ANÁLISIS DEL PROYECTO DE LEY DE PROTECCIÓN DE DATOS PERSONALES DE HONDURAS, UNA PERSPECTIVA COMPARADA

DOI: https://doi.org/10.5377/lrd.v46i1.21572

Liza Escober G.[1]
ORCID: 0000-0002-2998-6737

Alberto Rivas-Almendares.[2]
ORCID: 0000-0002-9724-1120

RESUMEN:

Los avances tecnológicos de la cuarta revolución industrial, particularmente del comercio electrónico y las redes sociales, han marcado una evolución en casi todos los aspectos de la vida y también el auge acelerado de los mercados digitales. Este fenómeno trajo tantas bondades como amenazas, por lo que se pretende destacar la importancia del resguardo de la persona humana en cuanto a su privacidad como derecho inherente frente a estos espacios virtuales donde se recopilan datos de forma masiva y sin regulación local. Por tanto, el presente estudio, cuya metodología es la revisión documental, la exégesis y la sistematización, hace un análisis del proyecto de ley de protección de datos personales de Honduras con relación a los estándares internaciones pioneros pautados por la Unión Europea (UE) y busca identificar si tiene similitud con la regulación de países de la región. Los resultados muestran que el proyecto sí demuestra un apego a los principios rectores establecidos por el reglamento de la UE y, de ser aprobado, se contaría con una legislación ventajosa con algunas oportunidades de mejora dentro del contexto regional.

PALABRAS CLAVE:

Protección de datos, Tecnología, Privacidad, Derechos Humanos, Leyes.

Fecha de recepción: 29/5/2025
Fecha de aprobación:10/11/2025

1 Docente de la Carrera de Derecho, Universidad tecnológica Centroamericana (UNITEC), Tegucigalpa, Honduras.
Correo Electrónico: liza.escober@unitec.edu.hn
2 Docente de la Carrera de Derecho, Universidad tecnológica Centroamericana (UNITEC), Tegucigalpa, Honduras.
Correo Electrónico: albertitorivass@gmail.com

ANALYSIS OF THE DRAFT DATA PROTECTION LAW OF HONDURAS: A COMPARATIVE PERSPECTIVE

DOI: https://doi.org/10.5377/lrd.v46i1.21572

Liza Escober G.[3]
ORCID: 0000-0002-2998-6737

Alberto Rivas-Almendares.[4]
ORCID: 0000-0002-9724-1120

ABSTRACT:

The technological advances of the fourth industrial revolution, particularly e-commerce and social networks, have marked an evolution in all aspects of society's life and the accelerated rise of digital markets. This phenomenon brought as many benefits as threats, which is why it is intended to highlight the importance of protecting the human person in terms of their privacy as an inherent right against these virtual spaces where data is collected massively and without local regulation. Therefore, the present study, whose methodology is documentary review, exegesis and systematization, analyzes the personal data protection bill of Honduras in relation to the international standards set by the European Union (EU) due to which are a reference to guide the related bill and identify its status in relation to other countries in the region. The results show that the project does demonstrate adherence to the guiding principles established by the EU regulation and, if approved, there would be advantageous legislation with some opportunities for improvement within the regional context.

KEY WORDS:

Data protection, Technology, Privacy, Human Rights, Law.

Reception date: 05/29/2025
Approval date: 11/11/2025

3 Professor of Law, Central American Technological University (UNITEC), Tegucigalpa, Honduras. Email: liza.escober@unitec.edu.hn
4 Professor of Law, Central American Technological University (UNITEC), Tegucigalpa, Honduras. Email: albertitorivass@gmail.com

I. INTRODUCCIÓN

La sociedad del siglo XXI ha sido testigo del avance acelerado de la tecnología, reconociendo que ya no se puede vivir ignorándole y que es indispensable adaptarse a esta, si se desea percibir los beneficios en todas las actividades del ser humano como la industria, la economía, el comercio, las finanzas, entre otros. Esta nueva etapa, conocida como Cuarta Revolución Industrial o Industria 4.0, se consolidó como tal en el 46° Foro Económico Mundial en Davos, Suiza, año 2016, en esta reunión internacional se reflexionó sobre su potencial, riesgos e impacto y se instó a los líderes mundiales a revisar sus políticas y su consecuente adaptación a los cambios; en pocas palabras se motivó a los gobiernos y empresas a profundizar en el mundo de la alta tecnología y sus consecuencias (Perez, 2016).

Sin embargo, los cambio acelerados de esta etapa han traído consigo vulneraciones para las cuales el mundo no ha estado preparado, por ejemplo, un evento relevante fue protagonizado por Facebook, la red social más grande del mundo que fue atacada por Cambridge Analítica, empresa dedicada a la recolección de datos en el Reino Unido pudiendo acceder ilícitamente a los perfiles de 87 millones de usuarios para identificar patrones de comportamiento, ideología y opiniones de los usuarios con fines de influir en los resultados electorales de los Estados Unidos de Norteamérica en 2016 (Grupo Atico, 2023). Asimismo, plataformas como Yahoo, Quora, Target, Equifax, Marriot, Dropbox, Sony Pictures, eBay, Linkedln entre otras, son otras plataformas que fueron objeto de ciberataques que tuvieron como consecuencia la exposición de la información personal de cientos de millones de usuarios.

Existen datos más sensibles como aquellos que almacenan las instituciones financieras, centrales de riesgo oficiales y burós de crédito privados, centros hospitalarios y el Estado mismo, cuya vulnerabilidad ha podido pasar desapercibida por la confianza del público en el principio de confidencialidad del sector. Pero también existen otras industrias, como la de telecomunicaciones, quienes pueden colectar datos tan delicados como la ubicación de las personas en tiempo real, su círculo cercano de interacción, conversaciones, medios de pago y recientemente, datos biométricos, como la identificación facial.

Tiempo atrás, en enero de 2024 la empresa regional latinoamericana, CLARO, hizo del conocimiento público mediante un comunicado en sus sitios oficiales, que fue víctima de un Ransomware; una especie de robo de datos con fines de extorsión, por el que se vieron afectados algunos de sus equipos que tuvieron que ser aislados y otros apagados temporalmente (Infobae, 2024). Esta situación no tuvo el impacto que debió generar en la sociedad hondureña porque no se aclaró sobre la gravedad del problema y sus consecuencias, así que se secuestraron y, a su vez, estuvieron expuestos datos sensibles como historiales de comunicación, números de tarjetas de crédito y hasta geolocalizaciones personales (Osorio, 2024).

