
DATA
UNINION
DATA
PROTECTION
REGULATION
DATA
PROTECTION
HONDURAS
EU/2018/725
2018/725
DATA
PROTECTION

FORTALEZAS DEL REGLAMENTO (UE) 2018/1725 DEL PARLAMENTO EUROPEO DE LA UNION EUROPEA APLICABLES AL MARCO LEGAL DE HONDURAS

Melba Aurora Rivera Reyes[1]
DOI: https://doi.org/10.5377/lrd.v45i1.19394

RESUMEN:

La legislación de la Unión Europea, en particular el Reglamento (UE) 2018/1725, presenta una serie de fortalezas que pueden ser altamente beneficiosas para el marco legal de Honduras. Por ello, se procedió a realizar una revisión literaria comparando el Reglamento (UE) 2018/1725, con la legislación hondureña teniendo como objetivo. Se destacan muchas fortalezas como la adopción de los principios de protección integral de datos, derechos claros para los ciudadanos, transparencia, responsabilidad, supervisión y adaptación tecnológica, contribuiría a crear un entorno más seguro y confiable para el manejo de datos personales en Honduras. La metodología aplicada es la Selección de Fuentes Relevantes, luego la elaboración de una análisis comparativo y evaluación de la aplicabilidad y formulación de conclusiones y recomendaciones. Conclusión: Esta adaptación de las fortalezas del Reglamento (UE) 2018/1725 a la legislación hondureña y no solo protegería mejor a los ciudadanos, sino que también fortalecería la confianza en las instituciones y empresas que manejan información personal, fomentando así un entorno más favorable para el crecimiento y desarrollo tecnológico.

PALABRAS CLAVES:

Protección de Datos personales y Privacidad. Principios. Seguridad de datos Personales. Supervisión. Cumplimiento.

Fecha de recepción: 31/8/2024
Fecha de aprobación: 06/11/2024

1 Abogada, Máster en Administración de Empresas, Docente de la Universidad Nacional Autónoma de Honduras. Correo Electrónico: melba_reyes@unah.edu.hn

STRENGTHS OF REGULATION (EU) 2018/1725 OF THE EUROPEAN PARLIAMENT OF THE EUROPEAN UNION APPLICABLE TO THE LEGAL FRAMEWORK OF HONDURAS

Melba Aurora Rivera Reyes[2]
DOI: https://doi.org/10.5377/lrd.v45i1.19394

ABSTRACT:

European Union legislation, in particular Regulation (EU) 2018/1725, presents several strengths that can be highly beneficial for Honduras' legal framework. Therefore, a literature review was carried out comparing Regulation (EU) 2018/1725, with Honduran legislation with the objective. Many strengths are highlighted such as the adoption of the principles of comprehensive data protection, clear rights for citizens, transparency, accountability, supervision and technological adaptation, would contribute to creating a safer and more reliable environment for the handling of personal data in Honduras. The methodology applied is the Selection of Relevant Sources, then the elaboration of a comparative analysis and evaluation of applicability and formulation of conclusions and recommendations. Conclusion: This adaptation of the strengths of Regulation (EU) 2018/1725 to Honduran legislation would not only better protect citizens but would also strengthen trust in institutions and companies that handle personal information, thus fostering a more favorable environment for technological growth and development.

KEY WORDS:

Protection of Personal Data and Privacy. Principles. Security of Personal Data. Supervision. Compliance

Reception date: 8/31/2024
Approval date: 06/11/2024

2 Lawyer, Master's in Business Administration, Lecturer at the National Autonomous University of Honduras.
Email: melba_reyes@unah.edu.hn

I. INTRODUCCIÓN

La privacidad y la protección de datos personales se convirtieron en un factor central en el entono mundial provocando una revisión profunda en cuanto a su normativa en todos los países. La experiencia europea ha sido liderada por el Parlamento Europeo quien crea el Reglamento (UE) 2018/1725 (REGLAMENTO (UE) 2018/1725 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 DE OCTUBRE DE 2018 DE LA UNION EUROPEA , 2018). En el mismo, se determina un marco jurídico **avanzado** para la protección de datos que se encuentran archivados y en custodia de diferentes instituciones y organismos de la Unión Europea. El reglamento garantiza un amplio nivel de protección para los datos personales, y determina una serie de principios acompañado de las obligaciones para su tratamiento, convirtiéndose en una de las **mejores prácticas internacionales.**

