**CENTRO UNIVERSITARIO TECNOLÓGICO**

**FACULTAD DE CIENCIAS ADMINISTRATIVAS Y SOCIALES**

**INFORME DE PROYECTO DE GRADUACIÓN**

# EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES POR PARTE DE ENTIDADES PRIVADAS COMERCIALES EN HONDURAS

**SUSTENTADO POR:**

**JESSY MARÍA FLORES LÓPEZ**

**11511351**

**SUPERVISOR**

**ABOG. ALEJANDRA SUAREZ FORTIN**

**TEGUCIGALPA M.D.C.** **HONDURAS, C.A.**

**MAYO, 2021**

**CENTRO UNIVERSITARIO TECNOLÓGICO**

**CEUTEC DE UNITEC**

**FACULTAD DE CIENCIAS ADMINISTRATIVAS Y SOCIALES**

**AUTORIDADES UNIVERSITARIAS**

**RECTOR**

**MARLON BREVE REYES**

**SECRETARIO GENERAL**

**ROGER MARTÍNEZ MIRALDA**

**VICERRECTOR ACADÉMICO**

**DINA ELIZABETH VENTURA**

**DIRECTORA ACADÉMICA**

**IRIS GABRIELA GONZALES**

**JEFE DE CARRERA**

**CARLOS PECORRELLI**

# Agradecimiento

Quiero agradecer a Dios, por guiarme en el camino y fortalecerme espiritualmente para continuar una ruta llena de éxito.

Quiero mostrar mi gratitud a todas aquellas personas que estuvieron presentes a lo largo de mi vida como estudiante, gracias por todas sus ayudas, sus palabras motivadoras, sus conocimientos, sus consejos y su dedicación.

A mis docentes, muchas gracias por compartir sus conocimientos y experiencias profesionales. Gracias por la paciencia, dedicación, tiempo y entusiasmo invertido en cada lección dentro del aula de clases.

Agradezco con mucha estima a mis amigos y compañeros, quienes me motivaron siempre a sumar un logro más en mi carrera profesional y con los que compartí muchas experiencias.  A mis compañeros de la Dirección General de Imagen País por brindarme su apoyo incondicional, motivación y la oportunidad de poder comenzar y desarrollar mi carrera profesional mientras profundizaba mi amor por nuestro hermoso país.

Por último, quiero agradecer al pilar fundamental de mi vida, a mi familia. Especialmente, a mi madre, cuyo apoyo incondicional me ha impulsado durante todo este recorrido, quien con su ejemplo me motivó a emprender esta segunda carrera. A mi hermano, por ser siempre mi admirador incondicional. Finalmente, a mi padre, por sus consejos que me han ayudado desenvolverme profesional y académicamente.

Gracias a todos por su paciencia y comprensión, y sobre todo por su amor.

¡Muchas gracias por todo!

# Tabla de Contenido

## Índice De Tablas

## Índice De Figuras

# Resumen Ejecutivo

La globalización y el desarrollo tecnológico han resaltado la importancia de los datos personales y necesidad de desarrollar marcos jurídicos eficientes que garanticen el Derecho a la Protección de Datos Personales para evitar riesgos como la comercialización de bases de datos, especialmente por parte de entes comerciales privados. Honduras reconoce el derecho a la intimidad personal y a la inviolabilidad de las comunicaciones, pero no cuenta con una regulación sectorial que garantice la protección de datos personales. En esta investigación se utilizaron las metodologías de encuestas, revisión documental, derecho comparado y entrevistas a expertos para determinar el mecanismo ideal para proteger los datos personales de la comercialización ilegal de bases de datos y la subsecuente deducción de responsabilidad a los entes comerciales privados que quebranten dicha protección. Los datos recolectados muestran la vulnerabilidad a la que se exponen los usuarios hondureños respecto a la protección de sus datos personales, evidenciando así, la necesidad de una regulación jurídica eficiente y eficaz sobre el tema.

*Palabras clave:* Protección de Datos Personales, Honduras, Comercialización, Bases de Datos, Entes comerciales privados, Datos, Tecnología, Usuarios.

# Abstract

Globalization and technological development have highlighted the importance of personal data and the need to develop efficient legal frameworks that guarantee the Right to Personal Data Protection to avoid risks such as the commercialization of databases, especially by private commercial entities. Honduras recognizes the right to personal privacy and the inviolability of communications but does not count with a specific regulation that guarantees personal data protection. This research used the different methodologies of surveys, documentary review, comparative law, and interviews with experts to determine the ideal mechanism to protect personal data from the illegal commercialization of databases and the subsequent deduction of responsibility to private commercial entities that violate this protection. The data collected shows the vulnerability to which Honduran users are exposed with respect to the protection of their personal data, thus evidencing the need for an efficient and effective legal regulation on the subject.

*Keywords:* Protection of Personal Data, Honduras, Marketing, Databases, Private commercial entities, Data, Technology, Users.

# Introducción

Esta investigación aborda el tema de la protección de datos personales de la comercialización ilegal de bases de datos y la subsecuente deducción de responsabilidad a los entes comerciales privados que quebranten dicha protección en Honduras.

La Constitución de la República de Honduras reconoce a través de varias disposiciones, el Derecho a la Protección de Datos Personales. Sin embargo, la globalización y el desarrollo tecnológico han facilitado a entes comerciales privados el acceso a datos personales de los hondureños, poniendo en riesgo el derecho de acceso de los usuarios si se comercializan ilegalmente las bases de datos personales.

Esta investigación pretende analizar la situación jurídica actual de Honduras respecto a la protección de datos personales para evitar la comercialización ilegal de bases de datos para proponer el mecanismo ideal de protección de datos personales.

El objetivo general de la investigación es proponer un mecanismo legal de protección de datos personales para evitar la comercialización ilegal de bases de datos y determinar la subsecuente deducción de responsabilidad a los entes comerciales privados que quebranten dicha protección a través del estudio y análisis del marco jurídico hondureño, contratos y proyectos de ley para garantizar la privacidad e intimidad de los usuarios.

Para dar respuesta a las preguntas de investigación, esta investigación desarrolló una metodología de encuestas, revisión documental, derecho comparado y entrevistas no estructuradas a expertos. Se determinó la perspectiva de la población al respecto, la normativa hondureña vigente, la eficacia de esta y aciertos y sugerencias para el

Anteproyecto de Ley de Protección de Datos Personales y Acción de Hábeas Data, que al momento no ha sido aprobada por el Congreso Nacional de la República.

Los resultados muestran que cada vez son más los usuarios hondureños que proporcionan libremente sus datos personales a entes comerciales privados, teniendo estos, un enorme valor como parte de bases de datos. Muchos consideran que sus datos personales han sido cedidos sin su consentimiento por entes comerciales privados. Esta situación se relaciona con la escasa regulación jurídica nacional sobre la protección de datos personales en entes comerciales privados, la cual se limita constitucionalmente al derecho fundamental a la intimidad y a la inviolabilidad de las comunicaciones, y la garantía del Habeas Data.

Adicionalmente, la normativa jurídica vigente hondureña incluye Tratados Internacionales, la Ley sobre Justicia Constitucional que desarrolla el Habeas Data como medida de protección y el Código Penal que regula la responsabilidad penal de quien comercializa ilegalmente bases de datos. A la luz de los estándares del Reglamente General de Protección de Datos europeo, la normativa hondureña resulta ineficaz para garantizar una cesión legítima por parte de los entes comerciales privados. Lo anterior evidencia la necesidad de contar con una regulación sectorial sobre protección de datos personales en Honduras.

Finalmente, como resultado de la validación y el trabajo de campo realizado en esta investigación, se realiza una propuesta de innovación para fortalecer el contenido del Anteproyecto de Ley de Protección de Datos Personales y Acción de Hábeas Data.

# CAPÍTULO I

# 1. PLANTEAMIENTO DEL PROBLEMA

## 1.1 Descripción de la Realidad Problemática

La coyuntura actual causada por la pandemia de la Covid-19 y las medidas de aislamiento ha causado que la digitalización y el comercio electrónico se vuelvan una herramienta y práctica indispensable para las empresas, el gobierno y los consumidores/ usuarios. Castellanos et al. (2020) consideran que esta nueva realidad obliga a revisar las herramientas digitales para determinar si "cumplen con lo que la regulación de cada país establece al respecto, especialmente en temas de protección al consumidor, así como para definir lo relativo a la responsabilidad, en caso de incumplimiento de algunas de las partes".

Los entes privados que se dedican al comercio se encuentran recolectando una gran cantidad de datos personales de los usuarios, dejando a su discreción el uso que estos reciben. Gracias al internet y al comercio electrónico, "disponemos de un volumen creciente de información y de múltiples sensores conectados capaces de generalas. Además, poseemos la capacidad de almacenarla y la condiciones para procesarla a una velocidad razonable" (Martínez, 2017, p. 153).

Estas tendencias y facilidades traen a discusión el nivel de protección que se da a los datos personales de los usuarios del comercio electrónico. Muchas legislaciones relacionan los datos personales con los derechos al honor, privacidad e intimidad, protegiéndolo con la garantía de hábeas data y hasta considerándolo un derecho fundamental (Richter, 2015, p. 18):

> La protección de datos de carácter personal representa el reconocimiento de un derecho humano que se desarrolla a partir de la evolución de la tecnología. La dignidad del individuo, al igual que su intimidad y su honor deben ser resguardados de los usos indebidos que pueden hacer de los datos de carácter personal que se encuentran en bancos de datos, tanto de carácter público como privado.

En el caso de Honduras, la Constitución garantiza el derecho a la intimidad personal e inviolabilidad de las comunicaciones y se cuenta con una garantía que lo protege, el Hábeas Data. Aunque ha habido esfuerzos de proyectos de ley, Tomé (2019) considera que la legislación actual en Honduras es limitada ya que no cuenta con una ley vigente que regule especialmente la protección de datos como sucede en otros países (p.3 y 5).

Los ciudadanos tienen derecho a poder controlar su información personal, sobre su uso, destino y a impedir su tráfico ilícito y lesivo para su dignidad y derechos. La desprotección de legal de los datos personales expone a los usuarios a perjuicios físicos, económicos, sociales, materiales e inmateriales (Kluwer, 2018).

El comercio electrónico se presentó como la alternativa ideal para continuar la actividad económica y sobrevivir la crisis de la Covid-19, demostrando así la rescilencia del sector, pero no de la legislación hondureña. Las nuevas tendencias comerciales exigen una legislación adecuada que garantice la seguridad jurídica de los usuarios.

## 1.2 Formulación del Problema

### *1.2.1 Problema general*

La actual facilidad con que los entes comerciales privados están recolectando datos personales a través de medios digitales ha proliferado la venta o comercialización de las bases de datos recolectadas. Esta información puede ser comercializada para fines publicitarios, de ventas, políticos y hasta delictivos. Si no hay consentimiento del titular, este se considera un desvío de los propósitos originales del tratamiento (Fernández de Heredia, 2018), siendo un uso abusivo o discrecional de los datos personales ajenos que puede infringir el derecho a la privacidad e imagen personal.

La ausencia de una normativa específica que regule la protección de datos personales y la proliferación de ventas de bases de datos por parte de entes comerciales privados hace considerar, ¿mediante qué mecanismo legal se podrían proteger los datos personales de la comercialización ilegal de bases de datos y la subsecuente deducción de responsabilidad a los entes comerciales privados que quebrante dicha protección?

### *1.2.2 Preguntas de Investigación*

A. ¿Considera la población hondureña que su información personal se encuentra en riesgo de ser comercializada ilegalmente por entes privadas?
B. ¿De qué manera la legislación actual regula la responsabilidad de los entes comerciales privados con relación a la comercialización ilegal de bases de datos?
C. ¿Es el marco jurídico actual eficaz en regular la protección de datos personales para la comercialización ilegal de bases de datos por entes comerciales privados o precisa una mayor regulación?

D. ¿Qué aciertos y vacíos tiene el Anteproyecto de Ley de Protección de Datos Personales (2014) con relación a su aplicabilidad en la actualidad para evitar la comercialización ilegal de datos por entes comerciales privados?

## 1.3 Objetivos de la Investigación

### *1.3.1 General*

Proponer un mecanismo legal de protección de datos personales de la comercialización ilegal de bases de datos y la subsecuente deducción de responsabilidad a los entes comerciales privados que quebranten dicha protección a través del estudio y análisis del marco jurídico hondureño, contratos y proyectos de ley para garantizar la privacidad e intimidad de los usuarios.

### *1.3.2 Específicos*

A. Evaluar la percepción de la población hondureña sobre la protección de su información personal frente a la comercialización ilegal de sus datos por entes comerciales privados.
B. Describir la manera en que el marco jurídico hondureño vigente regula la responsabilidad de los entes comerciales privados frente a la comercialización de bases de datos personales.
C. Determinar la eficacia del marco jurídico hondureño actual que regula la protección de datos personales para evitar que entes comerciales privados comercialicen ilegalmente bases de datos a fin de establecer si precisa una regulación especial.

D. Examinar aciertos y vacíos del Anteproyecto de Ley para la Protección de Datos Personales (2014) con relación a su aplicabilidad en la actualidad para evitar la comercialización ilegal de bases de datos por parte de entes comerciales privados.

