Estudio Centroamericano de Protección de Datos,

HONDURAS

Eduardo Tomé

Diagramación: Isabel Valladares
Edición: Raúl Altamar
Coordinación: Sara Fratti
Autoría: Eduardo Tomé

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

Desde un punto de vista constitucional, la legislación hondureña garantiza el derecho a la intimidad personal y la inviolabilidad de las comunicaciones.

La Constitución hondureña añadió a su lista de recursos el Hábeas Data en el 2015 (Art 182 no. 2). Sin embargo, el conocimiento de este recurso se enfoca exclusivamente a la Sala de lo Constitucional de la Corte Suprema de Justicia. Esto limita el acceso a la población general al acceso a la interposición de este recurso, ya que la Corte Suprema solamente tiene sede en la ciudad capital y este recurso debe ser interpuesto directamente por la persona cuya información es la que consta en los registros.

Honduras es un país con casi 9 millones de habitantes y es importante tomar en cuenta que la Sala Constitucional solamente cuenta con 4 magistrados, quienes también conocen los recursos de Amparo, Revisión, Inconstitucionalidad y Hábeas Corpus. Es irrisorio pensar que cuentan con la capacidad para darle una pronta resolución a los recursos presentados sin poder garantizar la seguridad jurídica a la ciudadanía de manera efectiva.

En los siguientes artículos de la Constitución Hondureña se determina cómo se encuentran regulados diferentes derechos relacionados a esta materia:

Artículo 76. "Se garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen".

En este caso se garantiza el derecho a la intimidad y a la propia imagen. Sin embargo, este segundo precepto es de los más violentados, en vista de que a diario la Policía Nacional de Honduras exhibe a las personas capturadas sospechosas de cometer delitos comunes ante los medios de comunicación. Esto también violenta de cierta manera la presunción de inocencia, debido a que esto los presenta como culpables ante la sociedad y en casos muy puntuales se ha acusado a personas de cometer crímenes horrendos, como masacres o parricidios, para después terminar absueltos en el proceso.

Artículo 100. "Toda persona tiene derecho a la inviolabilidad y al secreto de las comunicaciones, en especial de las postales, telegráficas y telefónicas, salvo resolución judicial. Los libros y comprobantes de los comerciantes y los documentos personales únicamente estarán sujetos a inspección o fiscalización de la autoridad competente, de conformidad con la Ley. Las comunicaciones, los libros, comprobantes y documentos a que se refiere el presente artículo, que fueren violados o sustraídos, no harán fe en juicio. En todo caso, se guardará siempre el secreto respecto de los asuntos estrictamente privados que no tengan relación con el asunto objeto de la acción de la autoridad." [1]

[1] Asamblea Nacional Constituyente. Constitución Política de 1982, Decreto N 131. Disponible en http://www.poderjudicial.gob.hn/CEDIJ/Leyes/Documents/

Sin embargo, esto no siempre es respetado por el Estado, y no solamente en los habituales casos de arbitrariedades cometidas contra activistas, defensores de derechos humanos y periodistas contrarios al gobierno. Recientemente hubo una escalada de esta situación en la cual los miembros de la Junta Nominadora, encargada de elegir a los candidatos para las Magistratura actual de la Corte Suprema de Justicia, denunciaron la intervención de sus teléfonos personales, así como la instalación de cámaras ocultas en la sede de la Junta. Esto fue calificado por uno de sus miembros como una medida de presión externa y un atropello a sus garantías fundamentales.

El Estado reconoce la garantía de Hábeas Corpus o de exhibición Personal, y de Hábeas Data. En consecuencia, en el Hábeas Corpus o exhibición Personal, toda persona agraviada o cualquiera otra en nombre de ésta tiene derecho a promoverla; y en el Hábeas Data únicamente puede promoverla la persona cuyos datos personales o familiares consten en los archivos, registros públicos o privados regulados en el Artículo 182, no 2) de la siguiente manera:

2) EL HÁBEAS DATA: "Toda persona tiene el derecho de acceso a la información sobre si misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros Públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o suprimirla. No podrá afectarse el secreto de las fuentes de información periodística. Las acciones de Hábeas Corpus o de Hábeas Data se deben ejercer sin necesidad de poder ni de formalidad alguna, verbalmente o por escrito, utilizando cualquier medio de comunicación, en horas o días hábiles e inhábiles y libres de costas.