Lo anterior ha despertado una alarma de seguridad entre los ciudadanos conscientes de la vulneración de su derecho a la privacidad. Se hizo evidente que la sociedad y los tomadores de decisiones necesitan estar listos para reconocer estas amenazas como nunca. Es menester poner interés en regular la privacidad digital o derecho a la intimidad, la seguridad y la ética para los usuarios (Chavarri & Terol, 2020) e incluir dentro de la misma necesidad, los datos personales de las instituciones financieras y comerciales que almacenan datos de personas naturales pese a de que tengan su propia regulación.

Se plantea entonces una premisa que no existía hace 20 años, si el acceso no autorizado de la información personal almacenada en servidores presuntamente de forma segura ¿representa una transgresión al derecho a la intimidad de las personas? Efectivamente, ya ha sido confirmado por varios estudios, la protección de datos personales es un derecho humano fundamental en la era de la tecnología (Visar, 2023), así como lo son los captados por el ecosistema financiero digital (Hidayatulloh, 2023) y la obligación del Estado, como afirma García-Gonzalez (2007), "exige un reconocimiento en sede constitucional".

Por supuesto, así lo recogen tratados internacionales, la legislación, doctrina y jurisprudencia de la Unión Europea y otros países alrededor del mundo, incluyendo de Latinamerica; sin embargo, en Honduras pese a que la evolución de la tecnología le sigue los pasos al primer mundo, aun no se protege ni se sanciona, por ley, el acceso de información sin el consentimiento de los usuarios.

Desde 1982, la Constitución de la República de Honduras [Const.], estableció los derechos concernientes la las libertades individuales del ser humano, determinando que la vida, la integridad física, síquica y moral, la igualdad, el honor, la intimidad personal y familiar, y las libertades personales, de expresión, de asociación, de circulación, de defensa y de culto son motivo de tutela jurídica por parte del Estado (Const, 1982)

No obstante, con el referido avance tecnológico, las obligaciones nacidas de los tratados internacionales como el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana de Derechos Humanos, es inminente que Honduras tiene que adaptar su marco jurídico e institucional a esta nueva necesidad.

De igual manera, localmente, se han hecho aproximaciones a estos conceptos mediante la Ley de Transparencia y Acceso a la Información Pública, pero desde la perspectiva del derecho de los ciudadanos para conocer datos que deben de ser públicos, enfocándose en la administración pública, la transparencia de sus funcionarios y sus operaciones. Esto es distinto al objeto de este estudio, que es abordar la protección de la información personal pero desde la pespectiva del sector privado, tal y como, la intimidad personal vunerable ante la entrega voluntaria y/u obligatoria de datos sensibles a las empresas proveedoras de bienes y servicios y las obligaciones que esto implica, no solo de forma contractual, sino, por sometimiento a la potestad normativa y punitiva del Estado para la tutela del bien jurídico en cuestión.

Esta oscuridad normativa ya ha sido señalada por los organismos internacionales relacionadas con los derechos humanos, especialmente las Naciones Unidas mediante resolución 45/95 sobre los Principios Rectores para la Reglamentación de las Bases Computarizadas de Datos personales, la Red Interamericana de Protección de Datos personales, entre otros; por esta razón, el Instituto de Acceso a la Información Pública (IAIP) ha propuesto un proyecto de ley desde el año 2018, mismo que permanece en revisión en el Poder Legislativo y no ha sido aprobado por razones desconocidas, aun cuando su objetivo es precisamente ser el mitigador del riesgo de exposición de datos personales sin autorización o con fines distintos para el que fueron otorgados, creando un ente supervisor y con efectos punitivos por incumplimiento.

Conforme al planteamiento anterior, entonces, el objetivo de este estudio es analizar el referido proyecto de Ley considerando el estándar internacional referente, el Reglamento de Protección de Datos Personales de una la unión

Europea (RGDP), contrastarlo con legislacion de otros países que compartan el derecho romano-germánico con regulación de protección de datos personales. Finalmente, se podrá determinar si el paso que dará Honduras con la aprobación de esa propuesta tiene solidez jurídica para proteger este derecho inherente al ser humano.

II. METODOLOGÍA

Este estudio se desarrolló bajo la metodología de la investigación jurídica cualitativa (Hernandez-& Durán, 2002). Para ello, entre varias técnicas se recurrió a la técnica de análisis documental que lo define Corbetta (como se citó en Tonon, 2011) como aquel análisis que trabaja con documentos que sirven como material informativo de un determinado tema y permite estudiar el pasado. Se utilizaron documentos sobre tecnología, seguridad de la información, derecho positivo nacional e internacional y el proyecto de ley. Finalmente, se utilizó la interpretación jurídica que como explica Ramos (2011), "es una operación en la cual se busca dar sentido a algo" (p. 123); y en este caso es para comprender el cumplimiento de los estándares internacionales de normas jurídicas regionales en materia de protección de datos personales.

Además, se aplicó el derecho comparado, pero limitado a una micro comparación. La micro comparación se puede definir según Mancera (2008) como aquella que "selecciona un tema específico dentro de un sistema jurídico, lo que tiene que ver con seleccionar el sujeto a comparar" (p. 228); para esto fueron seleccionados países de la familia del derecho romano-germánico dado a que este derecho es el que comparten algunos países europeos, latinoamericanos, gran parte de África, países del cercano oriente, Japón e Indonesia (Instituto de Investigaciones Juridicas de la UNAM, 2010). El tema específico fue el proyecto de Ley de Protección de Datos de las personas naturales, aplicable especialmente al sector privado para contrastarlo con otra normativa utilizando categorías de análisis dependientes de los principios rectores del RGDP por ser este el referente y pionero para la creación y reforma de las leyes para los países de derecho codificado.

III. RESULTADOS

3.1. Fase Descriptiva

Como establece Mancera (2008) "la fase descriptiva consiste en describir cada uno de los conceptos, reglas, instituciones o procedimientos seleccionados" (p. 229). Por lo que se hace una descripción acerca del Reglamento General de Protección de Datos de la Unión Europea ya que contiene los principios rectores que serán la categoría base de comparación. De igual forma, se describen las leyes de España, México, Ecuador y Costa Rica con relación al proyecto de ley hondureño.