Honduras se encuentra en proceso de creación de un marco solido para enfrentar grandes desafíos en la privacidad y protección de datos personales. Aún mantiene en proyecto de ley un marco legal para la protección de los datos personales y se encuentra en un punto decisivo para tomar la decisión de adoptar principios solidos en un marco legal integral. La necesidad de fortalecer las normativas existentes e impulsar un **Plan Nacional de Digitalización**, destaca la importancia del momento y lo oportuno que es explorar modelos regulatorios efectivos que puedan adaptarse al mercado hondureño. Ya lo hace mención el autor José Antonio Rivera en su artículo *El Derecho a la protección de la Vida Privada y el derecho a la libertar de información la doctrina y en la Jurisprudencia, Una perspectiva en Bolivia que* es una responsabilidad de orden público proteger a los ciudadanos: *"constituyendo una obligación positiva para el Estado, consistente en la adopción de medidas legislativas, administrativas y jurisdiccionales para establecer vías y mecanismos de protección de la vida íntima o privada de la persona"* (Rivera, 2008)

El presente estudio pretende contribuir resaltando mejoras significativas que pueden ser aplicadas a los esfuerzos del país en la construcción de un marco jurídico moderno y eficiente para la protección de datos personales. Mediante el análisis de las mejores prácticas que ya se encuentran en el Reglamento (UE) 2018/1725 se destacan las normas que garantizan la protección adecuada de los datos personales, alineación con Estándares Internacionales y el fortalecimiento del marco legal para una mayor residencia ante las amenazas que vienen con el progreso informático.

II. METODOLOGIA

La siguiente metodología permitirá una evaluación sistemática y comprensiva que permitirá identificar las fortalezas del Reglamento (UE) 2018/1725 y proporcionar lineamientos que podrían contribuir al fortalecimiento del marco legal hondureño en materia de protección de datos y privacidad. Para este análisis, se aplicar la metodología de revisión bibliográfica que consta de los siguientes pasos:

a. ***Selección de Fuentes Relevantes:*** se identificarán los documentos legales, artículos académicos, informes de organizaciones internacionales y otros recursos pertinentes que analicen el Reglamento (UE) 2018/1725. Se recopilan las fuentes sobre el estado actual de la legislación en Honduras sobre protección de datos y privacidad.

b. Análisis Comparativo: Identificados, seleccionados los documentos necesarios se procede a la Comparación de las disposiciones del Reglamento (UE) 2018/1725 con el marco legal hondureño actual. En esta parte, se identifican de las fortalezas y mejores prácticas del Reglamento (UE) 2018/1725 que no se encuentren en la legislación hondureña.

c. Evaluación de Aplicabilidad: Análisis de la aplicabilidad y relevancia de las disposiciones del Reglamento (UE) 2018/1725 en el contexto legal y socioeconómico de Honduras. Identificación de oportunidades para la implementación de estas disposiciones en el marco legal hondureño.

d. Formulación de Conclusiones y Recomendaciones: se desarrollarán las recomendaciones para la aplicación e implementación de las fortalezas y mejores prácticas del Reglamento (UE) 2018/1725 en la legislación de Honduras.

Todo lo anterior, para desarrollar conocimientos a fin de integrar las diversas investigaciones, libros y artículos científicos. La búsqueda ffue a través de los navegadores de consulta y fuentes acordes al objetivo de la investigación. Se utilizaron los descriptores:" Reglamento UE 2018/1725", "Marco Legal Hondureño" las cuales se combinaron en la exploración para la búsqueda y selección de la información, y luego se elaboró el presente documento.

III. ANALISIS DEL REGLAMENTO (UE) 2018/1725 DEL PARLAMENTO EUROPEO

Se detallarán los aspectos más relevantes del Reglamento para luego compararlo con nuestra legislación. Los Estados Europeos advierten la necesidad de esta legislación, tal y como lo explica Mónica Arenas Ramiro en su artículo *La Protección de Datos en los Países Europeos,* enunciando lo siguiente "El reconocimiento del derecho a la protección de datos personales es relativamente reciente en todos los Estados europeos, pues ha tenido lugar como consecuencia del desarrollo tecnológico y su impacto en los derechos fundamentales, cuando se advierten las ventajas y desventajas que el uso de las nuevas tecnologías, en especial la informática, representan para la vida privada de las personas" (Ramiro, 2008)

A. PRINCIPIOS FUNDAMENTALES DEL REGLAMENTO

A continuación, se detallan los principios básicos del Reglamento (UE) 2018/1725:

a. Licitud, Lealtad y Transparencia: Los datos personales deben ser tratados de manera lícita, fiel y transparente con respecto a los interesados.

b. Limitación de la Finalidad: Los datos personales deben ser recolectados con un fin determinado, claro y legítimo, y no deben ser tratados nuevamente de manera diferente con dichos fines.