Únicamente deben conocer de la garantía de Hábeas Data la Sala de lo Constitucional de la Corte Suprema de Justicia, quien tiene la obligación ineludible de proceder de inmediato para hacer cesar cualquier violación a los derechos del honor, intimidad personal o familiar y a la propia imagen. Los titulares de los órganos jurisdiccionales no pueden desechar la acción de Hábeas Corpus o Exhibición personal e igualmente tienen la obligación ineludible de proceder de inmediato para hacer cesar la violación de la libertad y la seguridad personal. En ambos casos, los titulares de los órganos jurisdiccionales que dejen de admitir estas acciones constitucionales incurren en responsabilidad penal y administrativa. Las autoridades que ordenaren y los agentes que ejecutaren el ocultamiento del detenido o que en cualquier forma quebranten esta garantía incurren en el delito de detención ilegal".[2]

[2] Congreso Nacional de Honduras. Ley de Protección de Datos Personales. Disponible en https://cei.iaip.gob.hn/doc/Ley%20de%20Proteccion%20de%20Datos%20Personales.pdf

2. Marco jurídico ordinario

En Honduras actualmente no existe una ley vigente que regule la protección de datos personales. No obstante, se han hecho esfuerzos en este sentido. En el año 2015, un proyecto de Ley de Protección de Datos Personales fue impulsado por el entonces vicepresidente del Congreso Nacional, el diputado Antonio Rivera Callejas. Este proyecto se basó en el anteproyecto que fue presentado por el Instituto Nacional de Acceso a la Información Pública en el año 2013 con el apoyo de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID).

Actualmente, el proyecto sigue en proceso de debate en el hemiciclo legislativo. El último debate se llevó a cabo en el mes de abril del año 2018. Sin embargo, este proceso se ha retrasado más de lo esperando, considerando que solo se han aprobado 19 de los 97 artículos que contiene el proyecto.

A falta de una legislación especial, los datos personales en Honduras cuentan con al menos una protección que se reconoce en la Ley del Instituto de Acceso a la Información Pública, Decreto Legislativo No. 170 – 2006. En los artículos 24 al 26 de esta ley se reconoce el Hábeas Data, la protección de los datos personales y presenta la figura del Comisionado Nacional de Derechos Humanos como una oficina facultada para incoar acciones para la protección de datos personales; además establece una prohibición en la cual ninguna persona puede solicitar a otros datos personales que puedan generar algún tipo de discriminación o poner en riesgo los derechos morales y patrimoniales de ese individuo.

En otro apartado, cabe mencionar que en el año 2011 el Congreso Nacional aprobó la Ley de Intervención de las Comunicaciones Privadas[3] (Decreto 243-2011), misma que faculta a los órganos jurisdiccionales a autorizar la intervención de las comunicaciones de personas que tengan causas criminales abiertas contra ellos. Sin embargo, como se mencionó anteriormente, esta ley ha sido objeto de mucha controversia debido a que se ha abusado de la misma, y en lugar de servir como un método de investigación criminal se ha vuelto un medio de presión social diseñado para amedrentar la ya precaria situación de activistas y defensores de derechos humanos en el país.

[3] Congreso Nacional de Honduras. Ley Especial sobre Intervención de las Comunicaciones Privadas. Disponible en http://www.poderjudicial.gob.hn/CEDIJ/Leyes/Documents/Ley%20Especial%20sobre%20Intervencion%20de%20las%20Comunicaciones%20Privadas%20(8,2mb).pdf

En la Ley del Instituto de Acceso a la Información Pública se regula lo relacionado a los datos personales de la siguiente manera:

Artículo 23. HÁBEAS DATA. “Se reconoce la garantía de Habeas Data”.

Artículo 24. SISTEMATIZACIÓN DE ARCHIVOS PERSONALES Y SU ACCESO. “Los datos personales serán protegidos siempre. El interesado, o en su caso el Comisionado de los Derechos Humanos por sí o en representación de la parte afectada, y el Ministerio Público, podrán incoar las acciones legales necesarias para su protección. El acceso a los datos personales únicamente procederá por decreto judicial o a petición de la persona cuyos datos personales se contienen en dicha información o de sus representantes o sucesores”.

Este precepto se vio violentado en 2014, luego de que se descubrió que el Registro Nacional de las Personas vendió su base de datos a bancos y empresas recolectoras de deudas para que estos pudiesen acosar y hostigar a los clientes que se encontraban en mora con sus obligaciones crediticias. Este evento fue el que propicio el debate en torno a la ley de protección de datos.

Artículo 25. PROHIBICIÓN DE ENTREGA DE INFORMACIÓN. “Ninguna persona podrá obligar a otra a proporcionar datos personales que puedan originar discriminación o causar daños o riesgos patrimoniales o morales de las personas”[4].

[4] Congreso Nacional de Honduras. Ley de Transparencia y Acceso a la Información Pública. Disponible en https://portalunico.iaip.gob.hn/assets/docs/leyes/ley-de-transparencia-y-reglamento.pdf

3. Definición de datos personales

El Artículo 3, numerales 8 y 9 del Proyecto de Ley de Protección de Datos Personales, define datos personales y datos sensibles de la siguiente manera:

- **Datos Personales:** “Cualquier información numérica, acústica, alfabética, biométrica, gráfica, fotográfica, de imagen, o de cualquier otro tipo concerniente a una persona natural identificada o identificable”.

- **Datos sensibles:** “Aquellos que se refieran a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada, tales como: Los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud, físicos o psíquicos y preferencias sexuales, así como cualquier otra información considerada como tal por ley; y, cualquier otro dato respecto de la libertad individual protegido por la Constitución de la República o en Convenios Internacionales suscritos por Honduras”.