El Reglamento General de Protección de Datos Personales de la Unión Europea (RGDP)

La Carta de los Derechos Fundamentales de la Unión Europea y el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales disponen y garantizan que toda persona tiene derecho a la protección de los datos de carácter personal, este precepto es el fundamento para crear el Reglamento (UE) 2016/679 (RGDP), adoptado en 2016 y con vigencia desde mayo de 2018. Este instrumento jurídico estandariza las leyes de protección de datos de toda la Unión Europea debido a que las regulaciones anteriores no se habían adaptado suficientemente a la era digital.

El RGDP se aplica a todas las organizaciones que traten datos de personas naturales, busca establecer derechos y libertades fundamentales para los individuos en cuanto a sus datos personales y su protección, bajo la premisa de que, dato personal, es toda información sobre una persona natural identificada o identificable cuya identidad pueda corroborarse, de forma directa o indirecta, mediante un nombre, un número de identificación, datos de ubicación, rasgos biométricos, psíquico, económico, cultural o social de la persona. Asimismo, consigna como derechos de los individuos respecto a esos datos personales: el derecho a ser informados sobre la recopilación de información, el de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y posición al tratamiento de la información. (RGDP, art.4, 2016,).

El RGPD se basa en 7 principios básicos relativos al tratamiento de datos personales. Estos principios son los siguientes:

1. Licitud, lealtad y transparencia en el tratamiento de los datos del individuo.
2. Minimización de datos, el cual disminuye la cantidad de datos que se permiten recolectar, almacenar y transferir
3. Limitación de la finalidad, o sea limitar al responsable de manejar los datos, de realizar lo que se quiera con estos.
4. Exactitud, para que los datos recolectados sean correctos y que no se almacenen con errores.
5. Limitación en el plazo de conservación, este principio limita el tiempo.
6. Integridad y confidencialidad de tal manera que se garantice una seguridad adecuada y la protección otra el tratamiento no autorizado o ilícito, pérdida y destrucción o daño accidental.
7. Responsabilidad Proactiva: exige una participación de los responsables del tratamiento de los datos en cuanto al cumplimiento de la normativa. (RGDP, art.5, 2016,).

La incorporación del RGPD de España

El Reino de España es previsor en materia de protección de datos personales desde su Constitución. Española, Art.18.4, 1978 (España), cuyo capítulo segundo es contentivo de los derechos y libertades del individuo y hace referencia a que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal, estipulación innovadora que avistaba la era de la digitalización y los riesgos frente a las nuevas tecnologías.

La Ley aborda aspectos clave como el consentimiento para el tratamiento de data personal, las obligaciones de los entes que manjean datos, las medidas de seguridad, las garantías y derechos de los ciudadanos con relación a sus datos y la regulación de aspectos específicos como el derecho al olvido, la portabilidad de los datos y la limitación del tratamiento de datos, conforme a los estándares exigidos por la UE. Además, incorpora disposiciones sobre derechos digitales, como el derecho a la intimidad y uso de dispositivos en el ámbito laboral, la protección del menor en internet y la regulación del uso de cámaras de video vigilancia y sistemas de geolocalización en el contexto laboral, lo mas importante, la consolidadción de un marco institucional sólido (AEPD, 2019).

En especial, los derechos reconocidos en este instrumento son, el derecho de información, acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición, con el

reconocimiento de los derechos ARCO (acceso, rectificacion, cancelación y oposición). Los principios de protección de datos personales se distinguen como el de exactitud, confidencialidad, tratamiento basado en el consentimiento del afectado, consentimiento de los menores de edad, tratamiento de datos por obligación legal, interés público ejercicio de poderes públicos, categorías especiales de datos y tratamiento de datos de naturaleza penal (AEPD, 2019).

Protección de datos personales en México

En julio de 2002, se publicó la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Esta norma tuvo como finalidad regular el acceso a la información pública y garantizar la protección de datos personales en posesión de los sujetos obligados (Gomez, 2020). Esta fue la primera legislación en cuanto al derecho de acceso a la información se refiere, pero surtía efecto para las entidades gubernamentales y no protegía a los ciudadanos del flujo y tratamiento de sus datos personales frente a las empresas privadas. En consecuencia, entra en vigor la Ley Federal de Protección de Datos Personales en Posesión de los Particulares [LFPDPPP], 5 de julio de 2010.

Esta norma que nace con el objetivo de regular a los particulares que realizan la recolección y manejo de datos personales de los individuos y para garantizar a estos el derecho a la privacidad y la autodeterminación informativa. Los sujetos a esta legislación son las personas naturales o jurídicas de carácter privado que por motivos de su accionar tengan manejos de bases de datos con información personal de los ciudadanos. Los principios de esta ley son licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad (LFPDPPP , 2010).

Con el transcurrir del tiempo, en 2017 se completó este marco normativo con una disposición que protege los datos personales en posesión de autoridades o entes gubernamentales dentro de la estructura estatal reconociendo los derechos de acceso, rectificación, cancelación y oposición (ARCO).

Protección de datos personales en Ecuador

En el año 2016 comienza un proceso para la creación de una Ley acerca de este tema, impulsado por el Tratado de Libre comercio con la Unión Europea acerca de relaciones comerciales de integración económica lo cual creo una necesidad de regular el flujo y transferencia de datos personales.

Dicho proceso fue impactado de manera negativa por lo que hasta el año 2019 se presenta el proyecto de Ley y finalmente entra en vigor la Ley Orgánica de Protección de Datos Personales en el Ecuador [LOPDP], 26 de mayo, 2021. Nace con el objetivo de garantizar a los ciudadanos el derecho a la protección de datos. Los principios contenidos en esta legislación son el principio de juridicidad, principio de lealtad, principio de transparencia, principio de finalidad, principio de pertinencia y minimización de datos, principio de proporcionalidad de tratamiento, principio de confidencialidad, principio de calidad y exactitud, principio de conservación, principio de seguridad de datos personales, principio de responsabilidad proactiva y finalmente el principio de aplicación favorable al titular.