c. Minimización de Datos: Los datos personales deben ser limitados a lo necesario en relación con el fin para lo que fue solicitado.

d. ***Exactitud:*** Los datos deben ser exactos y actualizados. Se debe garantizar que los datos inexactos se supriman o rectifiquen.

e. ***Limitación del Plazo de Conservación:*** Los datos personales deben ser conservados durante el tiempo necesario para el fin determinado y durante el tratamiento de dichos datos personales. Este principio requiere que una vez finalizado el tratamiento los datos sean eliminados o anonimizados cuando ya no sean necesarios.

f. ***Integridad y Confidencialidad:*** Los datos personales deben ser tratados asegurando su integridad y protegidos de un tratamiento no licito o no autorizado.

g. ***Responsabilidad Proactiva (Accountability):*** El responsable del tratamiento debe cumplir con todos los principios. Implica adoptar políticas para garantizar que se cumple con las normativas de protección de datos y privacidad y evidenciar las medidas aplicadas.

2. DERECHOS DE LOS INTERESADOS

Los principales derechos de los interesados según el reglamento son:

a. ***Derecho de Información:*** los interesados tienen derecho a ser informados sobre la recolección de sus datos personales y la utilización que se les dará a los mismos. Esto incluye tres aspectos: identificación de los destinatarios de los datos, precisión sobre la finalidad y el plazo de conservación.

b. ***Derecho de Acceso:*** los interesados tienen derecho a la entrega de la confirmación si se están tratando datos personales relacionados e indispensables para el fin determinado y, en su caso, acceder a dichos datos. También tienen derecho a recibir una copia de los datos personales que están siendo procesados.

c. ***Derecho de Rectificación:*** Los datos personales podrán ser corregidos, rectificados o actualizados por los interesados. También cuando existan datos incompletos tendrán los interesados el derecho de ser completados.

d. ***Derecho de Supresión (Derecho al Olvido):*** los interesados tienen derecho a solicitar que sean eliminados sus datos personales en ciertas circunstancias, cuando los datos no son necesarios para los fines determinados para los que fueron recogidos, o si el tratamiento es con fines ilícitos.

e. ***Derecho a la Limitación del Tratamiento:*** los interesados podrán solicitar que se limite el tratamiento de sus datos personales en determinadas condiciones, si se llegara a impugnan la exactitud o si el tratamiento es para causas ilícitas. El derecho del interesado es según su preferencia, ya sea limitar o supresión.

f. ***Derecho a la Portabilidad de los Datos:*** los interesados tienen derecho a recibir los datos personales que hayan proporcionado al responsable

del tratamiento, en un formato estructurad y a retransmitir esos datos a otro responsable del tratamiento, sin ningún impedimento.

g. ***Derecho de Oposición:*** los interesados tienen el derecho a oponerse al tratamiento de sus datos personales en cualquier momento. Esto incluye el derecho a oponerse al tratamiento de sus datos cuando sea para fines de marketing directo.

h. ***Derecho a No Ser Objeto de Decisiones Automatizadas:*** los interesados tienen derecho a no ser objeto de una decisión en el tratamiento automatizado, cuando solo en eso de base el tratamiento. Está incluido en este principio la elaboración de perfiles, que produzca efectos jurídicos o les afecte significativamente.

i. ***Derecho a Retirar el Consentimiento:*** El interesado tienen derecho a retirar su consentimiento cuando l tratamiento de los datos personales se basa en el consentimiento del interesado. Este retiro puede darse en cualquier momento sin que ello afecte a la licitud del tratamiento.

j. ***Derecho a Presentar una Reclamación*** los interesados tienen derecho a presentar una reclamación ante una autoridad de control cuando consideran que el tratamiento de sus datos personales infringe el reglamento.

Estos derechos son pilares fundamentales para la protección de la privacidad y la autonomía de los individuos respecto a sus datos personales. Las instituciones y organismos de la Unión Europea están obligados a agilizar el ejercicio de estos derechos y garantizar que los interesados puedan ejercerlos de manera eficiente.

C. OBLIGACIONES DE LOS RES PONSABLES Y ENCARGADOS DEL TRATAMIENTO

El Reglamento (UE) 2018/1725 determina las obligaciones para los responsables y encargados del tratamiento de datos personales.

Obligaciones de los responsables del Tratamiento

1) ***Licitud del Tratamiento:*** los tratamientos de datos personales de los interesados deben realizarse sobre un marco jurídico acorde que comprende las normas sobre el consentimiento del interesado, obligación licita, protección de intereses vitales, y la ejecución de un contrato.