4. Principios de tratamiento de datos personales

A. Principio de Lealtad y Legalidad: “Los datos personales no se recolectarán ni elaborarán con procedimientos desleales o ilícitos, ni se utilizarán con fines contrarios a los propósitos establecidos por esta Ley y demás normativa aplicable”.

B. Principio de Exactitud: “Los datos personales que se recolecten deberán ser exactos, adecuados, necesarios y no excesivos en relación con la finalidad para la cual se hubieran obtenido. El responsable del tratamiento tendrá la obligación de verificar la exactitud y pertinencia de los datos registrados y tomará las medidas necesarias en cuanto tenga conocimiento o constate el error, con respecto a los fines para los que fueron recolectados o para los que fueron tratados posteriormente, sean cancelados o rectificados”.

C. Principio de Finalidad de Propósito: “El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades determinadas, explícitas y legítimas del titular de los mismos. De igual forma, el responsable o el encargado del tratamiento deberá limitarse al cumplimiento de las finalidades previstas en la presente Ley. Si el responsable del tratamiento pretende tratar los datos para un fin distinto que no resulte compatible a los fines para los cuales fueron recolectados, requerirá obtener nuevamente el consentimiento del titular. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos”.

En el caso del principio de finalidad de propósito, es claro como este precepto es uno de los más importantes del ordenamiento y a la vez uno de los que más se violenta. Es importante enfatizar esto en las empresas que de una u otra manera manejan datos de los usuarios, sobre todo en aquellas corporaciones con intereses comerciales en múltiples rubros ya que el campo de afectación para los ciudadanos es mucho mayor.

D. Principio de Acceso a Información: “Los datos personales deberán ser almacenados de modo que permitan al titular de los mismos su acceso o conocimiento. En el tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento, en cualquier momento de acuerdo con lo previsto en esta Ley, información acerca de la existencia de datos que le conciernan”.

E. Principio de Consentimiento: “El tratamiento sólo puede ejercerse con el consentimiento, libre, previo, expreso e informado del titular. La acreditación de que dicho consentimiento ha sido prestado por el titular de los datos, corresponderá al responsable del tratamiento. Los datos personales no podrán ser obtenidos o comunicados sin previa autorización, o en ausencia de mandato legal, resolución administrativa o judicial, que sustituya el consentimiento. El consentimiento prestado podrá no ser considerado como tal, cuando exista un desequilibrio evidente entre la posición del interesado y el responsable del tratamiento”.

F. Principio de no Discriminación: “No deberán registrarse datos sensibles que puedan originar discriminación, en particular información que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, así como los relativos a la salud y a la vida sexual. Los datos biométricos no podrán ser utilizados como elementos de discriminación o arbitrariedad”.

G. Principio de Seguridad: “La información sujeta a tratamiento por el responsable o encargado del tratamiento, se deberá manejar con las medidas de seguridad, técnicas y organizativas que sean necesarias para otorgar seguridad a las bases de datos, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento”.

En el caso de Honduras este es uno de los menos se cumple, debido a que no solo las empresas si no que entes, como colegios profesionales u hospitales, rara vez invierten en recursos de seguridad digital que puedan proteger de manera efectiva los datos de los usuarios.

H. Principio de Responsabilidad: “El responsable o encargado del tratamiento deberá cumplir con los principios y obligaciones de la presente Ley, y dotarse de aquellos mecanismos necesarios para evidenciar dicho cumplimiento, tanto ante los interesados como ante el IAIP en el ejercicio de sus competencias y facultades”.

I. Principio de Proporcionalidad: “El responsable del tratamiento solo deberá recolectar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento”.

J. Principio de Confidencialidad: “Es el deber que tiene el responsable o el encargado del tratamiento de no mostrar, compartir, revelar o transmitir la base de datos a personas naturales o jurídicas que carezcan de la previa autorización por parte del titular”.

5. Derechos ARCO

En cuanto a los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO), el Proyecto de Ley de Protección de Datos Personales, los contempla en su segundo capítulo de la siguiente manera:

En primer lugar, se establece el derecho al acceso por parte del titular de la información que conste sobre el origen de la misma, la manera en la que estos son tratados, si han sido cedidos con anterioridad o si hay planes para ceder los mismos a terceros.

Artículo 12.- "Derecho de acceso. "El titular tiene derecho a solicitar y ser informado sobre sus datos personales que estén en posesión del responsable o encargado del tratamiento, el origen de dichos datos, el tratamiento del cual sean objeto, las cesiones realizadas o que se pretendan realizar, así como a tener acceso al aviso de privacidad al que está sujeto el tratamiento, en los términos previstos en la ley. El ejercicio de este derecho siempre será gratuito. El responsable del tratamiento debe responder al ejercicio del derecho de acceso, incluso en los casos en los que no haya tratado datos de carácter personal del interesado en su base de datos".