### 1.4 Justificación de la Investigación

Como resultado del aumento de la actividad comercial a través de medios digitales, los entes comerciales privados se encuentran recibiendo una gran cantidad de datos considerados personales de sus usuarios y estas plataformas son cada vez más eficientes en recolectar, analizar y utilizarla El usuario tiende a entregar su información sin saber cómo y para que fines será utilizada. Usualmente esta información se recopila por medio de los sitios web o aplicaciones que utilizan contratos de adhesión con formularios prediseñados por el proveedor para solicitar información personal del usuario (Mok, 2010, p. 118). Pero también se recolecta información a través de los sistemas de pago y hasta con el simple hecho de entrar en un sitio, este ya capta ciertos datos.

A pesar de las facilidades de esta modalidad, la digitalización, el desarrollo del internet y del comercio electrónico representan una amenaza para la privacidad e intimidad de los consumidores. En Honduras, el derecho fundamental a la protección de datos personales esta regulados por la misma constitución, incluso cuenta con una garantía especial que es la acción de Hábeas Data, pero su protección se dificulta en los medios digitales e internet, asegura Tomé (2019, p. 3).

El manejo de datos personales por parte de entes comerciales privados involucra una gran variedad de riesgos y perjuicios físicos, económicos, sociales, materiales e inmateriales

de los usuarios, por ejemplo, discriminación, usurpación de identidad, fraude, pérdidas financieras, daños a la reputación, pérdida de la confidencialidad de datos sujetos al secreto profesional, comercialización no autorizada y hasta destrucción, pérdida o alteración de estos (Kluwer, 2018). Por lo tanto, también implica una gran responsabilidad para estos entes.

González (2017) indica que "las bases de datos, sean propias o no, solo pueden utilizarse para aquellas finalidades derivadas de la prestación de servicios concretos que determina la relación entre empresa y cliente". De ahí que la comercialización no autorizada de las bases de datos recolectadas por entes comerciales privados en el comercio electrónico representa un abuso a su privacidad e intimidad, especialmente si estos no han dado su consentimiento para esos fines.

Aunque la legalidad de esta práctica depende de la legislación de cada país, si esta se realiza sin el consentimiento o conocimiento de los usuarios evidencia el mal uso que los entes comerciales privados dan a los datos personales ajenos que recolectan (Mailrelay: Email Marketing, 2018). Teniendo en cuenta que esto podría llevar a consecuencias más graves como pérdidas patrimoniales para la empresa o lesiones a la dignidad y privacidad del usuario.

En Honduras existen normativas que protegen en cierto grado los datos personales, pero existe una regulación específica que regule el uso de los datos personales en el comercio electrónico para evitar que los entes comerciales privados comercialicen ilegalmente estas bases de datos. Si hubo un Anteproyecto de Ley para la protección de datos personales (2014) que no fue aprobado y quedó en el olvido (Tomé, 2019, p. 5).

Es necesario garantizar la protección a los consumidores mediante un marco jurídico claro que se adapte al contexto institucional, legal, social y económico del país (Arroyo & Sierra Castro, 2019), que indique el tratamiento que se le debe dar a los datos personales que se recopilan a través de las transacciones comerciales electrónicas y la responsabilidad en que incurren los entes comerciales privados respecto al manejo de esta delicada información.

Por esta razón, resulta imperativo determinar la actual responsabilidad que tienen los entes comerciales privados frente a la venta de bases de datos según la legislación y sus contratos para determinar si es adecuada la protección que están recibiendo los datos personales de los consumidores. Asimismo, considerando que el anteproyecto de ley para la protección de datos personales (2014) no ha sido aprobado, también resulta beneficioso analizar sus regulaciones para concluir la posible necesidad y beneficio de su implementación.

### 1.5 Limitaciones de la Investigación

Para la presente investigación se ha identificado limitaciones propias de la pandemia de la Covid-19 y medidas de confinamiento. Como resultado de estas, se dificulta el acceso a información física en instituciones privadas y públicas hondureñas que por motivos sanitarios están restringiendo el acceso a sus instalaciones. Asimismo, estas dificultan las visitas presenciales y entrevistas físicas con expertos y técnicos.

A pesar de la enorme disponibilidad de información en el internet, se debe considerar que Honduras está apenas empezando a digitalizar sus sectores, por lo que no cuenta con una gran cantidad de portales de datos oficiales. Además, muchos de los portales que si están

funcionando no se pueden considerar como una fuente veraz y confiable al no estar siendo actualizados constantemente.

Luego, se debe tomar en cuenta que este es un fenómeno jurídico relativamente nuevo que específicamente en Honduras no ha sido lo suficientemente estudiado y al cual aún no se le ha dado la importancia que merece, evidenciado por la ausencia de una legislación específica y por la renuencia a discutir y aprobar su proyecto de ley.

Finalmente, vale la pena mencionar la limitante que representa el tiempo para esta investigación. Siendo que el tiempo total para su realización es de aproximadamente seis meses y durante un periodo nacional excepcional de crisis sanitaria, económica, humanitaria y política.

# CAPÍTULO II

# 2. MARCO TEÓRICO

## 1.1 Antecedentes Históricos

El Derecho a la Protección de Datos Personales es un derecho relativamente nuevo que ha ido evolucionando de manera heterogénea a través del tiempo partiendo de los derechos al honor, intimidad, privacidad, vida privada y dignidad humana. Su reconocimiento y protección ha tenido múltiples cambios para adaptarse a la coyuntura social, tecnológica, política e ideológica de cada sociedad.

Desde la Antigüedad se han venido recogiendo y manejando datos de las personas. Es menester mencionar que, desde el derecho romano, existió una clara protección jurídica al honor, como aspecto personal de la persona (Huerta, 2017, pp. 57–58).

Sin embargo, apenas si ha existido durante siglos ninguna norma jurídica que restringiera el tratamiento de la manera que se entiende hoy en día. Huerta (2017) explica que, durante la Antigüedad, no "existían grandes tratamientos masivos de datos personales dignos de este nombre. Ni se realizaban censos periódicos que comprendieran el conjunto de la población, ni existían ficheros hoy habituales" (p. 63), evidenciando la falta de necesidad de este derecho durante esta época.

La mayoría de los autores (Rodríguez, 2015, pp. 59–60), coinciden en que el verdadero punto de partida para la construcción del Derecho a la Protección de Datos

Personales se da entre un paralelismo del procesos vivido en Estados Unidos con la *privacy* y el Desarrollo Constitucional Alemán .

### *1.1.1 "The right to privacy" en Estados Unidos*

El origen del Derecho a la Protección de Datos Personales está relacionado con el término privacidad, que apareció por primera vez en 1890 en Estados Unidos con el famoso artículo "*The right to privacy*" o El derecho a la privacidad de Samuel D. Warren y Luois D. Brandeis, explica López- Torres (2014, p. 104).

Ruíz (2016) detalla que el famoso artículo hace un pronunciamiento sobre los cambios sociales, económicos y políticos que se están sufriendo en esa época, exigiendo el reconocimiento a la privacidad y a la protección personal. *The right to privacy* buscaba establecer límites jurídicos a la intromisión del periodismo luego de la realización de censos intrusivos (p.6).

Sin embargo, la privacidad que Warren y Brandeis exigían, se entendía como "*The right to be let alone*" o el derecho a ser dejado solo, que Frosini (1982, citado por Rodríguez, 2015) explica como:

> 'El derecho a gozar la vida, o sea el derecho a estar solo', frente a los ataques, amenazas, asfixia producida por las interferencias de la vida priva o en la esfera íntima ante una sociedad 'sometida al control de los medios de comunicación de masa'. (p.50).

El pronunciamiento llevó a discusión el derecho a la privacidad, logrando que "la mayoría de las cortes de Estados Unidos lo reconocieron, al grado de que la Suprema Corte

de dicho país lo consideró como derecho con protección constitucional" (López-Torres, 2014, p. 105).

### *1.1.2 Tribunal Federal alemán*

Por otro lado, Rodríguez (2015) fija la incorporación del Derecho a la Protección de Datos Personales al derecho europeo con el caso alemán y el establecimiento del "*informationelle Selbsbestimmungsrecht*" o derecho a la autodeterminación informativa. Esta construcción viene del pronunciamiento del Tribunal Constitucional Alemán sobre la constitucionalidad del Censo de la población de Alemania declarado por el *Bundestag* en marzo de 1982 (p. 56).

Los acontecimientos de la época en el país germano donde proliferaba un temor y desconfianza ante la evolución tecnológica y la iniciativa de una operación censal gigantesca que exigía información personal exhaustiva de los ciudadanos motivaron en 1983, la presentación del recurso de amparo constitucional contra la Ley del Censo, determinando que este violentaba los derechos a la personalidad, dignidad, libertad de expresión y garantías constitucionales (Rodríguez, 2015, pp. 56–58).

El Tribunal Alemán no solo admite el recurso, sino que dicta una medida cautelar de suspensión provisional de la ley, dictando sentencia en diciembre de 1983 donde acoge gran parte de la argumentación y anula parcialmente la ley. La sentencia plantea el derecho a la autodeterminación informativa como derecho vinculado a la personalidad (Rodríguez, 2015, p. 57)

Aunque realmente se habla del origen de la protección de datos personales en la Constitución Alemana de Weimar de 1919, donde se introdujo el concepto de datos personales de manera restringida al suscribirlo, únicamente, a los funcionarios públicos (Ruiz, 2016, p. 6).

### *1.1.3 Primeras regulaciones*

Es claro que Derecho a la Protección de Datos Personales es una tendencia relativamente nueva que tiene su origen de un doble proceso de transformación social y jurídica. Por una parte, la actual creciente utilización de tecnologías informáticas y digitales por parte del Estado, el sector privado y de la misma población para capturar, procesar y transmitir información. Lo anterior ha llevado a alertar respecto al impacto de estas herramientas en la protección de los derechos fundamentales, llevando a la doctrina y jurisprudencia a identificar una respuesta jurídica para controlar y legitimar el tratamiento de datos personales; de manera que, se lograra permitir el flujo de información mientras se garantiza la no afectación a los derechos fundamentales de las personas (Álvarez, 2020, p. 2).

> Gracias a los antecedentes anteriores, el nuevo derecho a la protección de datos de carácter personal se va perfilando de forma distinta en los diversos países, ante su expresión o ausencia en las diversas constituciones o su nacimiento por la vía judicial. De hecho, no es sino hasta la década de los años setenta cuando se produce una innovación en la historia de la legislación tanto europea como norteamericana, respecto a las personas y el tratamiento automatizado de datos de carácter personal a través del ‘proceso de positivación de los derechos integrantes de la tercera

> generación, en particular de la libertad informática o derecho a la autodeterminación informativa. (Rodríguez, 2015, p. 60).

De esta manera, la génesis de la legislación sobre datos personales moderna se remonta a 1970 con la primera ley de protección de datos en el mundo, la del Estado de Hesse en Alemania. Esta fue seguida por las leyes nacionales en Suecia (1973), Alemania (1977) y Francia (1978) (López-Torres, 2014, p. 112), llegando a tener Europa, una normativa comunitaria que reconoce y regula este derecho.

Vale la pena resaltar, que en el caso de América Latina, el desarrollo de la protección de datos personales ha sido distinta, ya que según Rodríguez (2015), "se ha asumido desde la figura del Hábeas Data, bajo una riqueza garantista que ha planteado un avance netamente procesal, lo cual (…), ha retrasado el florecimiento del nuevo derecho fundamental a la protección de datos de carácter personal" (p.85).

### 2.2 Datos Personales

Por su parte, la evolución constante de la protección de datos ha sido impulsada por los avances tecnológicos y la necesidad de proteger a la ciudadanía de estos. El desarrollo y aumento de uso de tecnologías despierta temores ya que "a través de las posibilidades de recopilación y almacenamiento de datos (…), es posible intervenir en la vida privada de cualquier persona, particularmente si para esta dicha injerencia pasa desapercibida" (Castro, 2015, p. 760).

En esta coyuntura, los datos personales se han vuelto “el nuevo petróleo de la internet y la nueva moneda del mundo digital” (Remolina-Angarita, 2010, citado en Vera & Vivero, 2019, p. 235).

De ahí, que varios autores (Vera & Vivero, 2019, p. 239) consideren necesario precisar que el vocablo dato viene del latín *datum* y se refiere a un antecedente necesario para un conocimiento exacto de una cosa o para deducir consecuencias legítimas sobre un hecho. Las personas se han vuelto esta “cosa” respecto a la cual las empresas recopilan y registran datos.

### *2.2.1 Concepto de Datos Personales*

La legislación europea actual considera que los datos de carácter personal se refieren a “cualquier información concerniente a personas físicas identificables o identificables” (Gil, 2015, p. 32).

Algunos datos que se consideran personales son el nombre y apellido, hay muchísimos más como por ejemplo los números de teléfono, datos de voz, condiciones y registros de trabajo, número de seguridad social, dirección, económicos, así como también perfiles en redes sociales, likes es Facebook, adn, forma de caminar, datos biométricos, ubicación, imágenes, respuestas en exámenes, anotaciones del examinador, etc. (Polo, 2020, pp. 108–109).

A su vez, también se habla una categoría particular, los datos especialmente protegidos. Gil (2015, pp. 45–46) enfatiza que estos datos son más delicados en el sentido de que de divulgarse indebidamente, pueden afectar lo más íntimo de una persona, por lo que

requieren un tratamiento y regulación especial. Algunos ejemplos son la ideología, afiliación política, sindical, religiosa, creencias, origen racial, salud y orientación sexual.