2) ***Transparencia y Comunicación:*** están obligados a brindar a los interesados información transparente y precisa sobre la recolección y uso de sus datos personales. Deberá incluir la identificación del responsable del tratamiento, los fines del tratamiento y los derechos de los interesados.

3) ***Seguridad del Tratamiento:*** son medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado al riesgo, incluyendo la protección contra el tratamiento no autorizado o ilícito y contra la pérdida, destrucción o daño accidental.

4) ***Evaluaciones de Impacto Relativas a la Protección de Datos:*** deben realizar evaluaciones de impacto sobre la protección de datos según un tipo de tratamiento, en particular si utiliza nuevas tecnologías, comprenda un alto riesgo para los derechos fundamentales y libertades de las personas físicas.

5) ***Designación de un delegado de Protección de Datos (DPD):*** Las operaciones con datos personales requieren de un tratamiento por un responsable, seguimiento de varias actividades como almacenamiento, resguardo y reportes periódicos acerca de las medidas de seguridad implementadas. Para ello, se hará el nombramiento de un delegado que tendrá como funciones vigilar y monitorear el cumplimiento del reglamento.

6) ***Registro de Actividades de Tratamiento:*** deben mantener un registro de las actividades de tratamiento bajo su responsabilidad, este debe incluir información como los fines del tratamiento, descripción de las categorías de interesados y de las categorías de datos personales tratados, y todas las medidas de seguridad implementadas.

7) ***Notificación de Violaciones de Datos Personales:*** se debe notificar a la autoridad de control que atenderá cualquier violación de la seguridad de los datos personales si es posible, en un periodo menor de 72 horas después de haber tenido reportada. También deben comunicar a los interesados la violación de datos personales.

Obligaciones de los Encargados del Tratamiento

1. ***Actuar Solo bajo las Instrucciones del responsable del Tratamiento:*** Tratar los datos personales siguiendo únicamente las instrucciones del responsable del tratamiento.

2. ***Confidencialidad:*** garantizar que las personas autorizadas para tratar los datos personales estén comprometido a respetar la confidencialidad.

3. ***Seguridad del Tratamiento:*** garantizar la seguridad del tratamiento implementando medidas técnicas y organizativas adecuadas.

4. ***Subcontratación:*** No podrá recurrir o delegar a otro encargado del tratamiento sin la autorización por escrito del responsable del tratamiento. Podrá subcontraten servicios, pero debe asegurarse que el sub encargado del tratamiento cumpla con las mismas obligaciones de protección de datos.

5. ***Supresión o Devolución de Datos:*** cuando finalice de la prestación de servicios relacionados con el tratamiento, se deben devolver o suprimir todos los datos personales al responsable del tratamiento y no deben dejar copias, salvo se le exija la conservación de los datos.

6. ***Cooperación con las Autoridades de Control:*** estar a disposición de la autoridad de control y proporcionarle toda la información necesaria, participar en auditorias e inspecciones para demostrar el cumplimiento de las obligaciones establecidas en el reglamento.

Estas obligaciones son necesarias para garantizar que los datos personales se traten de manera responsable, asegurando la protección de los derechos de los interesados y siguiendo el cumplimiento con las normativas europeas sobre protección de datos y privacidad.

D. DERECHOS DEL USUARIO Y MECANISMOS DE RECLAMACIÓN

Los principales mecanismos de reclamación disponibles según el reglamento son:

Proceso de Reclamación: los interesados tienen derecho a presentar una reclamación ante la autoridad de control competente, en la Unión Europea es el Supervisor Europeo de Protección de Datos (SEPD). El SEPD es la entidad responsable de supervisar que se aplique el reglamento y asegurar que se respeten los derechos de los interesados. La autoridad de control investigará la reclamación la solicitud del interesado y al responsable del tratamiento. Finalizada la investigación, la autoridad de control decidirá y podrá emitir órdenes de carácter vinculante para corregir cualquier incumplimiento del reglamento. Si el interesado no está satisfecho con la resolución, puede ejercer el recurso de apelación ante los tribunales competentes para una revisión judicial de la decisión de la autoridad de control.

Derecho a Retirar el Consentimiento: Cuando el tratamiento de datos personales tenga como base el consentimiento del interesado, este tiene derecho a retirar su consentimiento en cualquier momento. Esta acción de retiro del consentimiento no afectará a la licitud del tratamiento fundamentado en el consentimiento previo a su retiro. El interesado podrá detener el tratamiento de sus datos si ya no desean que sus datos sean parte del tratamiento.