Se reconocen los derechos de rectificación, cancelación y oposición; se establecen los procedimientos administrativos para hacerlos efectivos, al igual que los casos en los cuales se puede denegar la petición (cuando no sea el titular de los datos o este legitimada para hacerlo, cuando exista un impedimento legal o cuando se lesionen los derechos de terceros). Sin embargo, estos criterios son vagos, y en el caso de la rectificación no es claro quién sería el ente encargado de verificar la exactitud dentro del Instituto de Acceso a la Información Pública, ni cuáles son los criterios mínimos para solicitar la misma.

Artículo 13.- "Derecho de rectificación. "El titular tendrá derecho a solicitar la rectificación de sus datos personales cuando sean inexactos, incompletos, inadecuados o excesivos, siempre que sea posible y no exija esfuerzos desproporcionados. El responsable del tratamiento tiene la obligación de poner en conocimiento a quienes haya cedido o comunicado los datos de la rectificación realizada para que también proceda a hacer la respectiva rectificación".

Artículo14.- "Derecho de cancelación: "La cancelación de datos personales procede a solicitud del titular cuando se presente alguno de los siguientes supuestos:
Se dé un tratamiento a los datos personales en contravención a lo dispuesto por la presente Ley;
Los datos personales hayan dejado de ser necesarios para el cumplimiento de la finalidad o finalidades de la base de datos previstas en el aviso de privacidad".

El "derecho al olvido" y las condiciones de ejercicio del borrado, bloqueo o supresión de datos correspondientes a cualquier titular o afectado que se consideren obsoletos por el transcurso del tiempo, o que de alguna manera afecten al libre desarrollo de alguno de sus derechos fundamentales, será desarrollado reglamentariamente.

Artículo 16.- "Derecho de oposición: El titular de los datos tendrá derecho a oponerse al tratamiento de sus datos personales en el supuesto en que los datos se hubiesen recolectado sin su consentimiento, cuando existan motivos fundados para ello y la Ley no disponga lo contrario. La procedencia del derecho de oposición dará lugar a la cancelación de los datos, previo bloqueo de los mismos".

Artículo 19.- "Ejercicio de los derechos de acceso, rectificación, cancelación y oposición. El titular, o en su caso su representante, podrá ejercer los derechos de acceso, rectificación, cancelación u oposición en los términos previstos en la presente Ley. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de cualquier otro derecho. La procedencia de estos derechos, en su caso, se hará efectiva una vez que el titular o su representante acrediten su identidad o representación, respectivamente. El responsable del tratamiento tiene, en todo caso, obligación de dar respuesta al derecho ejercitado".

Artículo 20.- "Designación de representante. Todo responsable o encargado del tratamiento deberá designar con carácter inmediato un representante que se responsabilice de dar una respuesta a la mayor brevedad posible a la solicitud del titular de los datos o su representante, a consecuencia del ejercicio de los derechos a que se refiere la presente Ley. Dicho nombramiento podrá ser verificado en su caso por el IAIP".

Artículo 21.- "Contenido de la solicitud. La solicitud de acceso, rectificación, cancelación u oposición se podrá presentar de manera escrita o por medio electrónico, conteniendo como mínimo, los siguientes requisitos:
a. Lugar y fecha en que se presenta la solicitud.
b. El responsable o encargado del tratamiento a quien se dirija;
c. El nombre del titular de los datos;
d. Los documentos que acrediten la identidad o, en su caso, la representación del titular;
e. La descripción clara y precisa de los datos personales respecto de los que se pretende ejercer alguno de los derechos antes mencionados;
f. El medio elegido para comunicarle la respuesta a su solicitud, ya sea por escrito, por medio electrónico o en la forma prescrita por el responsable o el

encargo del tratamiento; y

g. Cualquier otro elemento o documento que facilite la localización de los datos personales".

Artículo 22.- "Entrega de información sobre datos personales. La información debe ser proporcionada por el responsable o encargado del tratamiento dentro de los diez (10) días hábiles después de haber sido solicitada, entregándose en forma clara y sencilla. Cuando no fuere posible atender la solicitud de acceso, rectificación, cancelación u oposición a datos personales dentro de dicho plazo, se informará al titular o a su representante bajo cualquier título, expresando los motivos del retraso y señalando la fecha en que se atenderá la solicitud, la cual en ningún caso podrá superar los diez (10) días hábiles siguientes al vencimiento del primer plazo".

Artículo 23.- "Límite temporal al ejercicio del derecho de acceso. La solicitud de acceso a datos personales almacenados en una base de datos solamente se podrá realizar en intervalos de seis (6) meses calendario, salvo que el titular haga constar en su solicitud la existencia de un interés legítimo, y una causa debidamente justificada".