#### 2.2.1.1 Características de los Datos Personales.

##### *2.2.1.1.1 Cualquier información.*

La doctrina hace referencia a ciertas características principales de los datos personales: Primer indica que puede ser cualquier información, indicando un concepto amplio que puede referirse a información objetiva e incluso subjetiva, ni siquiera se vuelve necesario que la información sea verídica o que esté probada, previendo la posibilidad de corrección (Gil, 2015, pp. 46- 47).

##### *2.2.1.1.2 Persona identificada o identificable.*

La segunda característica es que se refiere a una persona identificada o identificable, respecto a lo cual, Polo (2020) considera:

> Que la información hace referencia a una persona identificada cuando esa información indica directamente a esa persona sin necesidad de utilizar un conjunto de medios para averiguar su identidad (DNI, pasaporte, etc.). En cambio, consideramos que una persona es identificable cuando su identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. (p. 180).

Esto quiere decir, que para que para que se considere que la persona es identificable cuando, aunque no indique a la persona, es suficiente para poder averiguarlo o relacionarla.

#### 2.1.1.2 Clasificación de los Datos Personales.

Asimismo, en la doctrina se puede encontrar una doble clasificación de los datos personales. Como lo hace notar Ruiz (2016), la primera clasificación alude al derecho a la intimidad, dividiendo la información en personal e impersonal. La información impersonal es la que no está limitada constitucionalmente, específicamente por razones de publicidad, transparencia y eficiencia de la administración pública, mientras que la personal se relaciona directamente con la intimidad, buen nombre y Hábeas Data (pp. 24-15).

La segunda clasificación propuesta por el autor (Ruiz, 2016, pp. 25–29) tiene un enfoque cualitativo y según su grado de difusión, es decir, una perspectiva de identificar quien puede recolectar, tratar y acceder a esta información. La divide en datos públicos que son los residuales; datos privados como aquellos a los que no es lícito acceder sin consentimiento; datos semi privados de los cuales los administradores de un registro se reservan la información a que tienen un uso exclusivo; y los datos sensibles, aquellos que pueden lesionar la dignidad de la persona por su alto potencial de trato marginal o discriminatorio.

### *2.1.2 Concepto de Protección de Datos Personales*

El desarrollo tecnológico y especialmente en la información ha facilitado la conformación de grandes bancos y bases de datos públicos y privados, lo cual implica riesgos propios de este desarrollo. Vera y Vivero (2019) deducen que esta era tecnológica no solo implica que la información se ha vuelto fuente de negocio y comercio, sino también criminalidad, sosteniendo que el verdadero peligro no viene de la recopilación, sino de del manejo abusivo y la falta de capacidad de disposición de la persona (pp. 242 y 249).

Entre los peligros de la informática en la doctrina jurídica, Huerta (2017) señala: la acumulación de datos, la fácil transmisión a terceros, la reutilización ilimitada de los datos, la falta de calidad de datos, la falta de adecuadas medidas de seguridad, la pérdida de control del sujeto sobre la información, la elaboración de perfiles sobre las personas, el uso ilícito de la información por el poder político, la vigilancia y control social y la acumulación excesiva y exceso de poder (pp. 214- 221).

En la opinión de López-Torres (2014, p. 104), el desarrollo tecnológico es importante para el bienestar de los países, pero este no debe ser lesivo para sus habitantes.

La organización internacional sin fines de lucro, Access Now, define protección de datos como "las prácticas, salvaguardas y principios fundamentales puestos en ejercicio para proteger la información personal y asegurar que el usuario mantenga el control de ella" (LatinAlliance, 2020, p. 2).

Desde un enfoque jurídico, Enriquez (2017) define la protección de datos personales como "un mecanismo jurídico para proteger el derecho a la vida privada" (p.27).

Empleando las palabras de Maqueo et al. (2017),

> La base para garantizar una protección adecuada que se materialice en el control que la persona pueda tener sobre el tratamiento de sus datos personales, se constituye mediante unos criterios de legitimación, los principios de la protección de datos, la posibilidad de ejercer derechos por parte del titular de los datos y la supervisión, misma que puede concretarse en la tutela de la persona a la que se refieren los datos personales que son objeto del tratamiento, así como la atribución y el ejercicio de

> potestades de investigación y sanción por parte de una autoridad de control independiente. (p.92).

Lo anterior, sirve de base para determinar el grado de protección a los datos personales en un país determinado, siendo estos criterios relativamente generales.

## 2.3 Derecho a la Protección de Datos Personales

Desde la aparición de la informática, el flujo de información ha producido un progreso exponencial, pero al mismo tiempo se vuele una amenaza cuando esa información se puede clasificar y ordenar. Como una respuesta jurídica a los problemas que puede causar este desarrollo aparece el Derecho a la Protección de Datos Personales (Travieso, 2016, pp. 110–111).

### *2.3.1 Concepto y precisión del término*

Gil (2015) refiera al concepto brindado por la corte europea, que define este derecho como:

> Un poder de disposición y control sobre los datos personales que faculta a la persona para decidir cuáles de estos datos proporcionar a un tercero, sea el Estado o un particular, o cuales puede este tercero recabar, permitiendo también al individuo saber quien posee esos datos personales y para qué, pudiendo oponerse a esa posesión o su uso. (pp. 48- 49).

Este es un concepto lo suficientemente amplio para aclarar los sujetos, ámbitos y alcances que logra este derecho. Se debe enfatizar que el mismo implica un poder sobre los

datos personales propios, sobre su posesión y uso por parte de terceros, ya sea entidades públicas o privadas.

Otro concepto proveniente de las guías jurídicas europeas lo define como un poder de control y disposición, atribuyéndole un contenido esencial (consentimiento, finalidad, uso, seguimiento en la recogida y en su utilización: corrección, cancelación, actualización), además de brindarle las garantías necesarias, refiriéndose al Hábeas Data (Rodríguez, 2015, p. 77).

En la doctrina se encuentra una variedad de términos que hacen referencia a este derecho, como ser Derecho a la autodeterminación informativa, a la libertad informática o derecho a la protección de carácter personal.

#### 2.3.1.1 Tesis del derecho a la autodeterminación informativa.

De acuerdo con Polo (2020), la doctrina sugiere utilizar el término "Derecho a la Autodeterminación Informativa", ya que este es un término más amplio y completo que mezcla la protección de datos y la libertad informática. Este término se enmarca en la corriente germana ya que implica tener control y disposición absoluta sobre los datos, siendo más que la mera privacidad de la corriente anglosajona.

En contraste, Rodríguez (2015) considera que este término alude a un derecho subjetivo, es decir a la mera facultad de decidir sobre la información propia, lo cual forma parte del contenido esencial del derecho a la protección de datos personales y el consentimiento (p. 81).

#### 2.3.1.2 Tesis del derecho a la libertad informática.

Al respecto, se plantea que comprende hasta la propia autodeterminación informativa, atendiendo a la libertad y a la informática, por lo que este término permite la protección de la libertad frente a la tecnología, como lo hace el término de protección de datos personales (Rodríguez, 2015, p. 82) .

#### 2.3.1.3 Tesis del derecho a la protección de datos personales.

Este es el término que más se ha utilizado en Europa y que en palabras de Rodríguez (2015):

> Este se concibe como un verdadero poder de disposición y control sobre los datos personales, a través del cual se faculta a las personas para decidir cuales datos proporciona y proporcionará o cuales puedes recabar el tercero, cuya facultad no se agota allí mismo, sino que se extiende al destino y uso que se le dará a los datos personales y ante ello solicitar su cancelación, rectificación o modificación. De modo que, se protege realmente a los sujetos como portadores físicos y por ende al dato como elemento objetivo, pues el interés es que este último se pueda mantener al día, bajo resguardo, seguridad y protección -que no se modifique-, entendiendo con ello que el fin real es la protección de las personas a través de la protección de datos. (p. 38).

Por consiguiente, siendo que es el término más amplio y generalizado se ha considerado utilizar la denominación de Derecho a la Protección de Datos Personales como

el digno a seguir en la presente investigación, haciendo énfasis en que el uso de uno u otro término no parece reclamar mayores consideraciones.

### *2.3.2 Bien jurídico protegido*

Por lo que se refiere al bien jurídico protegido por este derecho, las diferentes regulaciones se determinan de diferentes maneras, siendo que este puede referirse al derecho a la intimidad, a la privacidad, a la vida privada, a la dignidad, al honor, e incluso, las concepciones más modernas lo consideran un derecho autónomo per se, que tiene como bien jurídico protegido la misma persona a través de sus datos personales.

Rodríguez (2015) argumenta que el Derecho a la Protección de Datos Personales se distingue del honor y la propia imagen en cuanto a que la informática no representa una gran amenaza para estos (p.71). En cuanto a privacidad y vida privada, aunque hay diferencias terminológicas, estos se utilizan indistintamente en la doctrina, entendiéndose como el mismo (Maqueo et al., 2017, p. 78).

La línea entre la privacidad y la intimidad es muy fina, siendo que estos términos también se han empleado indistintamente. Sin embargo, vale la pena resaltar algunas observaciones e ideas que se han desarrollado en la doctrina. (Vera & Vivero, 2019, p. 241) Se considera que la privacidad tiene una connotación amplia basada en la autodeterminación que rechaza la intromisión no consentida en la vida privada; mientras que la intimidad se enfoca el salvaguardar ese espacio exclusivo del individuo, incluyendo la supervisión, más allá de solo ser dejado solo.

De ahí que, el mayor debate este en definir si el bien jurídico protegido es la intimidad o los mismos datos personales, para lo cual destacan dos corrientes: la estadounidense anglosajona y la germana- europea.

#### 2.3.2.1 Corriente estadounidense-anglosajona.

Por un lado, la doctrina anglosajona con origen en la privacidad enmarca el Derecho a la Protección de los Datos Personales en la tutela de la personalidad. En esta corriente, la privacidad sería el derecho fundamental y la protección de datos es la legislación y herramienta que este implementa para hacerle frente a los avances tecnológicos (Polo, 2020, p. 171).

Este modelo postula que la esencia del Derecho a la Protección de Datos Personales y el Hábeas Data es un derecho del individuo, no un derecho fundamental. De esto deriva que considera que el consentimiento no es esencial, solo es necesario que el tratamiento sea transparente (Ruiz, 2016, p. 32).

Es decir, que esta corriente doctrinal centra el Derecho a la Protección de Datos Personales en la privacidad.

#### 2.3.2.2 Corriente germana- europea.

Por el otro lado, esta corriente con origen en Alemania considera que el Derecho a la Protección de Datos Personales goza de autonomía respecto al principio americano de privacidad, creando un nuevo derecho constitucional. Aunque se considera un derecho autónomo, este no puede separarse del derecho a la intimidad ya que protege datos que

identifican a una persona, lo cual puede llegar a influir en la intimidad y vida privada (Polo, 2020, pp. 172 y 176).

Este modelo plantea que la esencia del Derecho a la Protección de Datos Personales y Hábeas Data es "que es un derecho fundamental y por lo tanto requiere el consentimiento del titular y están los derechos arco (…) que deben ser protegidos mediante unos principios, leyes y sanciones" (Ruiz, 2016, p. 32).

Todavía cabe señalar, que esta doctrina (Polo, 2020, pp. 175–176; Rodríguez, 2015, pp. 67, 71) considera que la intimidad se queda corta al ser un concepto pre informático concebido bajo una visión individual, sin considerar el ámbito social que surge de las tendencias tecnológico; volviendo necesario emplear otro término.

Es necesario aclarar que la doctrina germano- europea se entra en el control absoluto y total de la persona sobre sus datos y vida privada, pero ha tenido una dinámica evolución para llegar a este punto. Polo (2020) argumenta que la primera fase se dio cuando se consideraba este derecho como una especificación del derecho a la intimidad, la segunda cuando se le consideraba un derecho autónomo pero unido a la privacidad, y adiciona una tercera, que no se ha alcanzado, donde se supera la mera privacidad para lograr un control absoluto de los propios datos (p. 178).

### *2.3.3 Contenido esencial*

#### 2.3.3.1 Finalidad.

Lo dicho hasta aquí supone que este derecho implica un poder de disposición sobre los propios datos, siendo que la finalidad del Derecho a la Protección de Datos Personales es:

> Garantizar a la persona un poder de disposición sobre el uso y destino de sus datos con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado, garantizando a los individuos un poder de disposición sobre sus datos. (Polo, 2020, p. 177).

#### 2.3.3.2 Consentimiento.

El consentimiento se considera un concepto clave que se encuentra en forma de requisito para el tratamiento de datos. Es a través de este que se permite respetar la autonomía de los individuos (Gil, 2015, p. 61). Empleando las palabras de Polo (2020), el consentimiento en el contexto de datos personales se entiende como:

> La facultad de la libertad del individuo para decidir acerca de sus datos constituye la capacidad de autodeterminación del individuo y equivale, en el mundo de las comunicaciones, a extender la capacidad de decisión de la persona con el fin de proteger su libertad y sus derechos en el mundo tecnológico. (pp. 182- 183).

A pesar de los riesgos y la importancia del consentimiento para el tratamiento de datos, muchos usuarios siguen sin prestar atención, tal como lo demuestra un estudio español de la Organización de Consumidores y Usuarios (2018, citado en Villan, 2018), “el 88% de los usuarios brinda el consentimiento en las condiciones de uso en Internet sin leerlas. El principal motivo es el lenguaje complejo en que esta escritas para aceptar sin leer”. Este estudio muestra la responsabilidad que tienen quienes tratan los datos de garantizar que el consentimiento de los usuarios sea lo más valido posible.