Protección de datos personales en Costa Rica

Se aprobó y público en el año 2011 la Ley No. 8968 – Protección de la Persona frente al Tratamiento de sus Datos personales y el correspondiente Reglamento N° 37554-JP. Cuyo

objetivo es garantizar a las personas el derecho a la autodeterminación informativa, como Derecho Fundamental derivado del Derecho a la privacidad e intimidad consignada en el artículo 24 de la Constitución Política (Durango, 2024).

Es importante mencionar que antes de promulgarse la Ley 8968, Costa Rica ya contaba con jurisprudencia sobre el derecho fundamental a la Autodeterminación Informativa, conceptualizándose como el derecho de toda persona a la información colectada, sea pública o privada; a conocer la finalidad de destino de la información, a estar informado del procesamiento de los datos, el derecho de acceso, corrección o eliminación de estos y que puedan ser rectificados, actualizados, complementados o suprimidos. El derecho a la Autodeterminación Informativa está constituido por principios como el de transparencia, correspondencia entre los fines y el uso de almacenamiento, exactitud, veracidad, actualidad y plena identificación de los datos almacenados, prohibición del procesamiento de datos relativos a la esfera íntima.

La Ley de Protección de Datos en el 2011, es el ordenamiento jurídico para proteger a las personas de una realidad tecnológica con automatización en el tratamiento de los datos personales (Ley 8968, 2011).

Protección de datos personales en Honduras

En el caso de Honduras, se estipula el derecho de información en la Constitución de la República, artículo 76, el en que se garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen. Por otro lado, el artículo 100 establece que toda persona tiene derecho a la inviolabilidad y al secreto de las comunicaciones, en especial de las postales, telegráficas y telefónicas, salvo resolución judicial. Finalmente, contiene la garantía constitucional del Habeas data contenida en el Articulo 182 numeral 2 (Constitución de la República de Honduras, 1982).

Asimismo, existe la Ley de Transparencia y Acceso a la Información Pública en la cual se regula la protección y transparencia de datos en el sector público. Esta legislación carece de disposiciones sobre la protección de datos personales en el sector privado, por tanto, considerando el avance de la tecnología y la protección al derecho de intimidad, el pleno de comisionados del Instituto de Acceso a la Información Pública (IAIP) presenta en el año 2018 el Proyecto de Ley de Protección de Datos Personales.

El Proyecto de la Ley mencionado es de orden público, regula el tratamiento legítimo, controlado e informado para garantizar la protección de datos personales. Incorpora la denominación al sistema jurídico hondureño de Derechos ARCO, dicho de otra manera, acceso, rectificación, cancelación y oposición de datos personales y establece como principios y derechos básicos los de lealtad y legalidad; exactitud, finalidad de propósito; acceso a la información; consentimiento; no discriminación; seguridad, responsabilidad y confidencialidad. Además de disposiciones sustantivas, crea también obligaciones a los responsables del tratamiento de datos con sus respectivos procedimientos de cumplimiento y sancionatorios.

3.2. Identificación y comparación

El segundo paso es la fase de identificación que se puede definir como la etapa en la cual se reconocen las semejanzas y diferencias de los elementos descritos (Mancera, 2008). Esta fase se realiza con base en los principios rectores del RGDP, la legislación de España, por pertenecer a la Unión Europea y estar jerárquicamente bajo los lineamientos del reglamento referente, seguido de México, Ecuador, Costa Rica y finalmente el proyecto de Honduras.

Tabla 1. Comparación de países referente al RGDP

País	Legislación	Licitud Lealtad y Transparencia	Minimización de Datos	Limitación de la Finalidad	Exactitud	Limitación de plazo de conservación	Integridad y Confidencialidad	Responsabilidad Proactiva
España	L.O.3/2018 (2018)	Art. 11	Relación Arts. 19 y 93	Art.16	Art. 4	Relación con Arts. 32	Art.5	Relación con Arts. 28 a 32
México	LFPDPPP (2010)	Arts. 7 y 8	Relación Art. 11	Art. 12 y 13	Art. 11	Relación Arts. 3, inciso III y 25	Art. 21	Art. 19
Ecuador	LOPDP (2021)	Art. 10, incisos a, b y c.	Art. 10 inciso e.	Art. 10 inciso d	Art. 10 inciso h.	Art. 10 inciso i	Art. 10 inciso j	Art.10 inciso k.
Costa Rica	Ley 3868	Relación Art. 4 y 5	Art. 9.1	Art. 6.4	Art.6.3	Art. 6.1	Arts. 10 y 11	No
Honduras	Proyecto de ley de LPDP	Art.4, inciso a.	Art.4, inciso i	Art. 4, inciso c.	Art. 4, inciso b	Art.15	Art. 4 inciso j	Art. 4, inciso h.

Fuente: elaboración propia.

Como se puede observar en la tabla 1, se distingue por columna el país, su normativa local seguida de los principios rectores dictados por el RGDP, para mostrar de forma sistematizada los resultados de este estudio, cuyos resultados se exponen a continuación.

Es importante mencionar que, en Guatemala, aunque aún no tiene en vigor una ley específica de protección de datos privados la Ley de Acceso a la Información Pública, Decreto 57-2008, tiene un relativo marco jurídico pero no específico, por tanto, se han presentado varias iniciativas legislativas como las leyes 6103, 6105 y 5921, con dictámenes favorables o en debate que buscan establecer derechos ARCO, procedimientos claros y sanciones penales importantes, pero aún no se han incorporado a la legislación interna. Lo similar del caso es que sí cuentan con su regulación sobre transparencia de la información pública, pero como ente regulador a la Procuraduría de los Derechos Humanos (PDH). Por ahora, la sede judicial y el Amparo son las alternativas más efectivas para exigir la tutela de este Derecho.

Principio de Licitud, Lealtad y Transparencia

La licitud implica que deben cumplirse ciertas condiciones como el consentimiento del interesado para fines específicos como la ejecución de un contrato, cumplimiento de una obligación legal para el responsable, proteger intereses propios u otros y para otros fines de interés público o satisfacción de intereses legítimos; la lealtad infiere dar un tratamiento de los datos de forma apropiada al consentimiento otorgado según su sensibilidad y categoría. Y la transparencia establece que la persona natural recibirá información relacionada con el responsable del tratamiento de los datos y su finalidad; los destinatarios y motivos de transferencia de los datos de forma local e internacional; los derechos y garantías que le conciernen (RGDP, 2016).