Artículo 24.- "Procedimiento de rectificación, cancelación u oposición. - El titular de los datos que considere que sus datos personales almacenados en una base de datos deben ser objeto de rectificación, cancelación u oposición, presentará una solicitud ante el responsable o encargado del tratamiento, la cual será tramitada bajo las siguientes reglas:

a. La solicitud ha de cumplir con las formalidades establecidas en el artículo 19 de la presente Ley. En el caso de solicitud de rectificación de datos personales, el titular de los mismos deberá indicar las modificaciones a realizar y aportar la documentación en que justifique su petición.

b. Si la solicitud resulta incompleta, el responsable o encargado del tratamiento requerirá al interesado dentro de los tres (3) días siguientes para que proceda a la subsanación de la misma. Transcurridos dos (2) meses calendario desde la fecha del requerimiento, sin que el interesado presente la información solicitada, se entenderá que ha desistido de dicha solicitud.

c. Una vez subsanada la solicitud, el responsable o encargado del tratamiento incluirá en la base de datos una leyenda que diga 'solicitud en trámite' y el motivo de la misma, en un plazo no superior a tres (3) días hábiles. Dicha leyenda deberá mantenerse hasta que la solicitud sea resuelta.

d. El plazo para atender la solicitud será de diez (10) días hábiles contados a partir del día siguiente de recibida la solicitud, o una vez que haya dado cumplimiento al requerimiento establecido en el apartado b) del presente artículo. Cuando no fuere posible atender la solicitud dentro de dicho término, se informará al interesado de los motivos del retraso, y la fecha en que se atenderá previsiblemente su solicitud, la cual en ningún caso podrá superar los diez (10) días hábiles siguientes al vencimiento del primer plazo.

e. El responsable o encargado del tratamiento comunicará al titular de los datos la determinación adoptada en un plazo máximo de diez (10)

días hábiles, contados a partir de la fecha en que se recibió la solicitud de rectificación, cancelación u oposición, a los efectos de que, si resulta procedente, se haga efectiva la misma en el plazo descrito en el inciso anterior. Cuando los datos personales hubiesen sido comunicados a terceros, con anterioridad a la fecha de rectificación o cancelación, el responsable o encargado del tratamiento deberá poner en conocimiento de dicho tercero en el plazo de los diez (10) días siguientes, el ejercicio de derechos por parte del titular de los datos, para que proceda también a dar cumplimiento a dicho derecho en igual término".

Artículo 25.- "Denegación justificada al acceso, rectificación, cancelación u oposición. El responsable o encargado del tratamiento podrá denegar el acceso a los datos personales, o a realizar la rectificación, cancelación, o conceder la oposición al tratamiento de los mismos, en los siguientes supuestos:

a. Cuando el solicitante no sea el titular de los datos personales o el representante no esté debidamente acreditado para ello;

b. Cuando en su base de datos, no se encuentren los datos personales del solicitante;

c. Cuando se lesionen los derechos de un tercero;

d. Cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos; y e. Cuando el ejercicio de los derechos de rectificación, cancelación u oposición haya sido ya satisfecho. En todos los casos anteriores, el responsable o encargado del tratamiento deberá informar el motivo de su decisión y comunicarla al titular de los datos, o en su caso, a su representante, en un plazo máximo de diez (10) días hábiles siguientes a la recepción de la solicitud, por el medio designado por el titular, acompañando, en su caso, los documentos o pruebas que resulten pertinentes. La negativa a que se refiere este artículo podrá ser parcial, en cuyo caso el responsable o encargado del tratamiento dará respuesta al ejercicio de los derechos de acceso, rectificación, cancelación u oposición efectuados por el titular".

Articulo 26.- "Excepciones a los derechos de acceso, rectificación, cancelación u oposición. El responsable o encargado del tratamiento que contenga los datos podrá denegar el acceso, la rectificación o cancelación en función de los riesgos que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando. Los responsables de la base de datos de la Secretaría de Estado en el Despacho de Finanzas podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas enfocadas a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del IAIP, el que deberá asegurarse de la procedencia o improcedencia de la denegación". [2]

6. Consentimiento

El Consentimiento es contemplado en el Título VIII del Proyecto de Ley en la sección de Cesión de Datos, se establece que los datos solo pueden ser utilizado para las funciones establecidas y consentidas por la persona que cede sus datos. El proyecto considera nulo todo consentimiento otorgado cuando la finalidad para el tratamiento de los datos no este establecida por el ente que los recolecte.

Además, se establecen excepciones a esto cuando se trate de casos en los cuales conocer los datos sea necesario para la creación efectiva de relaciones jurídicas entre partes y por parte de los organismos de la Administración Pública, operadores de justicia y el Sistema de Salud Pública, cuando sea necesario para el apropiado funcionamiento de las mismas.

Si bien la mayoría de estas excepciones son racionales, se puede considerar que el hecho que no se establezca que en el caso de los operadores de justicia no es necesaria la autorización por parte de ningún ente judicial. Esto podría dejar esto abierto a arbitrariedades la aplicación de esta disposición por parte de los entes de investigación del Estado.

Artículo 44.- "Cesión de datos a terceros. Los datos personales objeto del tratamiento sólo podrán ser cedidos a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, con el previo consentimiento expreso del titular de los datos".