#### *2.3.3.2.1 Requisitos.*

Para lograr la validez del consentimiento en el tratamiento de datos personales, la doctrina señala 4 requisitos específicos, este debe ser libre, especifico, informado e inequívoco.

Las normativas europeas (Reglamento General de Protección de Datos, 2018, citado por Polo, 2020) indican que " 'libre' se refiere a una elección y control real por parte de los interesados". De este concepto se puede entender que el consentimiento es una elección y que por lo tanto debe ser una opción real y libre de vicios como el engaño o intimidación.

Con "'especifico', se pretende garantizar un nivel de control y transparencia para el interesado, dando opción a este a elegir con respecto a cada uno de dichos fines, una garantía contra la desviación del uso" (Reglamento General de Protección de Datos, 2018, citado por Polo, 2020). De esta manera para que el conocimiento sea válido el usuario debe de saber el destino que tendrá la información y consiente solamente a lo expresamente mencionado; por lo que los terceros deben saber a priori los datos y motivos del tratamiento para garantizar que el consentimiento sea comprensible, claro y preciso, no indiscriminado (Gil, 2015, p. 66).

El requisito de 'informado' se vincula con la transparencia en el tratamiento "y exige facilitar información a los interesados antes de obtener su consentimiento (previamente informada) para que puedan tomar decisiones informadas" (Reglamento General de Protección de Datos, 2018, citado por Polo, 2020).

Al respecto, Gil (2015) deduce que esto “implica que toda la información necesaria debe suministrarse en el momento que se solicita el consentimiento, de forma clara y comprensible, y debe abarcar todas las cuestiones pertinentes” (p.63). Incluso la misma regulación europea (Reglamento General de Protección de Datos, 2018, citado por Polo, 2020) establece información mínima a proporcionar: identidad del responsable del tratamiento, fin de cada tratamiento, tipo de datos a recogerse y usarse, derecho a retirar el consentimiento, información sobre su uso en decisiones automatizadas e información sobre los riesgos.

Finalmente, el requisito de ‘inequívoco’ implica una declaración del interesado o clara acción afirmativa por parte del usuario (Reglamento General de Protección de Datos, 2018, citado por Polo, 2020).

De esta manera no puede haber duda sobre la intención del usuario en proporcionar sus datos personales. Más aún, Gil (2015, p. 64) agrega que el consentimiento debe ser una manifestación, apuntando a que debe de haber una acción y que no se puede deducir consentimiento de la falta de acción.

#### 2.3.3.3 Derechos ARCO.

Es necesario recalcar que la titularidad de los datos permanece siempre en los ciudadanos, es así que, las personas que brindan sus datos personales a terceros no dejan de ser sus titulares y “poseen derechos y garantías por sobre los que realizan el tratamiento de los datos, ante el sujeto obligado que este en posesión de los mismos” (Villan, 2018).

Estos son los derechos ARCO, que hacen referencia al Acceso, Rectificación, Cancelación y Oposición que tienen los usuarios respecto a sus datos personales.

#### *2.3.3.3.1 Derecho de Acceso.*

Primero, el derecho de **Acceso** es la facultad de poder exigir información sobre sus datos personales a quienes realizan su tratamiento. Este derecho implica determinar los fines del tratamiento, su origen y las comunicaciones realizadas o previstas (Villan, 2018).

A este también se le conoce como el derecho a ser informado sobre quien es el tratante de los datos, los registros que tiene, y su finalidad. Esto debe realizarse de manera gratuita (Ruiz, 2016, p. 21).

#### *2.3.3.3.2 Derecho de Rectificación.*

El derecho de **Rectificación** faculta al usuario a exigir al responsable de una base de datos que su información sea modificada, actualizada o rectificado en el caso que esta se inexacta, errónea o incompleta (Villan, 2018).

Este derecho también se conoce como modificación o actualización y permite aclarar e incluso agregar la información en una base de datos para garantizar que esta es verdadera y completa (Ruiz, 2016, p. 22). Para este fin, los tratantes deben poner a disposición procedimientos para la rectificación fáciles y accesibles, de esta manera se evitan errores que puedan perjudicar al dueño de los datos personales.

En este punto vale la pena relacionar la característica de que los datos personales pueden ser cualquier información, incluso si esta es errónea o no ha sido probada ya que existe este derecho de rectificación sobre la misma.

#### *2.3.3.3.3 Derecho de Cancelación.*

Luego, el derecho a la **Cancelación** faculta al individuo a solicitar la cancelación o eliminación de sus datos cuando considere que contravienen el marco normativo o que han dejado de ser necesarios para la base de datos (Villan, 2018).

Este derecho también es llamado eliminación o derecho a la caducidad del dato negativo (Ruiz, 2016, p. 23). Tiene una relación directa con el famoso "derecho al olvido" del internet.

En este derecho, Villan (2018) también menciona el fin del ciclo de vida de los datos personales, implicando que, una vez terminada la relación contractual con los tratantes, cumplido el plazo o el propósito del tratamiento, estos deben eliminar los datos de sus servidores, sistemas informáticos y servidores de terceros.

#### *2.3.3.3.4 Derecho de Oposición.*

Para terminar, el derecho de **Oposición** faculta para oponerse al tratamiento "si se hubiesen recabado sin su consentimiento o cuando existen motivos fundados para ello" (Villan, 2018).

#### 2.3.3.4 Alcance y límites.

El alcance del Derecho a la Protección de Datos Personales se proyecta en el reconocimiento del derecho a la autodeterminación informativa y en la garantía del Hábeas Data (Maqueo et al., 2017, p. 93).

Rodríguez (2015, p. 53) sostiene que este derecho "abarca la posibilidad de disponer libremente sobre la información que procesan otros y almacenan, independientemente si son particulares o la misma administración" (p. 53).

Ese control o decisión permite a la persona gozar de los derechos ARCO, por lo que el mismo autor (Rodríguez, 2015, p. 83) señala que comprende desde el consentimiento en la recolección de datos por terceros, el conocimiento y acceso -almacenamiento, tratamiento, uso y destino-, hasta la oposición, cancelación, rectificación o actualización en caso de ser afectado.

Sin embargo, esta protección encuentra sus límites en el propio derecho, en los de la misma constitución y en la legitimidad del fin y contenido esencial del derecho (Rodríguez, 2015, p. 76).

Entre estos se puede mencionar el derecho de acceso a la información pública y el periodismo, con los cuales es necesario generar un equilibrio para garantizar la transparencia y libertad de expresión. Sin embargo, se debe tomar en cuenta que ambos derechos se limitan entre sí, en tanto si (Gregorio, 2019):

> Efectivamente, si ciertos datos personales o íntimos son confiados por particulares al Estado para la toma de cisiones, el derecho de acceso no necesariamente alcanzaría

> la totalidad de esos datos, sino en la medida que esos datos son necesarios para establecer si el proceder del Estado ha sido dentro de la ley; entonces en la gran mayoría de los casos los nombres de las personas no son necesarios para realizar este control ciudadano.

En consecuencia, se vuelve imperativo lograr un equilibrio entre el acceso a la información y la protección de datos personales a través de criterios de confidencialidad y reserva.

#### 2.3.3.5 Mecanismo de protección: Hábeas Data.

El Derecho a la Protección de Datos Personales está íntimamente relacionado en el marco legal con la garantía del Hábeas Data, siendo que esta garantía protege constitucionalmente a este derecho.

En las palabras de Bazán (2009, citado en Ruiz, 2016), el Hábeas Data es una garantía constitucional donde,

> Se quiere connotar 'que se tenga, traiga, exhiba o presente el dato'. La locución 'habeas data' se forma con habeas (del latín habeo, habere), que significa tener, exhibir, tomar, traer, etc.; adosándole el vocablo data, respecto del cual existe alguna disputa léxica, pues mientras algunos afirman que se refiere al acusativo neutro plural de datan lo que se da datos -también en latín- otros sostienen que la palabra data proviene del inglés, con el significado de información o datos.

Vera y Vivero (2019) sugieren que el Hábeas Data es un mecanismo que intenta precautelar esta esfera de la intimidad de las personas frente al desarrollo de la informática.

Esta acción prevé que los titulares de datos personales puedan acceder a la justicia constitucional (p. 246).

El Hábeas Data sería complementario a una regulación previa de protección de datos personales que indique la manera de manejar y buenas prácticas en el tratamiento de datos personales. De esta manera, quienes consideren que se les ha violentado su Derecho a la Protección de Datos Personales pueden recurrir al Hábeas Data para acudir a un juez si no se les ha atendido una solicitud de acceso, rectificación, cancelación u oposición de la manera prescrita.

Como fue expuesto, el desarrollo del Derecho a la Protección de Datos Personales en América Latino ha estado ligado a la garantía del Hábeas Data, la cual fue constitucionalizándose en América Latina a partir de 1988 e Brasil, por lo que es un mecanismo relativamente nuevo en la región (Vera & Vivero, 2019, p. 247)

### 2.4 Comercialización Ilegal de Bases de Datos

La creciente informatización de los servicios públicos y privados han generado la creación de bases de datos con información personal de los usuarios. Más aún, varias empresas comenzaron a comercializar datos personales, generalmente operando dentro de un vacío legal.

Con comercialización de base de datos se hace referencia a la realización de esta práctica de manera ilegal, es decir sin el consentimiento y conocimiento del titular de los datos. Es decir, que esta práctica se está refiriendo a la compraventa o reventa a terceros sin el consentimiento del titular de los datos por parte del tratante de datos.

### *2.4.1 Cesión legal e ilegal de datos personales*

Es necesario recalcar que, para efectos legales, no toda comunicación o revelación datos personales a un tercero implica una cesión o comercialización de estos. Se debe diferenciar entre una cesión o comercialización como tal y el acceso a datos para la prestación de un servicio (Gallardo, 2018, p. 5).

"Habrá una cesión de datos si el tercero que recibe los datos puede aplicarlos a sus propias finalidades, decidiendo sobre el objeto y finalidad del tratamiento" (Gallardo, 2018, p.5). Esto quiere decir que cuando alguien comercializa, es decir que vende o alquila, su base de datos a un tercero para un fin cualquiera, se está hablando de una cesión de datos y se deben cumplir ciertos requisitos.

Gallardo (2019) también explica que se está frente a un acceso a datos para prestación de servicios, si quien recibe los datos se limita a realizar ciertas operaciones sobre estos, sin poder decidir sobre su finalidad. En este caso se están refiriendo a las figuras del responsable y del encargado del tratamiento (p.5).

El Responsable de Tratamiento es la persona que decide sobre el contenido, uso y finalidad que tendrá este, mientras el Encargado es quien trata los datos personales por cuenta del responsable (Gallardo, 2018, p. 2).

#### **2.4.1.1 Requisitos para la cesión de datos.**

Según el Reglamento General de Protección de Datos europeo, para que la cesión o comercialización se considere lícita debe cumplir las siguientes bases jurídicas (Gallardo, 2018):

- Que cuente con el consentimiento previo, específico e inequívoco de los titulares de dichos datos.
- Que la cesión sea necesaria para la ejecución o desarrollo de una relación contractual.
- Que constituya una obligación legal para el cedente.
- Que obedezca a intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.
- Que sirva para salvaguardar el interés vital del interesado o de otras personas. (p.5).

El consentimiento según el artículo 4.11 del RGPD (2016), se define como:

La manifestación de voluntad libre, específica, informada e inequívoca por la cual el interesado acepta, mediante una clara acción afirmativa, el tratamiento de sus datos personales.

Bajo estas mismas condiciones se debe otorgar el consentimiento para la cesión de datos personales. Por libre se entiende que no se otorga bajo engaño, amenazas o coacciones. Específico implica que se da para una finalidad determinada y si hay varias, se debe pedir consentimiento para cada una. Informado implica que este debe cumplir los requisitos del reglamento y expresarse de manera clara y sencilla. Inequívoco quiere decir que el responsable puede demostrar que el consentimiento obtenido es válido y que cuenta con el visto bueno del titular para el tratamiento. Finalmente la acción positiva indica no son válidos los consentimiento obtenidos a través del silencio, la inactividad o el uso de casillas pre marcadas (Andrés, 2019).

Los últimos cuatro requisitos mencionados por este autor hacen referencia a los intereses legítimos del tratamiento. Adicionalmente, se puede agregar el requisito de "informar a las personas, a más tardar en el momento de enviarles la primera comunicación, de que han obtenido sus datos personales" (Comisión Europea, n.d.) y la finalidad.

De no cumplir estos requisitos, la cesión o comercialización se considera ilegal.

### *2.4.2 Origen*

Gregorio (2019) considera que las empresas de riesgo crediticio aprovecharon el vacío cuando eran pequeñas y nacionales. La informalidad y falta de seguridad en las bases de datos estatales facilitó que obtuvieran bases de datos a través de compras ilegales de datos. Posteriormente, estas empresas fueron adquiridas por transnacionales o esa función se comenzó a desarrollar en Cámaras de Comercio, llevando a una mayor legalidad en la obtención de datos y suministro de registros.

La cantidad de registros privados ha aumentado exponencialmente con los avances tecnológicos, y en la mayoría de los casos los mismos usuarios son quienes brindan la información. Baste como muestra, bancos, empresas de tarjetas de crédito y compañías aéreas, entre muchas otras entidades privadas a las que les resulta útil las bases de datos personales ya sea para prevenir un delito u optimizar sus servicios (Gregorio, 2019).