España cumple de forma expresa con el principio y así lo ha incorporado a la política pública. México lo incluye al establecer la misma licitud para la obtención de los datos, asimismo que no se puede obtener datos personales de forma fraudulenta ni engaños y lo complementa para proteger el principio de lealtad y transparencia con el nominado aviso de privacidad, por el cual el responsable del tratamiento de datos tiene que identificar la finalidad de la recolección, opciones y medios para limitar el uso de los datos (LaFPDPPP, 2010).

Ecuador cumple con este principio homologando la licitud con juridicidad y la lealtad se consigna como la claridad de los datos que se recolectan, utilizan, consultan o se tratan; por su parte la transparencia implica el acceso fácil y comprensible de la información para el particular (LOPDP, 2021). Estos principios los robustece con la introducción del derecho de información que funciona como la herramienta por la cual el responsable del tratamiento informa al titular de todo movimiento, transferencia, utilización, entre otros, de sus datos.

Costa Rica incluye este principio, no de forma expresa o literal como el instrumento referente, pero, efectivamente, por interpretación se refiere a la autodeterminación informativa relativa al legitimo tratamiento de datos reconociéndola como derecho fundamental, derivado del derecho a la privacidad. Asimismo, considera la importancia del consentimiento y el acceso irrestricto y transparente a la información proporcionada por el titular (Ley 8968, 2011).

El proyecto de ley de Honduras incorpora expresamente el principio de lealtad y legalidad, al estipular que los datos personales no se recolectarán ni elaborarán con procedimientos desleales o ilícitos, ni se utilizarán con fines distintos a los propósitos de la Ley. Siguiendo la línea mexicana y ecuatoriana, la legislación hondureña incluye de igual forma el aviso de privacidad con la misma información y función.

Principio de Minimización de Datos

El RGPD (2016) de la Unión Europea define la Minimización de datos: "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados". Busca limitar el tratamiento de datos, con medidas técnicas y organizativas, con el objetivo de tratar los datos sumamente necesarios para cumplir el fin por el cual se recolectan. España en su normativa no lo expresa literalmente, pero está implícito en todas sus disposiciones, especialmente con el derecho al olvido de información no pertinentes y su sometimiento al RGDP.

México, obliga a los responsables a procurar que los datos sean pertinentes, correctos y para

los fines que fueron obtenidos (LFPDPPP, 2010) En la normativa ecuatoriana (LODPD, 2021) se estipula que "Los datos personales deben ser pertinentes y estar limitados a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento..." México y Ecuador buscan hacer esfuerzos por limitar la recolección de datos personales sensibles y España toma esfuerzos por limitar la recolección y manipulación de datos personales de menores de edad.

Por su parte, el proyecto de ley hondureño sí contempla una noción relativa del principio de minimización de datos, homologado como Principio de Proporcionalidad. Que expresa solo se deberán recolectar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento" (IAIP, 2018). Todos los países de forma manifiesta o tácita procuran limitar la recolección de datos sensibles y datos de menores de edad.

Principio de Limitación de Finalidad

El RGDP define el Principio de Limitación de la finalidad a aquellos recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; al igual que el principio anterior este busca asegurar que la recolección de los datos personales será para un fin específico y con tiempo limitado.

Dentro de la ley mexicana el principio de limitación de la finalidad estipula que el tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades contenidas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto o incompatible a los fines establecidos, se requerirá solicitar de nuevo el consentimiento del titular. El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad (LFPDPPP , 2010).

La legislación ecuatoriana incorpora este principio y estipula que las finalidades del tratamiento deberán ser determinadas, explícitas, legítimas y comunicadas al titular; así como que no pueden usarse los datos con fines distintos para los cuales fueron recolectados a excepción de ley (LOPDP, 2021). Similar a las otras legislaciones, la ecuatoriana incluye el derecho a la eliminación y de oposición.

En la legislación costarricense no se encuentra como tal el principio de limitación de la finalidad, pero dentro del principio de calidad de la información está el apartado de la recolección de datos adecuados al fin. La cual infiere que los datos de carácter personal serán para fines determinados, explícitos y legítimos, y no serán tratados de manera incompatible con dichos fines (Ley 8968, 2011).

El proyecto de ley en Honduras también incorpora el principio de finalidad de propósito como el tratamiento de datos personales limitado al cumplimiento de las finalidades determinadas, explícitas y legítimas. De igual forma el responsable del tratamiento, deberá limitarse a la ley (IAIP, 2018). Por otro lado, también se incluye una serie de derechos que se enmarcan como los Derechos ARCO, idénticos a los presentados por la ley mexicana y española.

Principio de Exactitud

El RGDP de la UE estipula que los datos tienen que ser exactos y, si fuera necesario, actualizados; con la habilitación del derecho de supresión o rectificación sin dilación de datos personales que sean inexactos con respecto a los

fines para los que se tratan. Este principio busca que toda la información que entren a las bases de datos sea correcta y que coincida con la realidad de las personas.

La ley mexicana LFPDPPP (2010) lo homologa como principio de calidad estipulando que "el responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados". Este principio aplica también dentro los derechos ARCO, para el de rectificación ya que este funciona como una herramienta para realizar modificaciones a la información inexacta.

Al igual que la anterior, la ley ecuatoriana establece el principio de calidad y exactitud, el cual expone que los datos personales en tratamiento deben ser exactos, íntegros, precisos, completos, comprobables, claros; y actualizados; de tal forma que sean verídicos. Aplica también el derecho de rectificación" (LOPDP, 2021).

En cuanto al principio de exactitud la ley costarricense lo contiene como el principio de calidad de la información y en este establece que los datos recolectados deben ser actuales, veraces, exactos y adecuados al fin para el que fueron obtenidos, responsabilizando a los encargos a tomar todas las medidas necesarias para evitar la inexactitud. También se otorga a los individuos el derecho de rectificación.