Artículo 45.- "Nulidad del consentimiento del titular de los datos. Será nulo el consentimiento para la cesión de datos personales a un tercero cuando el aviso de privacidad que se le facilita al titular de los datos, por parte del responsable del tratamiento, no le permita conocer la finalidad o finalidades que tendrán sus datos personales al ser cedidos a un tercero".

Artículo 46.- "Excepciones a la exigencia del consentimiento para ceder datos personales. El consentimiento exigido no será necesario cuando:
a. La cesión se encuentre autorizada por una Ley;
b. El tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo nacimiento, desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con la base de datos de terceros;
c. La cesión que deba efectuarse tenga por destinatario a los operadores de justicia, en el cumplimiento de sus atribuciones según Ley;
d. La cesión se produzca entre organismos de la Administración Pública en el ejercicio de sus funciones y atribuciones legales; y
e. La cesión de datos personales relativos a la salud sea necesaria para atender una emergencia, que requiera acceder a una base de datos, o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre salud pública". 2

En todo lo demás, el cedente de los datos personales tendrá que observar lo prescrito en la presente Ley.

7. Sujetos obligados

Los sujetos obligados por este proyecto ley son aquellos responsables por el tratamiento de datos. Se entiende que estos pueden ser entes públicos o privados ya que hay mención a empresas. Sin embargo, es algo sorprendente el hecho de que no incluya algún listado con las instituciones públicas vigentes que de manera conocida manejen datos personales, como el Registro Nacional de las Personas, el Instituto de la Propiedad o el Registro Mercantil.

Artículo 27.- "Responsabilidad del responsable del tratamiento. El responsable del tratamiento debe garantizar, en todo caso, la protección de los datos del titular de los mismos en cada tratamiento que realice. Consecuentemente con ello, se establece la responsabilidad general del responsable por cualquier tratamiento de datos personales realizado por él mismo o en su nombre. En particular, el responsable del tratamiento debe garantizar y está obligado a demostrar que cada operación de tratamiento cumple lo dispuesto en la presente Ley. Asimismo, el responsable del tratamiento debe garantizar que los datos personales no sean accesibles a un número indeterminado de personas". [2]

8. Obligaciones y responsabilidades de los sujetos obligados

En el Articulo 30 del proyecto de ley se establecen los deberes de los responsables por el tratamiento de datos. Estos se pueden resumir en el aseguramiento de los datos, respetar la finalidad para la cual los datos fueron recolectados, adoptar medidas de seguridad técnicas apropiadas para el aseguramiento de los datos, dar cumplimiento a los derechos ARCO, así como apegarse a las directrices y disposiciones del Instituto de Acceso de Información Pública.

Artículo 30.- "Deberes del responsable del tratamiento. El responsable del tratamiento deberá cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente Ley y en su Reglamento:

a. Garantizar al titular de los datos, el pleno y efectivo ejercicio del derecho fundamental a la protección de sus datos personales;
b. Informar debidamente al titular de los datos acerca de la finalidad de la recolección y los derechos que le asisten, sobre la base del consentimiento otorgado;
c. Cumplir con las obligaciones contenidas en el aviso de privacidad.
d. Tramitar y dar respuesta a las solicitudes de acceso, rectificación, cancelación y oposición en los términos previstos en la presente Ley;
e. Adoptar las medidas de seguridad técnicas y organizativas necesarias para conservar la información e impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
f. Dar instrucciones claras y precisas al encargado del tratamiento para que éste pueda llevar a cabo el tratamiento adecuado;
g. Adoptar las medidas necesarias para que la información suministrada se mantenga actualizada;
h. Exigir al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular;
i. Implementar un manual de políticas y procedimientos de seguridad para garantizar el adecuado cumplimiento de la presente Ley;
j. Registrar en la base de datos la leyenda "Solicitud en Trámite" en la forma en que se regula en la presente Ley;
k. Abstenerse de comunicar o ceder información que se encuentre bloqueada por el IAIP;
l. Informar al IAIP, cuando se presenten eventos que deriven en violaciones a las políticas y procedimientos de seguridad y existan riesgos en la administración de la información de los titulares de los datos;
m. Cumplir las instrucciones y requerimientos que imparta el IAIP; y
Cumplimentar los derechos de acceso, rectificación, cancelación y oposición (ARCO) ejercitados ante el encargado del tratamiento, cuando contractualmente el responsable haya asumido dicha obligación". [2]

9. Disposiciones sobre la transferencia y cesión de datos

La sección sobre Cesión de Datos en el proyecto de ley hace solamente alusión al consentimiento, y define que el hecho de que se nombre a una persona designada para el tratamiento de datos no constituye una transferencia de datos; pero no hay mención una definición clara de Transferencia de Datos en el estado actual del Proyecto de Ley.

10. Autoridad competente

En su artículo 62 el proyecto de Ley establece que la autoridad competente para conocer sobre estos procesos es el Instituto de Acceso a la Información Pública. Sin embargo, se debe considerar el hecho de que este ente gubernamental no está facultado para ejecutar sus propias sanciones, y las mismas prescriben en un plazo máximo de 3 años (artículo 92) en las sanciones más graves contempladas en esta ley, lo cual dificulta la aplicación efectiva de la misma.