### *2.4.3 Necesidad de los registros privados*

La información recolectada puede fácilmente ser transmitida o comercializada con terceros sin apenas coste y con un mínimo esfuerzo para que estos terceros pueden procesar los datos según sus propios fines. Los mismos avances tecnológicos, compatibilidad e

interconexión facilita esta práctica, volviendo factible una multiplicación indefinida de los tratamientos de datos personales para difundir la información más allá del consentimiento (Huerta, 2017, p. 216).

Es importante mencionar que “las empresas requieren transferir y manejar datos por el importante valor monetario que la información puede llegar a representar” (Vera & Vivero, 2019, p. 235).

Cubillos (2017, p. 37) menciona que anteriormente las compañías usaban los datos para la prospección comercial, pero ahora tiene una finalidad diferente, utilizando los datos para efectuar orientación personalizada de la publicidad a cada usuario.

Efectivamente, la información tiene un valor comercial ya que le facilita a la empresa acercarse y contactar a los clientes, así como promover su marca, producto o servicio de una manera más eficiente al ser personalizada o individualizada. Esto representa una ventaja competitiva, considerando que el acercamiento generalizado ya no es un método de mercadeo eficiente (Vera & Vivero, 2019, p. 252).

Pongamos por caso, un proveedor de tarjetas de crédito que puede monitorear el perfil de consumo de una persona para detectar una tarjeta robada e interceptarla. Las aerolíneas aéreas tienen perfiles de sus pasajeros para predecir probabilidades de ausencia al vuelo, optimizando sus servicios. También las antecedentes crediticios sirven para conceder un crédito de manera más segura (Gregorio, 2019).

Vera y Vivero (2019) indican que las estrategias para mantener y atraer clientes implican la necesidad de conocer los datos personales de los consumidores para acceder a la

privacidad de estos. Estas estrategias se valen de diferentes medios para lograr el contacto cliente- empresa, ya sea del internet, donde es relativamente fácil que el usuario proporcione sus datos o de los medios tradicionales como la recepción de datos vía presencial (p. 238).

Se puede concluir que se generado un debate entre "la capacidad de la empresa de obtener los máximos resultados en base al potencial de información adquirible sobre los clientes y le derecho a la privacidad de estos para mantener la confidencialidad de aquellos datos considerados más íntimos" (Vera & Vivero, 2019, p. 238).

### *2.4.4 Riesgos de la comercialización ilegal de datos personales*

A priori, el uso, administración y almacenamiento inadecuado de datos de carácter personal, así como la mala divulgación y transparencia, tienen el potencial de generar discriminación y falta de confianza en las instituciones (Comisión Nacional de Bancos y Seguros, 2020).

Gregorio (2019) advierte que la comercialización de datos personales entra en colisión con los derechos de privacidad e intimidad y son alicientes para la discriminación especialmente cuando se desarrollan en un vacío legal.

Se entiende que en teoría (Vera & Vivero, 2019), la transferencia de bases de datos no debería ser un problema ya que tiene un fin comercial que permite que las opciones de clientes crezcan y pone una variedad de alternativas a disposición del cliente. Sin embargo, el problema está en que muchas empresas intentan forzar las compras cuando el producto o servicio no ha sido solicitado, deseando ni requerido. Declinar estas ofertas resulta insuficiente ya que tienden a exigir explicaciones o pedir información, generando un desgaste

al consumir tiempo y energías. Muchas veces hasta es necesario emprender reclamos legales para retirar la información, pero no hay seguridad sobre una reacción de las autoridades. Por ejemplo, las empresas de bancos o aseguradoras que realizan llamadas por teléfono para ofrecer beneficios o productos que los usuarios no han solicitado (pp. 252- 253).

Otra situación que se presenta viene derivada de la falta de consentimiento informado o inequívoco por parte de los usuarios, lo cual, de producirse una transferencia de datos a terceros, podría derivar en una práctica perjudicial de comercialización ilegal de bases de datos.

En la práctica, usualmente el usuario no conoce las implicaciones de conceder libremente sus datos, no está consciente de estar cediendo sus datos (Vera & Vivero, 2019, p. 235) o a este no se le permite acceder a un servicio o aplicación si no da su consentimiento para la transmisión de datos que luego son utilizados para publicidad comportamental y reventa de datos a terceros (Gil, 2015, p. 66). Según el estudio español de la Organización de Consumidores y Usuarios (2018, citado en Villan, 2018):

> El 91% de los encuestados denunció que a la hora de registrarse a un servicio en línea a veces se le piden datos que no tienen que ver con dicho servicio, estos datos suelen ser utilizados con un provecho comercial de los clientes y ganancias. En ocasiones suelen ser utilizados también para realizar marketing dirigido a perfiles de todas las edades.

Por lo tanto, además de la necesidad de regulación jurídica, existe une responsabilidad de las empresas como tratantes de datos frente al consentimiento del usuario. Villan (2018)

sugiere que las empresas y la industria deberían de desarrollar políticas de privacidad y términos y condiciones de manera atractiva para informar a los usuarios sobre el tratamiento de sus datos.

La comercialización ilegal de bases de datos representa uno de los múltiples desafíos que enfrenta la sociedad y las sociedad, frente a los cuales se deben propulsar mecanismos idóneos y adecuados para regular y controlar el tratamiento de datos personales, así como sancionar su uso malicioso (Vera & Vivero, 2019, p. 235).

#### 2.4.4.1 Vulneración de los derechos ARCO.

Se ha establecido que el problema principal respecto a la comercialización ilegal de bases de datos radica en la pérdida de control del usuario sobre sus datos, por tanta conceptualmente, en la pérdida del Derecho a la Protección de Datos Personales y en consecuencia de los derechos ARCO. En la opinión de Benda (2001, citado en Huerta, 2017):

> El peligro para la privacidad del individuo no radica en que se acumule información sobre él, sino, más bien, en que se pierda la capacidad de disposición sobre ella y respecto a quien y con qué objeto se tramiten. La privacidad se destruye no por la información en sí misma, sino por su transmisión disfuncional sobre la que el afectado pierde toda posibilidad de influir.

De forma puntual, no se ha definido claramente los derechos ARCO vulnerados, sin embargo, es posible inferir que esta práctica vulnera directamente el derecho de Acceso ya que, como expone Cubillos( 2017), este derecho implica que el tratamiento debe ser realizado únicamente por la persona autorizada por el usuario (p. 31). Al transferir y

comercializar esta información con terceros sin haberlo estipulado previamente, se pierde el consentimiento del usuario, volviéndose un tratamiento inválido y hasta ilegal.

Al perder el usuario conocimiento de quienes realizan el tratamiento y los fines, se infiere que pierde control sobre estos al no poder ejercer el derecho de rectificación y cancelación por falta de conocimiento (Villan, 2018, pp. 22–23).

Es menester recalcar, que en estas situaciones, el usuario podría valerse del derecho de oposición, considerando que puede oponerse a este tratamiento por haber sido recabado sin su consentimiento y porque es un motivo fundado (Villan, 2018).

### 2.5 Marco Jurídico Actual

Frente al desarrollo del Derecho a la Protección de Datos Personales, los avances tecnológicos y los riesgos que implican, una gran parte de Estados han avanzado frente a la responsabilidad legal que deriva con la elaboración de normas nacionales e internacionales que toman en cuenta dicho desarrollo.

Rodríguez (2015) propone que según como sea reconocido el Derecho a la Protección de Datos Personales, los países se pueden clasificar en aquellos que lo reconocen expresamente en sus textos constitucionales, aquellos en los que el texto constitucional no lo reconoce expresamente pero que tienen disposiciones relacionadas que han permitido a los tribunales reconocer este derecho fundamental y los que no establecen este nuevo derecho, pero cuyo tribuna lo ha reconocido como parte de otro derecho ya establecido en la Constitución, por ejemplo con la intimidad, vida privada, dignidad, etc. (p. 61).

### *2.5.1 Marco jurídico internacional: Tratados y convenios*

El Derecho a la Protección de Datos Personales se considera un derecho fundamental y derecho humano al encontrarse en una variedad de referencias en tratados y convenios de Derechos Humanos. Junto al derecho a la intimidad, este se considera un "derecho personalísimo que poseen todos los individuos al nacer ya que tienen la característica de ser innatos" (Villan, 2018).

La normativa internacional incluye en el artículo 12 de la Declaración Universal de Derechos Humanos de 1948 el reconocimiento al derecho de la intimidad, el cual posteriormente inspiró el artículo 17 del Pacto Internacional de Derechos Civiles y Públicos en 1966 (Ruiz, 2016, p. 6).

El artículo 17 del Pacto Internacional de Derechos Civiles y Públicos (1966) expresa que:

> 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.
> 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

A nivel americano, Ruíz (2016, p. 6) menciona que también existe una referencia a este derecho en el artículo V de la Declaración Americana de los Derechos y Deberes del Hombre (1948), que literalmente dice, "toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar".

En América este es luego contemplado de manera más amplia en el artículo 11 de la Convención Americana sobre Derechos Humanos (1969) de la siguiente forma:

**Protección de la Honra y de la Dignidad**

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.

2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

Es menester resaltar, que los instrumentos internacionales mencionados hasta el momento hacen referencia al Derecho a la Protección de Datos Personales a través de la interpretación del texto que vincula a los datos y su tratamiento, lo cual según López- Torres (2014), muestra que en la época de su redacción los avances tecnológicos no representaban el mismo riesgo para los datos personales que en la actualidad (p. 108).

Ruíz (2016, p. 5- 9) menciona una gran cantidad de instrumentos internacionales que reconocen esta protección en el derecho comunitario europeo, comenzando con el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales que lo reguló bajo el derecho a la intimidad. Entre estos, resalta la regulación lograda en el artículo 8 de la Carta de Derechos Fundamentales (2000), el cual es el primer tratado internacional en reconocer la autonomía del Derecho a la Protección de Datos Personales, regulándolo de la siguiente manera:

**Protección de datos de carácter personal**

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.
3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

El Comité de los Derechos Humanos de las Naciones Unidas señala que de manera general, los Estados deben de regular la recopilación y el registro de información personal en bancos de datos, computadoras y otros registros (López-Torres, 2014, p. 109).

### *2.5.2 Marcos jurídicos de referencia*

Además del desarrollo del Derecho a la Protección de los Datos de Carácter Personal como derecho humano, vale la pena conocer las formas en las que varios Estados lo han incorporado a sus legislaciones con el objetivo de garantizar este derecho fundamental.

#### **2.5.2.1 La Unión Europea como legislación más avanzada.**

La Unión Europea cuenta con una gran cantidad de instrumentos jurídicos nacionales e internacionales que regulan el tratamiento de datos personales. Una gran cantidad de sus Estados miembros cuentan con legislación interna, los cuales, según las categorías mencionadas de Rodríguez (2015), se ubican de la siguiente manera (p. 61):

*Tabla 1. Clasificación de los países europeos según el reconocimiento del Derecho a la Protección de Datos Personales.*

| Categoría | | *Países* |
|---|---|---|
| 1. | Países que reconocen el derecho expresamente en sus textos constitucionales. | Portugal, Suecia, Eslovaquia, Hungría y Polonia y Alemania[1]. |
| 2. | Países que el texto constitucional no reconoce expresamente el Derecho a la Protección de Datos Personales, pero que poseen disposiciones sobre la materia que han permitido a los Tribunales Constitucionales reconocer dicho derecho fundamental. | España, Finlandia, Países Bajos y Lituania. |
| 3. | Países que no establecen el nuevo derecho, pero el Tribunal Constitucional los ha reconocido al formar parte integrante del contenido de otro derecho ya establecido expresamente en la Constitución, como es el caso de la intimidad, vida privada, libre desarrollo de la personalidad o dignidad humana. | Italia. |

*Fuente: Elaboración propia a partir de Rodríguez (2015, p. 61).*

[1] Incluyendo los que han reformado sus constituciones e incorporado el derecho, como el caso de Alemania.

Respecto al derecho comunitario, producto de reconocer el Derecho a la Protección de Datos Personales como un derecho humano, Europa cuenta con un Reglamento General de Protección de Datos Personales que entró en vigor el 25 de mayo del 2018 (Villan, 2018).

Este reglamento se considera reciente y moderno, incorporando a la protección de datos personales dos nuevos derechos: la portabilidad de datos y al olvido. Villan (2018) La portabilidad de datos se refiere a la información que reciben los usuarios que solicitan acceso a sus datos personales, según este derecho esta información se debe presentar al usuario de manera clara, en un formato estructurado, de uso común, de lectura mecánica e interoperable. El derecho al olvido complementa el derecho a la cancelación, obligando al tratante que publica datos a suprimir todo enlace, copias o réplicas de datos, especialmente cuando existen datos que pueden comprometer el derecho al honor e intimidad.

El marco jurídico europeo se considera un referente en materia de legislación para la protección de datos personales, ya que, como señala López- Torres (2014), "los estándares emanados de la Unión Europea, aún sin proponérselo, están sirviendo como base para la regulación de la materia a nivel global" (p. 103).

#### 2.5.2.2 Situación regional: América Latina.

Latinoamérica no cuenta con una legislación homogénea como sucede en la Unión Europea. Sin embargo, en varios países de la región se han dado reformas constitucionales o procesos legislativos tomando en consideración la problemático desde el hábeas data, protección de datos personales, acceso a la información administrativa, regulación de las empresas que comercializan datos y seguridad de los datos (Gregorio, 2019, p. 1).