Medidas Provisionales y Correctivas: Cuando la autoridad de control reciba una reclamación de un interesado, puede ordenar al responsable o encargado del tratamiento que aplique medidas correctivas específicas, las cuales pueden ser: rectificación, supresión o limitación del tratamiento de datos personales.

E. SEGURIDAD DE LA INFORMACIÓN

Los principales aspectos del reglamento en materia de seguridad de los datos son:

1. Evaluación de Riesgos y Medidas de Seguridad

Los responsables y encargados del tratamiento deberán realizar una evaluación de riesgos para identificar las amenazas potenciales a los datos personales y determinar las medidas de seguridad necesarias. En las evaluaciones se revisará consentimiento, naturaleza y fin del tratamiento, los riesgos a los cuales están expuestos los datos personales. Se deberán implementar medidas de seguridad para proteger los datos personales, entre ellas:

a. ***Pseudonimización y cifrado de datos personales*** para asegurar la protección de información calificada como sensible.

b. Se debe establecer el ***Control de acceso a los datos personales*** de tal manera que solo el personal autorizado pueda acceder a dichos datos personales.

c. Las ***Copias de seguridad*** de forma regular para prevenir la pérdida de datos.

d. ***Sistemas de protección contra malware*** y cualquier otra amenaza de seguridad contra Protocolos de comunicación que sean seguros para proteger los datos mientras

son almacenados, durante la transmisión y tratamiento.

Se deben configurar sistemas de manera que por defecto solo se traten los datos personales necesarios para cada propósito específico del tratamiento. Todas las violaciones reportadas por parte de los interesados deben ser reportadas inmediatamente o en menos de 72 horas por parte del responsable del tratamiento, a la autoridad competente (SEPD). Si la violación de datos personales resulta en un ***alto riesgo*** para los derechos fundamentales y libertades de las personas físicas, el responsable del tratamiento deberá comunicar la violación a los interesados sin dilación indebida. La notificación de la violación de los derechos personales debe incluir:

a. *Naturaleza* de la violación de datos personales.
b. Registros de *datos personales afectados.*
c. Posibles *consecuencias* de la violación de datos personales.
d. Las *medidas adoptadas* o propuestas para hacer frente a la violación y, si es pertinente, medidas para mitigar sus posibles efectos negativos.

Evaluaciones de Impacto sobre la Protección de Datos (DPIA)

Estas evaluaciones de impacto deben incluir:

a. Descripción del tratamiento previsto y fines del tratamiento,
b. Evaluación y proporcionalidad del tratamiento,
c. Evaluación de los riesgos a los cuales esta expuesto los derechos y libertades; y
d. Medidas previstas para hacer frente a los riesgos.

F. SUPERVISIÓN Y CUMPLIMIENTO

La supervisión del cumplimiento del Reglamento (UE) 2018/1725 está a cargo del Supervisor Europeo de Protección de Datos (SEPD) ***autoridad independiente*** responsable de supervisar el tratamiento de datos personales por parte de las instituciones y organismos de la Unión Europea.

El SEPD actúa con independencia en el desempeño de sus funciones. En el cumplimiento de las funciones y responsabilidades hará ***monitoreo a las instituciones*** y organismos de la UE tratan los datos personales. Llevaran a cabo ***investigaciones y auditorías*** sobre el tratamiento de datos personales para verificar el cumplimiento. Proporciona ***orientación y asesoramiento*** a las instituciones y organismos de la UE sobre cómo cumplir con las disposiciones del reglamento.

El SEPD gestionara a las reclamaciones presentadas por los interesados que consideran que sus derechos han sido vulnerados y podrá ***emitir opiniones y recomendaciones*** sobre cualquier aspecto relacionado con la protección de datos personales. Tendrá autoridad para ordenar que se rectifique, elimine o restrinja los datos personales que se estén tratando de manera no conforme con el reglamento. Por último, aunque el SEPD no puede imponer multas, puede ***recomendar acciones disciplinarias*** en casos de incumplimiento grave.

El SEPD cooperara con las ***autoridades nacionales*** de protección de datos de los Estados miembros de la UE para asegurarse que se aplique de forma coherente las normas de protección de datos y su reglamento. El SEPD participara en el ***Comité Europeo de Protección de Datos (EDPB),*** que facilitara la cooperación y la coherencia en la aplicación del Reglamento General de Protección

de Datos (GDPR) y del Reglamento (UE) 2018/1725.