En el proyecto de ley hondureña, el principio de exactitud implica que los datos personales deberán ser exactos, adecuados, necesarios y no excesivos con relación a la finalidad para la cual se hubieran obtenido" (IAIP, 2018). Al igual que las demás leyes analizadas, el proyecto de ley hondureño otorga el derecho de rectificación para poder acceder a su información y actualizarla. Pero carece de otras figuras como el derecho de supresión.

Principio de Limitación en el Plazo de Conservación

El RGDP de la UE define el plazo de conservación de los datos personales como que estos deben ser almacenados de forma que se permita la identificación de los interesados únicamente para el tiempo que sea necesario; solo podrán guardarse durante períodos más largos con fines de archivo en interés público, de investigación científica o histórica o estadística para protección de los derechos y libertades del particular.

En España este principio se configura con la supresión de los datos, este a su vez impide el tratamiento de los datos cuando se extinga la finalidad que justificó su recolección, es decir, obtenido el dato ya no puede conservarse, excepto para ponerla disposición de determinadas autoridades y para la exigencia de responsabilidades derivadas del tratamiento. (AEPD, 2019). Asimismo, en México no establece plazos generales, pero sí, de igual manera, establece que los datos personales deben conservarse el tiempo necesario para cumplir con las finalidades para las que fueron recabados y con las obligaciones legales que apliquen en cada (LFPDPPP, 2010). Costa Rica no tiene esta protección.

Ecuador es el único país que incorpora expresamente dentro de su legislación noción del principio de conservación al estipular que los datos personales serán conservados durante un tiempo no mayor al necesario para cumplir con la finalidad de su tratamiento y para garantizarlo, el responsable del tratamiento establecerá plazos para su supresión o revisión periódica. Además, similar al RGDP solamente permite la conservación ampliada de los datos por razones de interés público, investigaciones científicas o históricas, que garanticen un nivel de seguridad adecuado (LOPDP, 2021).

En este caso el proyecto de ley de Honduras no incorpora el principio de límite en el plazo de conservación. Pero sí agrega la misma excepción que tienen las normativas de España y México, en cuanto al derecho de supresión. Esta excepción estipula que la conservación de esta data será por elección del responsable del tratamiento de los datos por el plazo derivado de las relaciones contractuales entre la persona interesada y este o la extinción de las responsabilidades nacidas del tratamiento (IAIP, 2018).

De igual forma, el proyecto de ley estipula que el Registro de bases de datos de titularidad privada que se creará con la aprobación de la normativa, debe proponer los tiempos máximos de conservación de datos. Esto se interpreta como que el legislador podría permitir mecanismos para limitar la conservación, pero no lo visualizan como un principio rector de la protección de datos.

Principio de Integridad y Confidencialidad

El RGDP de la UE define el principio de integridad y confidencialidad al enunciar que la información personal debe ser tratada de manera que garantice la seguridad adecuada, la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño. Este principio obliga a los responsables y encargados del tratamiento de la data.

En la legislación mexicana se encuentra establecido respecto a que el responsable o terceros que intervinientes en el tratamiento de datos tienen el deber de confidencialidad respecto de estos, lo cual permaneceré hasta después de finalizar sus relaciones con el particular o con el responsable. Este principio se protege mediante la imposición de sanciones por parte de la autoridad correspondiente. (LFPDPPP, 2010).

En Ecuador el principio de confidencialidad debe concebirse sobre la base del debido sigilo y secreto, no deben tratarse o comunicarse datos personales para un fin distinto para el cual fueron obtenidos, a menos que concurra circunstancias que habiliten un nuevo tratamiento conforme a la ley (LOPDP, 2021).

En cuanto a este principio la ley costarricense no expresa, pero sí lo recoge como el deber de confidencialidad de toda persona que tenga contacto con los datos personales o sean parte del tratamiento de estos están obligados a guardar el secreto profesional (Ley 8968, 2011).

Respecto al principio de confidencialidad el proyecto de ley estipula como el deber del responsable de no mostrar, compartir, revelar o transmitir la data almacenada a personas naturales o jurídicas que carezcan de la previa autorización por parte del titular (IAIP, 2018). Es en este apartado donde se hace alusión a la seguridad de la información por parte de los responsables.

Principio de Responsabilidad Proactiva

El RGDP de la UE define la Responsabilidad Proactiva como la responsabilidad del cumplimiento que busca garantizar que las empresas responsables del tratamiento de datos personales cumplan con la ley y con las certificaciones necesarias de seguridad para poder operar bases de datos.

En la ley mexicana se establece el principio de responsabilidad de forma específica respecto a implementar medidas de seguridad distintas para proteger contra el daño, pérdida, alteración, destrucción o el uso de los datos e incluso el acceso o uso no autorizado (LFPDPPP, 2010).

En cuanto al principio de responsabilidad proactiva la legislación ecuatoriana es la que

probablemente tenga una definición más completa, al obligar a demostrar que se han implementado mecanismos para la protección de datos personales; para lo cual, además podrá valerse de estándares, buenas prácticas, modelos de auto y co-regulación, protocolos de protección, certificación, seguridad o cualquier otro mecanismo adecuado a los fines según la naturaleza o el riesgo (LOPDP, 2021).

Este principio no se contempla expresamente como parte de los principios y derechos básicos que estipula la ley costarricense, pero en su capítulo de seguridad y confidencialidad del tratamiento de los datos introducen lo que son los protocolos de actuación. Dichos protocolos son similares a los mecanismos de autorregulación presentados en la ley ecuatoriana, teniendo como objetivo la creación de códigos de conducta en cuanto al tratamiento de bases de datos con certificación de las autoridades nacionales.

El proyecto de ley hondureño incorpora este principio en el mismo sentido anterior frente a los interesados como ante el IAIP-PRODATOS (ente supervisor) (IAIP, 2018). Aunque incorporado dentro de la normativa no se encuentran mecanismos claros para evidenciar el cumplimiento. Además, no incorpora ningún capítulo, como si lo hace la legislación española y ecuatoriana, refiriéndose a la responsabilidad proactiva que debe de existir entre los responsables del tratamiento y la autoridad nacional dejando un vacío legal que queda a interpretación de las entidades.