Con base a la clasificación propuesta por Rodríguez (2015, p. 61), los países latinoamericanos se pueden ubicar de la siguiente manera:

*Tabla 2. Clasificación de los países latinoamericanos según el reconocimiento del Derecho a la Protección de Datos Personales.*

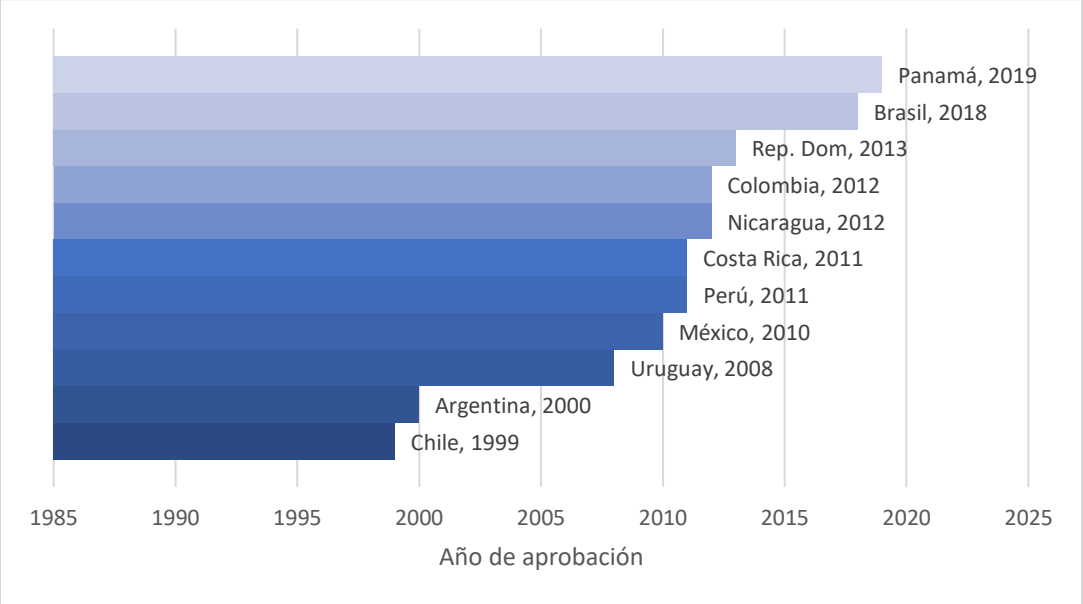
| Categoría | | *Países* |
|---|---|---|
| *1.* | Países que reconocen el derecho expresamente en sus textos constitucionales. | Rep. Dominicana, Ecuador, México y Chile. |
| *2.* | Países que el texto constitucional no reconoce expresamente el Derecho a la Protección de Datos Personales, pero que poseen disposiciones sobre la materia que han permitido a los Tribunales Constitucionales reconocer dicho derecho fundamental. | Brasil, Guatemala, Perú, Colombia, Honduras, Paraguay, Argentina y Venezuela. |
| *3.* | Países que no establecen el nuevo derecho, pero el Tribunal Constitucional los ha reconocido al formar parte integrante del contenido de otro derecho ya establecido expresamente en la Constitución, como es el caso de la intimidad, vida privada, libre desarrollo de la personalidad o dignidad humana. | Uruguay, Panamá, Nicaragua, El Salvador y Costa Rica. |

*Fuente: Elaboración propia a partir de Gregorio, Red Iberoamericana de Protección de Datos y Rodríguez* (2019, p. 1; 2020; 2015, p. 61).

Conviene subrayar el hecho que existan países latinoamericanos que reconozcan expresamente el Derecho a la Protección de Datos Personales como en Europa, siendo en su mayoría, los que lo reconocen de manera indirecta.

En la siguiente figura se pueden observar la creciente tendencia de los países latinoamericanos en la regulación de la protección de datos personales a través de una norma general, siendo Chile el primer país de región en implementarla.

*Figura 1. Leyes de protección de datos personales por año de aprobación en América Latina.*




*Fuente: Elaboración propia a partir de Rodríguez y Red Iberoamericana de Protección de Datos* (2020; 2015, p. 61).

A la luz de los estándares regulatorios europeos, solamente dos países poseen una regulación adecuada en América Latina: Argentina y Uruguay. Villan (2018) explica que la Unión Europea:

> Mediante una decisión de adecuación se declara que un Estado ofrece un nivel de protección adecuado y por tal razón se pueden transferir datos a otra empresa en un Estado que no pertenezca a la Unión Europea.

En la opinión de Gregorio (2019), la legislación sectorial de Argentina refleja el modelo europeo de protección de datos personales, mientras que la de México se aproxima al

modelo de Estados Unidos. No obstante, hay autores (Maqueo et al., 2017) que afirman que el derecho europeo sirvió de fuente de inspiración para el caso de México, ya que "reconocen la protección de datos personales como un derecho humano diferenciado, aunque relacionado con el derecho a la vida privada" (p. 82).

Se debe subrayar, que Chile y Brasil han realizado avances que representan un impulso de los nuevos estándares en protección de datos personales en la región. Brasil, por ejemplo, aplica su legislación a empresas con sede en su país y las que realicen recolección de datos en este. Además de requerir consentimiento para el tratamiento, exige herramientas para que el usuario pueda fácilmente acceder, corregir y eliminar sus datos personales, con multas hasta del 4% de los ingresos de la compañía por incumplimiento (Villan, 2018).

Mientras que Chile modificó su normativa en el 2018 ampliando su alcance al incluir datos combinados, también se define la cesión de bases de datos, regula derechos ARCO, define nuevas categorías de datos especiales y aumenta sanciones (Villan, 2018).

A pesar de esto, a juicio de Villan (2018) las legislaciones latinoamericanas se podrían considerar desactualizadas si se toman en cuenta las nuevas técnicas y formas de recopilar información que se han desarrollado, además de las nuevas amenazas a los datos personales.

Llama la atención, que varios países latinoamericanos no cuentan con una legislación sectorial para la protección de datos personales. Incluso se podría llegar a pensar, que la protección de datos personales en América Latina, "constituye una condición necesaria, pero no suficiente para su abordaje" (Travieso, 2016, p. 115). Esto representa un problema al

dificultar perseguir delitos informáticos relacionados con el mal uso y abusos en el tratamiento de datos personales (Sarmiento, 2016).

### *2.5.3 Marco jurídico hondureño*

#### 2.5.3.1 Constitucional e internacional.

Respecto a la constitucionalización de este derecho, se debe mencionar que no solo implica aumentar el nivel de protección de los datos personales, sino que también fortalece las normas de protección de privacidad (Álvarez, 2020, p. 4).

En Honduras, la Constitución (1982) recoge como derecho fundamental el derecho a la intimidad personal y a la inviolabilidad de las comunicaciones al indicar en su artículo 76 que "se garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen" (p. 67) y en su artículo 100 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" (p. 71).

La Constitución (1982), con la reforma del 2005, establece en su artículo 182 la garantía de Hábeas Data, haciendo referencia al derecho fundamental de acceso a la información pública o privada: "el Estado reconoce la garantía de Hábeas Corpus o de exhibición Personal, y de *Hábeas Data*" .Además de mencionar que:

> 2. Hábeas Data
>
> Toda persona tiene el derecho de acceso a la información sobre si misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros Públicos o privados y, en el caso de que fuere necesario, actualizarla,

> rectificarla y/o suprimirla. No podrá afectarse el secreto de las fuentes de información periodística (p. 87).

López (2014) analiza que, por lo tanto, la acción de Hábeas Data se establece como un mecanismo procedimental de aplicación inmediata por parte de las autoridades jurisdiccionales hondureñas, con la finalidad de hacer cesar cualquier violación contra el honor, intimidad personal o familiar y la propia imagen.

Desde el punto de vista de López (2014), Honduras incorporó la garantía de Hábeas Data en su legislación dejando pendiente el desarrollo normativo propio de la protección de datos personales como parte de una tendencia latinoamericana.

Más aún, Tomé (2019) enfatiza que el conocimiento del recurso de Hábeas Data como garantía constitucional:

> Se enfoca exclusivamente a la Sala Constitucional de la Corte Suprema de justicia. Esto limita el acceso a la población general al acceso a la interposición de este recurso, ya que la Corte Suprema solamente tiene sede en la ciudad capital y este recurso debe ser interpuesto directamente por la persona cuya información es la que consta en los registros
>
> Honduras es un país con casi 9 millones de habitantes y es importante tomar en cuenta que la Sala Constitucional solamente cuenta con 4 magistrados, quienes también conocen los recursos de Amparo, Revisión, inconstitucionalidad y Hábeas Corpus. Es irrisorio penar que cuentan con la capacidad para darle una pronta resolución a los recursos presentados sin poder garantizar la seguridad jurídica a la ciudadanía de manera efectiva. (p. 3).

Por otra parte, Honduras también es suscriptor de instrumentos internacionales que reconocen el Derecho a la Protección de Datos Personales. Además de tratados y convenios en materia de derechos humanos (como el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana de Derechos Humanos), también se protege a través de instrumentos como el Convenio Budapest para homogenizar la persecución de cibercriminalidad y el Convenio de las Naciones Unidas sobre la utilización de las comunicaciones electrónicas en los contratos internacionales (Sarmiento, 2016).

#### *2.5.3.1.1 Bien jurídico protegido.*

En Honduras, el Derecho a la Protección de Datos Personales o a la Autodeterminación Informativa es un derecho fundamental.

Dada la regulación constitucional y que la misma no reconoce expresamente el Derecho a la Protección de Datos Personales como un derecho fundamental autónomo, se puede entender que en Honduras se protege contra las violaciones al honor, intimidad personal o familiar y la propia imagen, siendo una de estos, los abusos y mal uso de los datos personales.

De manera que con el Derecho a la Protección de Datos Personales lo que se quiere proteger son los datos que identifican o puedan llegar a identificar a una persona, lo cual influye en la intimidad y vida privada de esta porque traspasa el dato y se llega a hablar de la persona, no del dato (Polo, 2020, p. 176).

#### 2.5.3.2 Marco jurídico ordinario.

Honduras no cuenta con una ley sectorial vigente que regule la protección de datos personales, por lo que está regulada de manera dispersa e imprecisa. A continuación, se revisará las normas jurídicas sobre protección de datos personales que existen en el marco jurídico ordinario hondureño.

##### *2.5.3.2.1 Legislación.*

A falta de una regulación especial, los datos personales cuentan con una protección dispersa e imprecisa.

La Ley sobre Justicia Constitucional desarrolla la garantía del Hábeas Data en defensa del orden público constitucional (LatinAlliance, 2020). Brewer-Carías (2016) destaca que este desarrollo se da en conjunto a la garantía de exhibición personal y que contiene escasas normas en las cuales se reguló o refirió al Hábeas Data (p. 65).

La *Ley de Transparencia y Acceso a la Información Pública* hondureña también garantiza en cierto grado el derecho a la protección de sus datos personales al permitir acceder a la información pública de la Administración Pública y sus organismos. La misma obliga alos tres poderes del Estado, así como Organizaciones No Gubernamentales, Organizaciones Privadas de Desarrollo y personas naturales y jurídicas que reciban o administren fondos públicos, independientemente de su origen y nacionalidad (López, 2014).

Se reconoce su protección en la *Ley del Instituto de Acceso a la Información Pública* que en sus artículos 24 al 26 reconoce la garantía al Hábeas Data. Esta regulación también faculta al Comisionado Nacional de Derechos Humanos para incoar acciones para la

protección de datos personales y establece la prohibición de solicitar datos que puedan generar discriminación o poner en riesgo derechos morales y patrimoniales (Tomé, 2019, p. 5), haciendo referencia a los datos personales especiales.

#### *2.5.3.2.2 Anteproyecto de ley.*

En el marco de la globalización se continúa discutiendo la necesidad de desarrollar una normativa que regule el tratamiento de datos personales considerando los derechos fundamentales y riesgos, asunto que en Honduras parece haber quedado de lado. Deloitte (n.d. citado en Sarmiento, 2016) señala que sin una ley sectorial, se disminuye los niveles confianza y fortalecimiento de las instituciones, exponiéndolas a daños de reputación, credibilidad y hasta pérdidas económicas.

Desde principios del 2014 se dio a conocer el Anteproyecto de Ley de Protección de Datos Personales y Hábeas Data en Honduras a través del Instituto de Acceso a la Información Pública. Para la elaboración de este proyecto se tomaron en cuenta la Resolución 34/95, Principios rectores para la Reglamentación de los Ficheros de Datos Personales, la Directiva Europea 95/46/CE y diferentes documentos de la Red Iberoamericana de Protección de Datos (D. López, 2014). Para su elaboración también se contó con el apoyo de la Agencia Española de Cooperación Internacional para el Desarrollo (Tomé, 2019, p. 5).

El ámbito de aplicación que tenía el anteproyecto de ley eran los datos personales registrados en bases de datos automatizadas y manuales de organizaciones públicas y privadas, exceptuando las mantenidas por personas naturales en el ejercicio de actividades

personales o domésticas, las que tengan como finalidad la seguridad pública, defensa, seguridad del Estados, material penal y su investigación, y las creadas por leyes especiales, archivos y datos periodísticos (D. López, 2014).