Artículo 62.- "Autoridad de Protección de Datos. Para los objetivos y propósitos de la presente Ley, el Instituto de Acceso a la Información Pública y de Protección de Datos Personales (IAIP) es el responsable de promover y garantizar el derecho fundamental de protección de datos personales, y ejercer la vigilancia para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente Ley y su Reglamento. Le corresponde al IAIP asumir todas las competencias que se le atribuyen por esta Ley, así como adoptar las resoluciones, elaborar los reglamentos y las demás disposiciones pertinentes para asegurar la correcta aplicación de la presente Ley y su Reglamento. Para tal fin, el IAIP, creará la Gerencia de Protección de Datos Personales (PRODATOS) y determinará en todo momento su estatuto orgánico y funcionamiento. Los servidores públicos al servicio del IAIP y de la Gerencia de Protección de Datos Personales (PRODATOS) estarán, asimismo, sometidos a un estatuto profesional especial, donde se determinará su régimen de incompatibilidades". [2]

Dichos servidores públicos no podrán dedicarse a la actividad desarrollada por el IAIP y por la Gerencia de Protección de Datos Personales (PRODATOS), hasta transcurridos tres años desde su cese de actividad efectivo en dichas Instituciones.

Artículo 92.- "Prescripción de la Infracción. Las infracciones muy graves prescribirán a los tres (3) años, las graves a los dos (2) años y las leves en un (1) año. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido". [2]

11. Procedimientos y Sanciones

El ente encargado de la aplicación de las sanciones en este proyecto de ley es el Instituto de Acceso a la Información Pública. El mismo impone sanciones administrativas pecuniarias entre 10 y 60 salarios mínimos, sin perjuicio de que se puedan incoar acciones civiles o penales contra los infractores. Sin embargo, ley no deja claro si esta acción procederá a instancia de parte o de oficio por la autoridad competente.

Artículo 92.- "Prescripción de la Infracción. Las infracciones muy graves prescribirán a los tres (3) años, las graves a los dos (2) años y las leves en un (1) año. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis (6) meses por causas no imputables al presunto infractor".

Artículo 93.- "Prescripción de la Ejecución de las Sanciones Impuestas. La ejecución de las sanciones impuestas por faltas muy graves prescribirá a los tres (3) años, las impuestas por faltas graves a los dos (2) años y las impuestas por faltas leves en un (1) año. El plazo de prescripción de la ejecución de las sanciones impuestas comenzará a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor".

Artículo 94.- "Otras responsabilidades. Las sanciones que se señalan en este Capítulo se impondrán sin perjuicio de la responsabilidad civil o penal que resulte de la comisión de las infracciones previstas en esta Ley".

12. La computación en la nube y los servicios financieros

El área de los servicios financieros es de especial interés para esta ley, en vista que mucho de su apoyo viene de personas que creen que el sector bancario y financiero ha cometido abusos en contra de los usuarios, particularmente en el campo crediticio. Actualmente, cuando una persona cae en mora entra a la "Central de Riesgo" por un plazo de 2-3 años, los legisladores buscaban activamente cambiar esto ya que consideran indispensable el derecho de rectificación en este sentido ya que sin esto se puede mermar de manera tajante el poder de adquisición de una gran parte de la población.

Dentro del capítulo VII, en la Categoría Especial de Datos del Proyecto de Ley, se establece en el Artículo 40 lo siguiente:

Artículo 40.- "Datos relativos a la prestación de servicios de información de la actividad financiera, crediticia y comercial.

1. Los prestadores de servicios de información financiera, crediticia y comercial, en el tratamiento de datos de carácter personal, estarán sometidos a lo establecido en esta Ley en lo referente a su actividad exclusivamente.
2. Quienes se dediquen a la prestación de servicios de información financiera, crediticia y comercial sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto, o procedentes de información facilitada por el interesado o con su consentimiento.
3. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones pecuniarias, facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos, con carácter previo a la inscripción en cualquier Base de Datos de solvencia patrimonial y crédito, se procederá a notificar al presunto deudor o deudores de la posibilidad de llevar a cabo la inscripción de sus datos de carácter personal a consecuencia de su deuda, para que en el plazo de treinta días (30) calendario antes de proceder a dicho registro, el deudor pueda cumplir con sus obligaciones. Transcurrido dicho plazo, sin que las mismas se hayan satisfecho, se podrá proceder sin más trámites a la indicada inscripción. Corresponde la acreditación de la notificación al responsable del tratamiento.