IV. DISCUSIÓN

Al tener por conocidas las similitudes y diferencias, concierne reconocer que la normativa española es el acercamiento más apropiado al RGDP por seguir su directriz jurídica y por contextualizarse en un escenario pionero en la recolección de datos y su tratamiento en una asociación de países geopolítica y económicamente más avanzados que toda Latinoamérica. Asimismo, una Agencia de Protección de Datos como ente regulador, resulta muy apropiado, y podría ser replicable en Honduras siempre y cuando tenga absoluta independencia funcional, capacidad técnica y tecnológica. Resulta obvio que el Reino de España tiene un sistema jurídico más evolucionado, sin embargo, esta característica lo convierte en un referente para analizar incorporando el análisis de factores culturales y políticos.

De igual manera, se debe reconocer que la legislación mexicana ha logrado un marco jurídico que tutela los datos de los particulares al igual que Costa Rica, pese a la antelación de su normativa al RGDP. Por su parte, Ecuador, también puede ser un referente cuya cultura pudiera tener más similitudes que la Española y convendría conocer la experiencia exclusiva de este caso a mayor profundidad para relacionarlo con el de Honduras. El Derecho Comparado resultará la herramienta más completa en conjunto con las ciencias como la antropología y la informática.

Con relación a la legislación hondureña, su similitud estructural y de fondo al RGDP es evidente y positiva, pues se adapta a los principios generales de forma expresa y en algunos casos tácita, pero con el mismo efecto, con sutiles diferencias, aunque sin contravenciones. Es probable que por la fecha en que ha sido elaborado el anteproyecto tenga tanta similitud y contemple una protección similar a la referente. De hecho, su aprobación colocaría a Honduras en una posición ventajosa en la región en cuanto a la protección de datos personales.

La única debilidad detectada por este estudio en cuanto al anteproyecto es que el principio que atiene al límite en el plazo de conservación, no debería dejarse al arbitrio del responsable del tratamiento, porque estos acuerdos normalmente se presentan como contratos de adhesión y en este caso, no beneficia al particular, por lo que el reglamento que autoriza a realizarse debería definir exactamente un plazo después de finalizado el negocio que dio origen a la obtención de datos y en cuanto a otras transacciones como el uso de redes sociales o comercio electrónico, también establecer una fecha de prescripción para el uso de los datos una vez finalizada la relación.

A pesar de que el anteproyecto de la ley protectora de los datos no ha entrado en vigor, según este estudio la causa de la postergación no podría ser por deficiencias de la normativa propuesta, ya que se ha comprobado que cumple con el estándar de la legislación más avanzada, entonces, se estaría ante un caso de indiferencia o falta de conocimiento del riesgo que enfrenta la privacidad de las personas. Lo cual hace evidente que existe una profunda debilidad en la legislación relativa a los negocios jurídicos electrónicos y no se ha dimensionado la vulnerabilidad de la información almacenada en medios electrónicos y su impacto en los derechos humanos, considerando que no existan intereses externos que intentan el olvido de este anteproyecto porque pudiere perjudicar los beneficios económicos del tráfico indiscriminado de datos y vulneración del individuo ante el poder del Estado.

V. CONCLUSIONES Y RECOMENDACIONES

En conclusión, la creación de legislación para la protección de los datos de la vida privada de las personas se ha convertido, en los últimos años, en prioridad para muchos países en el mundo y ahora en América Latina. La necesidad de reducir la vulnerabilidad de las personas frente a las aplicaciones y sitios web que obtienen datos sensibles es urgente, no solo para actualizar el marco normativo a una realidad global, si no para impedir que las empresas que realizan comercio electrónico, las empresas financieras y centros de datos sobre comportamientos crediticios o de consumo abusen de la confianza o ingenuidad del usuario.

El tráfico comercial de datos es una práctica habitual que actúa bajo la sombra, entre empresas que conservan bases de datos sensibles para intercambio mercantil y no existe hasta ahora forma expresa de prohibir, sancionar o mitigar los daños causados a la intimidad personal. Las violaciones o vulneraciones presentadas al inicio de este artículo han sido verídicas. Honduras, aunque de tener una población que fue vulnerada en cuanto a sus datos personales, como Estado se ha llamado al silencio, se entiende que por falta de sustento normativo y se espera que no sea tolerancia a las prácticas abusivas de las grandes empresas.

Países como el Reino de España presenta mayores avances por responder jerárquicamente a la norma de la UE, la más avanzada; pero no puede obviarse que legislaciones como las regionales no están en gran desventaja, la norma sustantiva, independientemente de sutiles diferencias es relativamente suficiente para enfrentar el fenómeno, entonces corresponde poner la atención en la aplicación de la norma y el control de los interesados y sujetos obligados. En concreto, el estudio no señala la idoneidad de la norma, debido a que delgadas discrepancias pueden complementarse con la interpretación, sino que es aún más importante identificar o crear un ente regulador no apolítico y beligerante para una aplicabilidad efectiva en sustitución del IAIP.

En el caso de Honduras, no se cree conveniente que el IAPP deba ser el ente regulador y fiscalizador, ya que su función es la transparencia de la información relativa sector público y no debería tener relación con los datos del sector privado; finalmente es un ente adscrito al Estado, además de que se cuenta con un ente centralizado casi con las mismas funciones. Difícilmente habrá un ente con suficiente independencia técnica y administrativa, especialmente por la naturaleza política clientelar del Gobierno de Honduras y considerando que se trata de un principio a tutelar que puede ser violado por el mismo Estado.

Por tanto, se cree relevante focalizar la atención en el ente supervisor, que tenga además de independencia, facultades de acción preventiva, punitiva o sancionatorias. El escenario ideal es una institución apolítica, conviene analizar el caso de la Agencia Española de Protección de Datos o trasladarle la función a una unidad especial liderada por el Comisionado de los Derechos Humanos. Lo que puede hacer la diferencia es otorgarle las potestades suficientes para supervisar dos etapas; la preventiva de exigir protocolos de seguridad robustos cuyo incumplimiento pueda ser detectado; y la coercitiva para sancionar abusos como la comercialización no autorizada de datos y el uso de la información para fines distintos. Además de tener iniciativa de Ley para exigir reformas en el Código Penal de forma complementaria a la Ley.