El anteproyecto de ley también reconocía el derecho de las personas frente a la recolección de sus datos, estableciendo la obligación de informárselo de manera expresa, precisa e inequívoca a través de un aviso de privacidad. Definiendo Aviso de Privacidad como "el documento físico, electrónico o en cualquier otro formato, generado por el Responsable del Tratamiento que es puesto a disposición del Titular, previo al tratamiento de los datos", y estipulando que mínimo debe contener identidad y domicilio del responsable, finalidad del tratamiento y posibles destinatarios, opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos, consecuencias de proporcionarlos y de no hacerse o de su inexactitud (D. López, 2014).

Sarmiento (2016) resalta que este proyecto propone y establece:

> Un esquema procesal para darle mayor peso jurídico, así como la elaboración de un reglamente de la Ley, y la conformación e integración de una Gerencia de Protección de Datos (Prodatos) en el Instituto de Acceso a la Información Pública (IAIP), entidad que vigilará el cumplimiento de dicha ley.

Es menester resaltar, que en este anteproyecto también se hacía referencia a los derechos ARCO, reconociendo los cuatro derechos: acceso, rectificación, eliminación y oposición, además de incluir el derecho a la transferencia de datos y a la indemnización. Este derecho a la transferencia de datos limita al tratante a solo poder transmitir datos si el titular

ha prestado su consentimiento expreso e inequívoco para esto, el cual puede ser revocado. El derecho de indemnización se reconoce cuando el titular considere que por consecuencia de un incumplimiento legal en el tratamiento de sus datos, ha sufrido daños o lesiones ya sea en sus bienes o derechos (D. López, 2014).

Con relación al derecho al acceso, esta lo determina como la opción que tienen los usuarios a obtener toda la información que les concierna en bases de datos públicas y privadas, indicando que este se ejercerá de manera gratuita. Del derecho a la Oposición, establece que el titular se puede oponer al tratamiento si no se ha respetado las garantías y principios constitucionales y legales, pero que no se podrá ejercer este si el tratamiento es en cumplimiento de una obligación legal (D. López, 2014).

También se contempla el consentimiento, estableciendo que los datos personales de los ciudadanos solo pueden ser utilizados para las funciones establecidas y consentidas por los titulares y que será nulo el consentimiento otorgado cuando la finalidad del tratamiento no esté establecida. A pesar de esto, se critica que el anteproyecto no menciona claramente una definición de transferencia de datos, ni regula la cesión (Tomé, 2019, pp. 14, 17).

También se menciona (Tomé, 2019), que el anteproyecto contemplan sanciones administrativas pecuniarias entre 10 y 60 salarios mínimos sin perjuicio de las demás acciones civiles o penales que deriven, sin establecer si procederán a instancia de parte o de oficio y encargando de su aplicación al Instituto de Acceso a la Información Pública (p. 18).

A juicio de López (2014), el anteproyecto de ley de protección de datos personales y Hábeas Data representaba una “norma avanzada que plasma una evolución de la

responsabilidad de los Encargados de Ficheros, que incluye algo de los aspectos que las nuevas normas -iberoamericanas y europeas- están contemplando".

El anteproyecto "plantea con su aprobación que los ciudadanos sean los responsables y tengan los derechos a decidir, cómo y quién va a tratar su información personal" (Villan, 2018). Sin embargo, desde el 2018 el Congreso Nacional sometió a debate los artículos del proyecto de Ley de Protección de Datos Personales y hasta la fecha no se ha logrado su aprobación.

# CAPÍTULO III

# 3. DISEÑO METODOLÓGICO

## 3.1 Congruencia metodológica

### *3.1.1 Matriz metodológica*

Para la realización de la presente investigación se estará aplicando la metodología de investigación jurídica, siendo una investigación aplicada y no experimental. Siendo el derecho una ciencia, cuenta con sus propias metodologías de la investigación, que para Martínez (2010, citado por Sánchez, 2011) se entienden como el "estudio y análisis del procedimiento para poder determinar cuál es la respuesta jurídica para el caso que estamos examinando, aunque, como veremos, incluye también muchos otros aspectos" (p. 329).

La matriz de congruencia se define como:

> Una herramienta que brinda la oportunidad de abreviar el tiempo dedicado a la investigación, su utilidad permite organizar las etapas del proceso de investigación de manera que desde el principio exista una congruencia entre cada una de las partes involucradas en dicho procedimiento (Pedraza, 2001, p. 313).

La matriz de congruencia metodológica muestra un resumen de la investigación y permite comprobar la secuencia lógica. La siguiente tabla muestra la matriz de congruencia metodológica de esta investigación y señala la relación entre variables:

*Tabla 3. Matriz de Congruencia Metodológica.*

| ***Tema*** | **Objetivo General** | **Objetivos Específicos** | **Preguntas de Investigación** | **Instrumentos o técnicas de recolección** |
|---|---|---|---|---|
| *Protección de los datos personales de la comercialización ilegal de bases de datos y la subsecuente deducción de responsabilidad a los entes comerciales privados que quebrante dicha protección en Honduras.* | Proponer un mecanismo legal de protección de datos personales de la comercialización ilegal de bases de datos y la subsecuente deducción de responsabilidad a los entes comerciales privados que quebranten dicha protección a través del estudio y | Evaluar la percepción de la población hondureña sobre la protección de su información personal frente a la comercialización ilegal de sus datos por entes comerciales privados. | ¿Considera la población hondureña que su información personal se encuentra en riesgo de ser comercializada ilegalmente por entes privadas? | Encuesta. |
| | | Describir la manera en que el marco jurídico hondureño vigente regula la | ¿De qué manera la legislación actual regula la responsabilidad | Investigación documental. |

| | | | |
|---|---|---|---|
| análisis del marco jurídico hondureño, contratos y proyectos de ley para garantizar la privacidad e intimidad de los usuarios. | responsabilidad de los entes comerciales privados frente a la comercialización ilegal de bases de datos personales. | de los entes comerciales privados con relación a la comercialización ilegal de bases de datos? | |
| | Determinar la eficacia del marco jurídico hondureño actual que regula la protección de datos personales para evitar que entes comerciales privados comercialicen ilegalmente | ¿Es el marco jurídico actual eficaz en regular la protección de datos personales para la comercialización ilegal de bases de datos por entes comerciales | Investigación documental. |

| | | | |
|---|---|---|---|
| | bases de datos a fin de establecer si precisa una regulación especial. | privados o precisa una mayor regulación? | |
| | Examinar aciertos y vacíos del Anteproyecto de Ley para la Protección de Datos Personales (2014) con relación a su aplicabilidad en la actualidad para evitar la comercialización ilegal de bases de datos por parte de entes | ¿Qué aciertos y vacíos tiene el Anteproyecto de Ley de Protección de Datos Personales (2014) con relación a su aplicabilidad en la actualidad para evitar la comercializació n ilegal de datos por entes | Entrevistas no estructuradas. |

| | | | |
|---|---|---|---|
| | comerciales privados. | comerciales privados? | |

*Fuente: Elaboración propia.*

### 3.2 Hipótesis

Una hipótesis es una premisa determinada que responde de manera tentativa la pregunta de investigación y que debe ser demostrada. Villabella (2015, p. 932) la define como:

> Una conjetura o suposición establecida con base científica, y que presupone una conclusión no verificada sujeta a la demostración científica. Es un enunciado con cierta generalidad que puede ser verificado, es el punto de partido de un raciocinio que puede confirmarse, poniendo a prueba sus consecuencias particulares. (p. 932)

La hipótesis debe de ser llevada al campo de los hechos para contrastarse con la realidad y poder demostrar a relación existente entre el planteamiento y los sucesos. Se constituye en base a información previa, por lo que se define como una suposición o explicación anticipada, respuesta previa y tentativa que la investigadora formula respecto al problema y que puede resultar ser verdadera o no verdadera (Olvera, 2015, p. 71).

En Honduras se reconoce constitucionalmente el Derecho a la Protección de Datos Personales de manera tácita en la figura del Hábeas Corpus, el derecho a la intimidad y a la inviolabilidad de las comunicaciones. Sin embargo, el país no cuenta con una legislación especial como en otros países, que regule y oriente el uso de datos personales por parte de la

empresa privada para garantizar la protección de los usuarios. Considerando lo anterior, la hipótesis de la presente investigación es:

La implementación de una legislación de protección de datos personales en Honduras servirá como mecanismo legal para garantizar la privacidad e intimidad a los usuarios al regular la comercialización de bases de datos y la subsecuente deducción de responsabilidad a los entes comerciales privados que la quebranten.

### 3.3 Tipo de investigación

En la investigación científica se identifican dos tendencias: la investigación básica y la investigación aplicada. La investigación básica, fundamental, exacta o pura, se ocupa del objeto de estudio sin considerar una aplicación inmediata ya que a partir de sus resultados pueden surgir nuevos avances científicos. Por otro lado, la investigación aplicada o empírica utiliza los conocimientos adquiridos al aplicarlos en procesos que generan nuevos conocimientos y enriquecen la disciplina, es decir que tiene una aplicación inmediata (Vargas, 2009, p. 159).

Se entiende que esta es una investigación aplicada ya que se desarrolla sobre problemas que ya han sido planteados, siendo su objetivo aplicar teorías y revisar críticamente el conocimiento existente para aportar soluciones (Villabella, 2015, p. 924). Esta investigación pretende plantear una solución respecto a la protección de datos personales en Honduras para evitar la comercialización ilegal de datos personales.

### 3.4 Enfoque de la investigación

El enfoque de la investigación hace referencia a la perspectiva asumida o rutas para aproximarse al conocimiento. En la teoría generalmente se mencionan tres enfoques: cuantitativo, cualitativo y mixto (combinación de los dos anteriores).

El enfoque cuantitativo hace referencia a lo cuantificable o medible en cantidades determinadas. En este enfoque se trabaja con números y medidas, y "se busca la exactitud de mediciones o indicadores sociales con el fin de generalizar sus resultados a poblaciones o situaciones amplias" (Olvera, 2015, p. 85).

El cualitativo se refiere a cualidades y se realizan descripciones detalladas de situaciones específicas, personas o comportamientos. Este enfoque analiza a profundidad una realidad y aunque se obtienen datos, estos no se cuantifican. Vale la pena resaltar, que en este enfoque de investigación, el conocimiento obtenido es válido únicamente para el fenómeno estudiado (Olvera, 2015, pp. 86–88).

La presente investigación tiene un enfoque cualitativo ya que busca conocer y describir la realidad hondureña respecto a la protección de datos personales para evitar la comercialización ilegal de bases de datos.

### 3.5 Alcance de la investigación

Resulta imperativo conocer el alcance del estudio para poder definir una estrategia de investigación, estableciendo sus límites conceptuales y metodológicos. La teoría determina cuatro tipos de alcances: exploratorio, descriptivo, correlacional y explicativo.

El alcance exploratorio busca familiarizar con un tema desconocido o novedoso; el descriptivo analiza cómo es y cómo se manifiesta un fenómeno; el correlacional pretende determinar relaciones entre variables, conceptos o características y el explicativo encontrar razones o causas que provocan ciertos fenómenos. Una misma investigación puede abarcar varios de estos alcances (Hernández et al., 2014, p. 99).

La presente investigación tiene un doble alcance: exploratorio y descriptivo.

### *3.5.1 Alcance exploratorio*

Los estudios con alcance exploratorio son la base de los demás alcances, preparando el terreno para nuevos estudios. Generalmente en este alcance se investigan problemas poco estudiados en los que hay muchas dudas o problemas estudiados desde una perspectiva innovadora (Hernández et al., 2014, pp. 89, 91).

Muchos autores (Hernández et al., 2014) consideran que los estudios exploratorios sirven para familiarizar con fenómenos relativamente desconocidos mientras se recolecta información para determinar la posibilidad de realizar una investigación más compleja, encontrar nuevos problemas, identificar conceptos, variables y prioridades o sugerir postulados en futuras investigaciones (p. 91).

Aunque la protección de datos personales en Honduras no es un tema novedoso, existe poca información al respecto en el país y su regulación continúa siendo un problema especialmente para evitar la comercialización ilegal de bases de datos. Por esta razón, esta investigación tiene un alcance exploratorio.

### *3.5.2 Alcance descriptivo*

Los estudios de alcance descriptivo se basan en estudios exploratorios para medir conceptos y definir variables. “Busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis” (Hernández et al., 2014, p. 92). Es decir, que solamente se busca recolectar información para describir el problema, sin indicar relaciones o dar explicaciones.

Esta investigación tiene un alcance descriptivo al pretender recolectar información para mostrar los mecanismos de protección de datos personales para evitar la comercialización ilegal de bases de datos en Honduras.

La siguiente tabla resume el doble alcance de esta investigación.