IV. ANALISIS DEL MARCO LEGAL DE HONDURAS EN MATERIA DE PROTECCION DE DATOS PERSONALES

La legislación específica en materia de protección de datos personales y privacidad en Honduras aún se encuentra en desarrollo. Existe normativas aislada, como la ***Constitución de la República de Honduras***: en el artículo 76 la proclamación del derecho de los interesados en la protección de sus derechos y libertades: *"Articulo 76.- Se garantiza el derecho al honor, a la intimidad personal y a la propia imagen"* (CONSTITUCION DE LA REPUBLICA DE HONDURAS, Decreto no. 131 - 1982) En vista que el concepto quedaba muy limitado, se iniciaron modificaciones para modernizar y ampliar este concepto. En el DECRETO 381-2005 (Decreto 381-2005 REFORMA HABEAS DATA CONSTITUCION DE LA REPUBLICA DE HONDURAS, 2005) se define **el Habeas Data** en el Articulo 182 numeral 2) Reformado: *"Para obtener **acceso** a la información, **impedir su transmisión** o divulgación, **rectificar** datos inexactos o erróneos, **actualizar** información, exigir confidencialidad y la eliminación de información falsa, respecto de cualquier archivo o registro, privado o público, que conste en medios convencionales, electrónicos o informáticos, que se produzcan daño al honor, a la intimidad personal, familiar y a la propia imagen. Esta garantía no afectará el secreto de las fuentes de información periodística."* (Decreto 381-2005 REFORMA HABEAS DATA CONSTITUCION DE LA REPUBLICA DE HONDURAS, 2005). Establece el concepto ampliando a la **imagen personal** y adoptando los derechos ARCO.

Seguidamente en el mismo artículo, encontramos las acciones en caso qué los derechos personales se vean afectados: *"Las acciones del Habeas Corpus o Habeas Data se ejercerán 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 libre de costas. Únicamente conocerá de la garantía de Habeas Data la sala constitucional de la Corte Suprema de Justicia. Los titulares de los órganos jurisdiccionales no podrán desechar estas acciones constitucionales y tienen la obligación ineludible de proceder de inmediata para hacer cesar la violación a la libertad, la seguridad personal, el honor, la intimidad personal, familiar o la propia imagen. Los titulares de los órganos jurisdiccionales que dejaren de admitir estas acciones incurrirán 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 delito de detención legal."* (Decreto 381-2005 REFORMA HABEAS DATA CONSTITUCION DE LA REPUBLICA DE HONDURAS, 2005) Se establece una vía para atención de reclamaciones expedita, pero sin una autoridad a nivel nacional que oriente y de seguimiento.

Código Penal: contiene algunas disposiciones relacionadas con delitos informáticos y protección de datos de manera limitada. (CODIGO PENAL DECRETO No.130-2017, 2017)

***Decreto 33-2020*:** incluye normas orientados a la simplificación administrativa, pero en su sección octava contiene la implementación de mecanismos de comercio y firma electrónicos. No se centra exclusivamente en la protección de datos personales. (Decreto Legislativo No.33-2020 Seccion Octava., 2020)

Circulares CNBS No.025/2022 y CNBS No.008/2023: emitidas por la Comisión Nacional de Bancos y Seguros (CNBS), establecen las normas para la gestión de contrataciones por medios electrónicos, ciberseguridad, tecnologías de información y continuidad del negocio, así como lineamientos para prevenir fraudes y estafas cibernéticas. Estas circulares representan un paso hacia la protección de los datos, pero limitado al sector financiero.

Ley de Transparencia Financiera y Acceso a la Información pública: ratifica el derecho constitucional Habeas data, mantiene en su artículo 23, 24 y 25 que dicen así: *"ARTÍCULO 23.- HÁBEAS DATA. Se reconoce la garantía de Hábeas Data. ARTÍCULO 24.- SISTEMATIZACIÓN DE ARCHIVOS PERSONALES Y SU ACCESO. Los datos personales serán protegidos siempre. El interesado o en su caso el por si 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* (Ley de Transparencia y Acceso a la Informacion Publica Decreto Legislativo No.170-2006, 2006) nuevamente no amplia los procesos de reclamación.

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" (Ley de Transparencia y Acceso a la Informacion Publica Decreto Legislativo No.170-2006, 2006) De esto se basa la IAIP para liderar las actividades del proyecto de Ley de protección de datos y privacidad.

Existen organismos e instituciones que, de manera aislada, abordan aspectos de la protección de datos y la ciberseguridad. Pero no existe una autoridad central específica para la protección de datos personales. La Comisión Nacional de Bancos y Seguros (CNBS) es la entidad responsable de la regulación y supervisión de la protección de datos, pero exclusiva para el sector financiero.

