%20(v2_%2017abr2017).pdf

Reglamento del Centro de Información Crediticia. Consejo Nacional de Supervisión del Sistema Financiero. 11 de mayo de 2015. Disponible en: https://www.sugef.fi.cr/normativa/normativa_vigente/documentos/SUGEF%207-06%20(v8%20%20%20mayo%202015).pdf