4. Deberá procederse a la cancelación de manera inmediata de los datos de carácter personal del deudor o deudores inscritos a consecuencia de la falta de cumplimiento de sus obligaciones, una vez que las mismas hayan sido cumplidas. En ningún caso la inscripción podrá permanecer más del plazo de cinco (5), años, a contar desde que se produjo la mencionada inscripción.
5. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis (6) meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.
6. Se podrán registrar y ceder los datos de carácter personal que sean necesarios para determinarla solvencia económica de los interesados y que no se refieran, cuando le sean adversos, a más de tres (3) años, siempre que respondan con veracidad a la situación actual de aquéllos.
7. Con relación a la prestación de servicios financieros, crediticios y comerciales, se aplicarán los derechos de acceso, rectificación, cancelación y oposición en los términos previstos en esta Ley.
8. Para la prestación de cualquier otro servicio de información financiera, crediticia y comercial se tendrán que aplicar las disposiciones contenidas en la presente Ley".

13. Agenda Digital

La Agenda Digital de Honduras 2014-2018 fue promovida por la Secretaria Técnica de Planificación y Cooperación Externa (SEPLAN), con la idea de promover la competitividad e innovación a través del uso masivo y efectivo de las TICS. Se basa en la Visión de País establecida por el gobierno de entonces, donde buscaban darle mayor modernidad, transparencia y eficiencia al Estado, así como manifestar la importancia de tener un ordenamiento jurídico eficiente en la sección 4, la cual se basa en el desarrollo del marco institucional y regulatorio.

Objetivo

"Crear un marco institucional y regulatorio adecuado y eficiente que permita una efectiva promoción y desarrollo de las TIC en los diferentes ámbitos del Estado de Honduras, considerando estándares internacionales y elementos básicos que garanticen protección, seguridad y equidad en el aprovechamiento de los beneficios de la innovación tecnológica"[5].

Dentro de este objetivo se identificaron las siguientes líneas de acción:

A. "Fortalecer la institucionalidad del sector para garantizar la implementación y sostenibilidad de políticas, programas y proyectos orientados al desarrollo de las TIC en Honduras.

B. Promover legislación sobre documentos y firma electrónica, consensuada con los diferentes actores del sector, que tenga como objetivo dar equivalencia legal a los documentos electrónicos y fomentar la utilización de la firma electrónica e identificación digital.

C. Desarrollar un plan de seguridad integral de la información para el sector público.

D. Desarrollar proyectos de transferencia tecnológica de aplicación común que permitan optimizar el uso de los recursos y mejorar las prácticas en la administración pública.

E. Consolidar lazos de cooperación internacional que faciliten el desarrollo de proyectos tecnológicos que mejoren los servicios ofrecidos por las instituciones públicas". [5]

[5] Secretaría Técnica de Planificación y Cooperación Externa (SEPLAN). Agenda Digital de Honduras 2014 – 2018. Disponible en: http://agendadigital.hn/

Referencias

Asamblea Nacional Constituyente. **Constitución Política de 1982.** Disponible en: http://www.poderjudicial.gob.hn/CEDIJ/Leyes/Documents/ConstitucionRepublicaHonduras.pdf

Secretaría Técnica de Planificación y Cooperación Externa (SEPLAN). **Agenda Digital de Honduras 2014 – 2018.** Disponible en: http://agendadigital.hn/

Congreso Nacional de Honduras. **Ley de Protección de Datos Personales.** Disponible en: https://cei.iaip.gob.hn/doc/Ley%20de%20Proteccion%20de%20Datos%20Personales.pdf

Congreso Nacional de Honduras. **Ley de Transparencia y Acceso a la Información Pública.** Disponible en: https://portalunico.iaip.gob.hn/assets/docs/leyes/ley-de-transparencia-y-reglamento.pdf

Congreso Nacional de Honduras. **Ley Especial sobre Intervención de las Comunicaciones Privadas.** Disponible en: http://www.poderjudicial.gob.hn/CEDIJ/Leyes/Documents/Ley%20Especial%20sobre%20Intervencion%20de%20las%20Comunicaciones%20Privadas%20(8,2mb).pdf

Pasos de Animal Grande. **Junta Nominadora confirma espionaje telefónico en Honduras: Asesor presidencial revela nombres de próximos magistrados.** (2016). Disponible en: http://www.pasosdeanimalgrande.com/index.php/en/contexto/item/1167-junta-nominadora-confirma-espionaje-telefonico-en-honduras-asesor-presidencial-revela-nombres-de-proximos-magistrados/1167-junta-nominadora-confirma-espionaje-telefonico-en-honduras-asesor-presidencial-revela-nombres-de-proximos-magistrados

Ley sobre Justicia Constitucional. (2004). Corte Suprema de Justicia. Disponible en: http://www.oas.org/juridico/pdfs/mesicic4_hnd_justicia.pdf

Mercado, J. (2016). **Junta Nominadora denuncia intervención telefónica y vigilancia con cámaras ocultas.** Tegucigalpa, Honduras: El Heraldo. Disponible en: https://www.elheraldo.hn/pais/917190-466/junta-nominadora-denuncia-intervenci%C3%B3n-telef%C3%B3nica-y-vigilancia-con-c%C3%A1maras-ocultas

Piden que se controle "ley de escuchas". (2015). Tegucigalpa, Honduras: La Prensa. Disponible en: https://www.laprensa.hn/honduras/899871-410/piden-que-se-controle-ley-de-escuchas