Es importante destacar que el presente artículo pretende que exista una reactivación del debate acerca de la protección de datos personales en la era digital en Honduras y que deben existir estudios más profundos sobre el tema. De hecho, corresponde educar a la población respecto a los principios que fueron revelados en este estudio y de las amenazas ante las que la población es vulnerable, concientizar que esta data personal es objeto de comercialización en el ámbito nacional e internacional y que su información personal puede estar generando lucro a terceros, sin su consentimiento y sin recibir ninguna contraprestación.

Finalmente, es importante el seguimiento, que se retome la aprobación del anteproyecto, reconocer que las amenazas globales frente al fenómeno han evolucionado, que uno de los poderes más importantes que se puede tener en esta época es la información de las personas, por tanto, constituye una vulnerabilidad del ciudadano frente a los recolectores de datos. Esto implica no solo la iniciativa de crear la norma, sino que el esfuerzo debe ser a más largo plazo, se debe establecer la forma de aplicarla y hacerla efectiva frente a terceros. Se debe reconocerla importancia que reviste existir en el mundo de la industria 4.0.

VI. ABREVIATURAS

- **Const.:** Constitución de la República de Honduras
- **IAIP:** Instituto de Acceso a la Información Pública
- **RGDP:** Reglamento de Protección de Datos Personales de la Unión Europea
- **UNAM:** Universidad Nacional Autónoma de México
- **UE:** Unión Europea
- **ARCO:** Acceso, Rectificación, Cancelación y Oposición
- **AEPD:** Agencia Española de Protección de Datos
- **LFPDPPP:** Ley Federal de protección de Datos <Personales en Posesión de Particulares.
- **LOPDP:** Ley Orgánica de Protección de Datos Personales en el Ecuador

VII. REFERENCIAS

Agencia Española de Protección de Datos. (2019). Guia sobre el plazo de conservación de datos N/REF: 00148/2019. Gabinete Jurídico. https://www.aepd.es/documento/2019-0148.pdf

Asamblea Nacional República del Ecuador. (2021). Ley Organica de Protección de Datos Personales, No. 459, 26 de Mayo 2021.

Chavarri, G., y Terol, M. (2020). Blog ThinkBig: Telefonica.https://blogthinkbig.com/la-era-digital-educacion-y-trabajo-detalles-de-una-transformacion#:~:text=Se%20considera%20que%20la%20era,a%20las%20tecnolog%C3%ADas%20digitales%20actuales

Congreso General de los Estados Unidos Mexicanos. (2010). Ley Federal de Proteccion de Datos Personales en Posesion de los Particulares del 5 de julio de 2010.

Congreso Nacionalde Honduras. (1982). Constitucion de la República de Honduras, Decreto No. 131.

RAE. (2024). Diccionario Panhispanico del Español Juridico. https://dpej.rae.es/lema/derecho-comparado

Durango, J. (2024). GoLegal: Privacidad y Proteccion de Datos. https://golegalcr.com/proteccion-de-datos-personales-en-costa-rica/

García-Gonzalez, A. (2007). La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado. Boletín Mexicano de Derecho Comparado, 40(120), 743-778. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332007000300003&lng=es&nrm=iso

Cortes Generales. (29 de diciembre de 1978). Constitución Española.

Gomez Sanchez, M. (2020). La Protección de Datos Personales en México: Cambios Evolutivos a 10 años de su Inclusión a Nivel Constitucional. Revista Mexicana de Ciencias Penales(10), 48-58.

Grupo Atico. (2023). Ciberseguridad: Grupo Atico 34. https://protecciondatos-lopd.com/empresas/casos-privacidad-digital/

Hernández-Estevez, S., & Lopez-Durán, R. (2002). Técnicas de investigación jurídica. México: Oxfor University Press.

Hidayatulloh, H. (2023). Human rights and data protection in the digital financial ecosystem. Jurnal Hukum Replik. https://doi.org/10.31000/jhr.v11i1.8110

Congreso Nacional de Honduras, (1982). Decreto 131-82. Constitución de la República de Honduras [Const.].

Instituto de Acceso a la Información Pública. (2018). Proyecto de Ley de Protección de Datos Personales.

Instituto de Investigaciones Juridicas de la UNAM. (2010). https://archivos.juridicas.unam.mx/www/bjv/libros/6/2792/6.pdf

La Asamblea Legislativa de la República de Costa Rica. Ley n.º 8968. (2011). Ley De Protección De La Persona Frente Al Tratamiento De Sus Datos Personales.

Mancera Cota, A. (2008). Consideraciones durante el proceso comparativo. Boletin Mexicano de Derecho Comparado , 213-243.

Newsroom Infobae. (2 de febrero de 2024). infobae.com. https://www.infobae.com/america/agencias/2024/02/02/claro-sufre-un-incidente-de-ransomware-que-afecta-su-servicio-celular-en-centroamerica/

Osorio, J. (2024). @danojbt. https://twitter.com/danojbt/status/1753462301863125106?-t=AEKJV65nBKbOtm6DE3ebzQ&s=08

Parlamento Europeo y Consejo de la Unión Europea. (2016). Reglamento (UE) 2016/6795 Del Parlamento Europeo y fel Consejo, RGDP. Diario Oficial de la Unión Europea. https://doi.org/https://eu.vlex.com/vid/regulation-eu-2016-679-843418428?from_fbt=1&forw=go&fbt=webapp_preview&addon_version=6.8

Perez, M. J. (2016). Davos y la cuarta revolución industrial. Nueva Revista. https://doi.org/https://www.nuevarevista.net/davos-y-la-cuarta-revolucion-industrial/

Ramos Peña, L. A. (2011). La Interpretacion y Aplicacion del Derecho. Importancia de la Argumentacion Juridica en un Estado de Derecho. Revista del Instituto de Investigaciones Juridicas de la UNAM, 121-135.

Tonon, G. (2011). La Utilizacion del Metodo Comparativo en Estudios Cualitativos en Ciencia Politica y Ciencias Sociales: diseño y desarrollo de una tesis doctoral. KAIROS. Revista de Temas Sociales, 1-12.

Universidad Nacional Autónoma de México, UNAM. (22 de Enero de 2010). Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas. https://archivos.juridicas.unam.mx/www/bjv/libros/6/2792/6.pdf

Visar, S. (2023). Human rights in the technology era – Protection of data rights. European Journal of Economics, Law and Social Sciences. https://doi.org/10.2478/ejels-2023-000