Es imperativo la protección de los datos personales de una forma integral, como lo menciona Fredis Medina Escoto y Armando Jipsion en su artículo Gobernanza de Datos Publico en Honduras: *"La correcta gobernanza y gestión de los datos públicos permitirá la sostenibilidad de operaciones electrónicas, permitiendo contar con servicios efectivos, seguros, ágiles, modernos, competitivos, ubicuos y transparentes; permitiendo el ahorro de tiempo y dinero a los ciudadanos y a los gobiernos"*(Escoto & Jipsion, 2019)

Ante la falta de una legislación específica se presentó la iniciativa del **Proyecto de Ley Sobre la Protección de Datos Personales** presentado por el **Instituto de Acceso a la Información Pública (IAIP)** (proyecto de ley sobre la Protección de Datos Personales presentado por el Instituto de Acceso a la Información Pública (IAIP) , 2013) en Honduras representa un paso importante hacia la regulación de la privacidad y protección de datos en el país. Sin embargo, como todo proyecto de ley, puede tener algunas debilidades o áreas que requieren mejoras.

A continuación, se presentan algunas posibles debilidades del proyecto de ley:

1. Ambigüedades y Generalidades en el Lenguaje

El proyecto puede no especificar claramente los límites del ámbito de aplicación, especialmente en términos de qué tipo de entidades y que tipos de

datos personales estarán sujetos a esta regulación.

2. Falta de Claridad en los Derechos de los Interesados

Los derechos de los interesados, como el derecho de acceso, rectificación, cancelación y oposición (ARCO), pueden no estar suficientemente desarrollados o detallados, lo que dificulta su ejercicio efectivo.

3. Debilidades en las Obligaciones de los responsables y Encargados del Tratamiento

Las responsabilidades y obligaciones de los responsables y encargados del tratamiento de datos pueden no estar claramente delineadas, lo que podría llevar a la falta de rendición de cuentas y a la evasión de responsabilidades.

4. Falta de Detalles sobre Supervisión y Cumplimiento

Puede haber debilidades en la estructura y poderes de la autoridad de supervisión encargada de hacer cumplir la ley, como la falta de independencia, recursos insuficientes o poderes de ejecución limitados. Las sanciones y multas por incumplimiento pueden no ser suficientemente disuasorias o bien definidas, lo que podría reducir la efectividad de la ley para prevenir violaciones de datos.

5. Incoherencias con Normativas Internacionales

El proyecto de ley puede no estar completamente alineado con las normativas internacionales y mejores prácticas, como el Reglamento General de Protección de Datos (GDPR) de la UE, lo que podría dificultar la cooperación internacional y la confianza en el marco legal hondureño.

6. Capacitación y Concienciación Insuficientes

La falta de apoyo técnico y recursos para las organizaciones y entidades encargadas de cumplir con la ley puede dificultar su implementación y cumplimiento efectivo.

APLICACIÓN PRÁCTICA EN HONDURAS

El Instituto de Acceso a la Información Pública (IAIP) de Honduras, está principalmente enfocado en garantizar el acceso a la ***información pública y la transparencia en la administración pública.*** Esta finalidad puede parecer en contradicción con la función de ***supervisión de la protección de datos personales,*** que se centra en la ***privacidad*** y la protección de la información ***en el ámbito privado.***

Por lo anterior, se considera apropiado la creación de una autoridad de protección de datos ***independiente y especializada*** que esté claramente separada del IAIP. Se debería contar con los recursos necesarios para supervisar y garantizar la protección de datos personales **en todos los sectores,** tanto público como privado.

V. CONCLUSIONES

Honduras necesita de un **marco legal integral** para afrontar la transformación digital, que proporcione un ambiente legal de protección de datos tendiente a promover el desarrollo económico y digital en Honduras.

El Reglamento (UE) 2018/1725 establece un marco sólido para la seguridad de los datos personales en las instituciones y organismos de la Unión Europea, abarcando desde la **evaluación de riesgos y la implementación de medidas de**

seguridad, hasta la notificación de violaciones de datos personales y la protección de datos desde el diseño y por defecto. Estas disposiciones garantizan que los datos personales sean tratados de manera segura, leal y que se protejan contra accesos no autorizados, alteraciones, pérdidas o destrucción, respetando los derechos y libertades de las personas físicas que deben ser trasladadas a las leyes de Honduras.

La **supervisión del cumplimiento** del Reglamento (UE) 2018/1725 se basa en un sistema integral que incluye la **vigilancia proactiva por parte del Supervisor Europeo de Protección de Datos (SEPD,** mecanismos internos de control en las instituciones y organismos de la UE, transparencia en las actividades de tratamiento de datos, y cooperación con otras autoridades de protección de datos. Las autoridades están claras en el Reglamento y podría aplicarse a las leyes en Honduras.

El Reglamento (UE) 2018/1725 también incluye mecanismos robustos de **supervisión y cumplimiento,** incluyendo la creación de la figura del **delegado de Protección de Datos (DPO)**, quien es responsable de asegurar que una organización cumpla con las regulaciones de protección de datos. Además, establece sanciones severas por incumplimiento.

El IAIP, con su mandato centrado en la transparencia y el acceso a la información pública, puede no ser la opción más adecuada para supervisar la protección de datos personales, dado el potencial conflicto de intereses y la necesidad de especialización en privacidad.

Si bien el proyecto de ley sobre la Protección de Datos Personales presentado por el IAIP en Honduras es un paso positivo hacia la regulación de la privacidad y protección de datos, presenta varias áreas que pueden requerir mejoras. El Plan Nacional de Desarrollo Digital debe continuar en beneficio de todas las partes.

VI. VI. RECOMENDACIONES

1. Adoptar una ley específica de protección de datos personales acorde a los estándares internacionales, para garantizar una protección robusta y coherente de los datos personales.

2. Establecer una autoridad nacional independiente como la Unión Europea, **Comité Europeo de protección de datos (EDPB),** el **Supervisor Europeo de Protección de Datos (SEPD)** que son autoridades a nivel internacional y nacional, y en cada organización e institución se encuentra el **delegado de Protección de Datos (DPD)** para la supervisión y mecanismos de cooperación regional para fortalecer la gobernanza y la implementación efectiva de la normativa.

3. Adoptar un enfoque de supervisión y cumplimiento, pero tomando referencia Reglamento (UE) 2018/1725 y Reglamento General de Protección de Datos (GDPR) que tienen un componente de **promoción** del uso de la tecnología y comercio electrónico.

4. Crear y fortalecer mecanismos de **cooperación entre diferentes entidades gubernamentales y regionales** para asegurar la implementación efectiva y el cumplimiento de las normativas de comercio electrónico.

5. Implementar **campañas de educación y concienciación para ciudadanos** y empresas sobre la importancia de la protección de datos personales y las mejores prácticas para garantizar la privacidad.

VII. BIBLIOGRAFÍA

(2017). CODIGO PENAL DECRETO No.130-2017.

CONSTITUCION DE LA REPUBLICA DE HONDURAS. (11 de Enero de Decreto no. 131 - 1982). Obtenido de TRIBUNAL SUPERIOR DE CUENTAS: https://www.tsc.gob.hn/biblioteca/index.php/leyes/177-constitucion-de-la-republica-de-honduras

(s.f.). decr.

(2005). Decreto 381-2005 REFORMA HABEAS DATA CONSTITUCION DE LA REPUBLICA DE HONDURAS.

Decreto Legislativo No.33-2020 Seccion Octava. (03 de Abril de 2020). Obtenido de Tribunal Superior de Cuentas: https://www.tsc.gob.hn/web/leyes/Decreto-33-2020.pdf

Escoto, F. M., & Jipsion, A. (2019). Gobernanza de datos públicos en Honduras. Recuperado el 2 de 9 de 2024, de https://ridda2.utp.ac.pa/handle/123456789/7059

(2006). Ley de Transparencia y Acceso a la Informacion Publica Decreto Legislativo No.170-2006.

(2013). proyecto de ley sobre la Protección de Datos Personales presentado por el Instituto de Acceso a la Información Pública (IAIP) .

Ramiro, M. A. (2008). La protección de datos personales en los países de la Unión Europea. Revista Jurídica de Castilla y León(16), 113-168. Recuperado el 2 de 9 de 2024, de http://jcyl.es/web/jcyl/binarios/763/616/02-arenas.pdf?blobheader=application/pdf;charset=utf-8&blobheadername1=cache-control&blobheadername2=expires&blobheadername3=site&blobheadervalue1=no-store,no-cache,must-revalidate&blobheadervalu

(2018). REGLAMENTO (UE) 2018/1725 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 DE OCTUBRE DE 2018 DE LA UNION EUROPEA .

Rivera, S. J. (2008). El derecho a la protección de la vida privada y el derecho a la libertad de informaciónen la doctrina y en la jurisprudencia. Una perspectiva en Bolivia. Estudios Constitucionales, 6(1), 43-67. Recuperado el 2 de 9 de 2024, de http://redalyc.org/pdf/820/82060103.pdf