*Tabla 4. Alcances exploratorio y descriptivo.*

| | **Exploratorio** | **Descriptivo** |
|---|---|---|
| **Propósito** | Estudiar la situación y los mecanismos legales actuales que regulan la protección de datos personales en Honduras para evitar la comercialización ilegal de bases de datos por parte de entes comerciales privados. Asimismo, estudiar el anteproyecto de ley que hubo para su regulación especial. | Establecer los diferentes mecanismos de protección de datos personales para evitar la comercialización ilegal de datos personales, estableciendo diferencias con una protección proveniente de una posible regulación especial |

| | | |
|---|---|---|
| | | (anteproyecto de ley). Identificar y describir la subsecuente deducción de responsabilidad por parte de entes comerciales privados que contravengan estas disposiciones. |
| **Utilidad** | Conocer la situación y los mecanismos legales actuales que regulan la protección de datos personales para evitar la comercialización ilegal de bases de datos y deducir responsabilidad de entes comerciales privados que la quebranten en Honduras, así como el anteproyecto de ley para su regulación especial. | Se podrá demostrar la necesidad y aplicabilidad de una regulación especial para la protección de datos personales para garantizar el derecho a la intimidad y privacidad de los usuarios. |
| **Relación con otros estudios** | Se tomarán como base estudios previos y teorías relacionadas con la protección de datos personales. | El resultado de la investigación podrá servir de base para estudios |

| | | |
|---|---|---|
| | | correlacionales o explicativos posteriores. |
| **Meta de la investigadora** | Investigar un problema poco estudiado desde una perspectiva innovadora. | Describir los mecanismos de protección de datos personales para evitar la comercialización ilegal de bases de datos en Honduras. |

*Fuente: Elaboración propia con base en (Hernández, Sampieri, 2014).*

### 3.6 Métodos de investigación

Generalmente por métodos se entienden los "procedimientos para alcanzar nuevos conocimientos, reglas específicas para investigar, caminos para producir nuevos conocimientos" (Mejía, 2006, p. 166). Sin embargo, concretamente en el campo jurídico se puede entender por "interpretar y procedimiento de investigación por reglas metodológicas" (Mejía, 2006, p. 166), aludiendo a reglas metodológicas y de interpretación particulares del derecho.

A continuación, se describen los principales métodos de investigación jurídica, habiéndose escogido para la realización de esta investigación el método inductivo, el intuitivo, el derecho comparado y sistemático.

### *3.6.1 Método inductivo*

El método inductivo sigue el proceso de inducción que va de lo particular a lo general, es decir que parte de situaciones específicas para inducir regularidades validas o aplicables a casos similares, sin tomar en cuenta lo relativo o cambiante (Villabella Armengo, 2015, p. 938). De esta manera se logra establecer conclusiones en los estudios cualitativos.

Al respecto, Villabella (2015) aclara que "en la ciencia jurídica – en donde las investigaciones cualitativas tienen presencia –, la inducción, como forma de razonamiento, posibilita construir teoremas desde situaciones particulares y casos concretos, establecer regularidades, generalizar y pautar conclusiones" (p. 983) .

Ponce (1996) considera que al analizar varios casos y objetos jurídicos con este método, se puede llegar a una conclusión general (p. 69).

### *3.6.2 Método intuitivo*

Este método de investigación jurídica tiene su sustento en la intuición, del verbo intuir que significa mirar. Consiste en aprender o capturar directamente el objeto de estudio, dando como resultado una primera aproximación o verdad que luego se puede someter a otros métodos (Ponce, 1996, pp. 66–67).

### *3.6.3 Método histórico*

El método histórico "permite enfocar el objeto de estudio de un decurso evolutivo destacando los aspectos generales de su desarrollo, las tendencias de su progreso, las etapas de desenvolvimiento, y sus fundamentales y causas" (Villabella, 2015, pp. 936–937).

Con este método de investigación es posible entender un comportamiento histórico para explicar sus características actuales, por lo que tiende a ser útil para un análisis evolutivo del objeto y para una valoración retrospectiva de este (Villabella, 2015, p. 937).

### *3.6.4 Método de derecho comparado*

El método de derecho comparado es un método de investigación propio de la ciencia jurídica. Este método permite cotejar dos objetos jurídicos del mismo dominio para destacar semejanzas y diferencias, establecer clasificaciones, descubrir tendencias y revelar modelos exitosos. Estos objetos jurídicos pueden ser conceptos, instituciones, normas, procedimientos, etc (Villabella, 2015, p. 940).

La doctrina (Villabella Armengo, 2015) clasifica la comparación jurídica en interna si los objetos pertenecen a un mismo ordenamiento jurídico; externa si son de ordenamientos jurídicos diferentes; técnica- concretizadora si se estudian como productos lingüísticos, a un nivel textual y desde el punto de vista técnico; y sociológica-jurídica si la comparación se realiza como parte de una red de condicionantes socio históricos y culturales.

### *3.6.5 Método dialéctico*

El método dialéctico consiste en “la confrontación de ideas a través de la exposición de tesis, y el surgimiento de antítesis o tesis contrarias, para el efecto de llegar a la síntesis” (Ponce, 1996, p. 70).

### *3.6.6 Método sistémico*

El método sistémico, también conocido como sistémico- estructural- funcional, permite estudiar un objeto en el contexto de una estructura compleja en la que se integra,

formada por diferentes subsistemas que tienen características y funciones específicas interactuantes (Villabella, 2015, p. 939). Con este método se ordenan el conocimiento al agruparlo en sistemas coherentes.

Este método desestructura un objeto en partes para estudiar cada una, determinando su papel, aclarando la jerarquización y apreciando la dinámica de funcionamiento. Es un método útil cuando el objeto de estudio forma parte de un sistema (Villabella, 2015, p. 939).

### *3.6.7 Método hermenéutico*

La palabra "hermenéutica" viene del vocablo griego hermeneutiké, que a su vez viene de Hermes, el mensajero de los dioses en la mitología griega. Su empleo significaba entender e interpretar el mandato de las deidades. El método hermenéutico permite entender significados del objeto de estudio a partir de descifrar el contexto lingüístico y los cánones psicológicos de quien los produce (Villabella, 2015, p. 944).

Este método resulta válido en las ciencias jurídicas cuando se estudian normas jurídicas, debiéndose tomar en cuenta cuatro variables: gramatical, teleológica, histórica y sistemática. La variable gramatical se refiere al significado literal del enunciado. La variable teleológica destaca la relación entre el objeto de estudio y su ratio, específicamente su finalidad o propósitos. La variable axiológica destaca los principios éticos que sostienen la norma objeto de estudio. Finalmente, la variable histórico trata del entorno histórico-cultural que dio origen a la norma, es decir de las razones que motivaron al legislador y el comportamiento evolutivo de la norma (Villabella, 2015, pp. 944–945).

### 3.7 Diseño de la investigación

Hernández et. al. (2014) definen el diseño de la investigación como el "plan o estrategia concebida para obtener información que se desea con el fin de responder al planteamiento del problema" (p. 128). Esta investigación tiene un diseño no experimental y cualitativo de la teoría fundamentada.

Los diseños de investigación pueden ser experimental y no experimental. En una investigación experimental se diseñan pruebas y se inducen cambios o manipulan las variables. (Olvera, 2015, p. 114- 115).

Con relación al diseño no experimental, Hernández et. al. (2014, p. 152) indican que, en este tipo de investigación, las variables independientes ocurren sin que la investigadora pueda manipularlas, es decir que no tiene control ni puede influir sobre ellas porque ya sucedieron, al igual que sus efectos (p. 152). Esta investigación es no experimental ya que, considerando que es un análisis de algo que ya sucedió, la investigadora no puede manipular deliberadamente las variables.

Este estudio tiene un diseño cualitativo de teoría fundamentada, "lo cual significa que la teoría (hallazgos) va emergiendo fundamentada en los datos" (Hernández et al., 2014, p. 422). Este diseño es útil cuando no se disponen de teorías o las existentes no son adecuadas para estudiar el fenómeno. Proporcionará información sobre las categorías del fenómenos y sus vínculos, así como una teoría que lo explica o responde al planteamiento (Hernández et al., 2014, p. 471).

### *3.7.1 Población*

Se entiende por población o universo al "conjunto de todos los casos que concuerdan con determinadas especificaciones" (Hernández et al., 2014, p. 174). El conjunto que integra la población de esta investigación está formado por los entes privados en Honduras que se dedican al comercio y los usuarios que les proporcionan sus datos personales.

### *3.7.2 Muestra*

La muestra se refiere a un segmento de entre todo el universo de observación (población) sobre el cual se realizará el estudio. Es un grupo representativo de la población al cual se le aplicarán las entrevistas, encuestas, cuestionarios, pruebas, etc., con el objetivo de obtener los datos requeridos por la investigación (Olvera, 2015, p. 64 y 127).

Hernández et al. (2014) definen la muestra en el proceso cualitativo como el "grupo de personas, eventos, sucesos, comunidades, etc., sobre el cual se habrán de recolectar los datos, sin que necesariamente sea estadísticamente representativo del universo o población que se estudia" (p. 384).

Vale la pena mencionar, que siendo esta una investigación cualitativa, "no se pretende generalizar los resultados obtenidos en la muestra a una población" (Hernández et al., 2014, p. 12). El muestreo en esta investigación será de tipo no probabilístico o dirigido, es decir que supone un procedimiento de selección orientado a las características de la investigación. Este tipo de muestreo es de gran valor en los estudios cualitativos al no interesar tanto que sea posible generalizar los resultados, pues logran obtener los casos que le interesan a la investigadora (Hernández et al., 2014, p. 189).

Los tipos de muestras no probabilísticos empleados en esta investigación fueron: a) muestras diversas (aplicación de encuestas a 333 usuarios en general); b) muestras teóricas o conceptuales (estudio comparativo de los mecanismos legales de protección de datos personales incluyendo 10 regulaciones internas de entes comerciales privados); y c) muestra de expertos (entrevistas no estructuradas con 2 expertos).

### *3.7.3 Unidad de análisis*

La unidad de análisis indica quiénes serán medidos, en otras palabras, los participantes o casos a quienes se les aplicará el instrumento de medición (Hernández et al., 2014, p. 183). Estos pueden ser personas, organización es, periodos, comunidades, procesos, significados, situaciones, etc.

La unidad de análisis de esta investigación es:

a. Usuarios que otorgan sus datos personales a entes comerciales privados (personas físicas).
b. Mecanismos legales de protección de datos personales (procesos).

## 3.8 Fuentes de información

### *3.8.1 Fuentes primarias*

Las fuentes primarias son las que proporcionan datos de primera mano ya que son documentos que incluyen resultados de los estudios correspondientes. Algunos ejemplos de fuentes primarias son libros, artículos de publicaciones periódicas, monografías, tesis, disertaciones, documentos oficiales, reportes de asociaciones, testimonios de expertos, documentales, foros, páginas de internet, entre otras (Hernández et al., 2014, p. 72).

En la presente investigación, las fuentes primarias son las encuestas y entrevistas realizadas a la muestra seleccionada, la Constitución de la República de Honduras, la Ley sobre Justicia Constitucional, los reglamentos o regulaciones de los entes públicos seleccionados, legislación comparada internacional, libros, tesis, revistas académicas, noticias y reportes de asociaciones.

### *3.8.2 Fuentes secundarias*

Las fuentes secundarias tienen información primaria, sintetizada y/o reorganizada. En esta investigación las fuentes secundarias son foros de internet, diccionarios, enciclopedias jurídicas, videos, comentarios de expertos, entre otros.

## 3.9 Técnicas e instrumentos de recolección de información

Para la realización de la investigación es necesario definir las técnicas e instrumentos que se utilizarán para medir las variables o dar respuesta a la pregunta general de investigación. La mayoría de los instrumentos se deben de construir de acuerdo con las variables de investigación que se quieren medir. Luego de ser diseñados, estos se aplican a la muestra seleccionada para obtener los datos que se presentarán y analizarán (Olvera, 2015, p. 118).

Los instrumentos utilizados en esta investigación son:

1. **Encuestas:** Se define encuesta como la "búsqueda sistemática de información en la que el investigador pregunta a los sujetos sobre los datos que desea obtener para luego acumular esos datos individuales y realizar con ellos una evaluación" (Olvera, 2015, p. 120).

La encuesta se realiza a partir de un cuestionario creado por la investigadora para conocer la opinión o perspectiva que tiene la muestra de la población respecto a la situación de protección de sus datos personales.

2. **Investigación documental:** Es la revisión específica y crítica de las fuentes documentales. En esta investigación se realiza un análisis de los mecanismos legales existentes en el marco jurídico hondureño para regular la responsabilidad de los entes comerciales privados frente a la comercialización ilegal de bases de datos personales. Se utilizan regulaciones en el marco jurídico ordinario, así como regulaciones y reglamentos propios de entes comerciales privados.
3. **Entrevistas no estructuradas:** Una entrevista es una conversación entre dos o más personas sobre un tema específico que sigue ciertos esquemas o pautas. Al ser no estructuradas, son flexibles y se pueden ir incorporando temas de interés que vayan surgiendo con las respuestas de los entrevistados (Olvera, 2015, p. 121).

   Para esta investigación se entrevistarán expertos en la materia de protección de datos personales que darán su opinión respecto a los aciertos y vacíos para la aplicación del anteproyecto de Ley de Protección de Datos Personales.

### 3.10 Limitantes del estudio

Esta investigación pretende analizar el fenómeno de la protección de datos personales para evitar la comercialización ilegal de bases de datos y la subsecuente deducción de responsabilidad de entes públicos que la contravengan. El tema es novedoso y actualmente no se encuentran contemplados en la legislación hondureña, mecanismos específicos que

regulen el uso de datos personales por parte de entes comerciales privados, por lo cual podría existir un desconocimiento del tema y una falencia de cifras y datos específicos.

Se han identificado limitaciones propias de la pandemia de la Covid-19 y las medidas de confinamiento, que dificultan la realización de encuestas, entrevistas y obtención de información de manera presencial. Será más conveniente realizar estas a través de plataformas virtuales, que son prácticas, pero limitan el contacto y la interacción. Además, limita la obtención de regulaciones internas a las publicadas en línea por algunas empresas.

Adicionalmente, es importante mencionar la limitante del tiempo, siendo que el tiempo total para la realización de esta investigación es de aproximadamente seis meses.

# CAPÍTULO IV

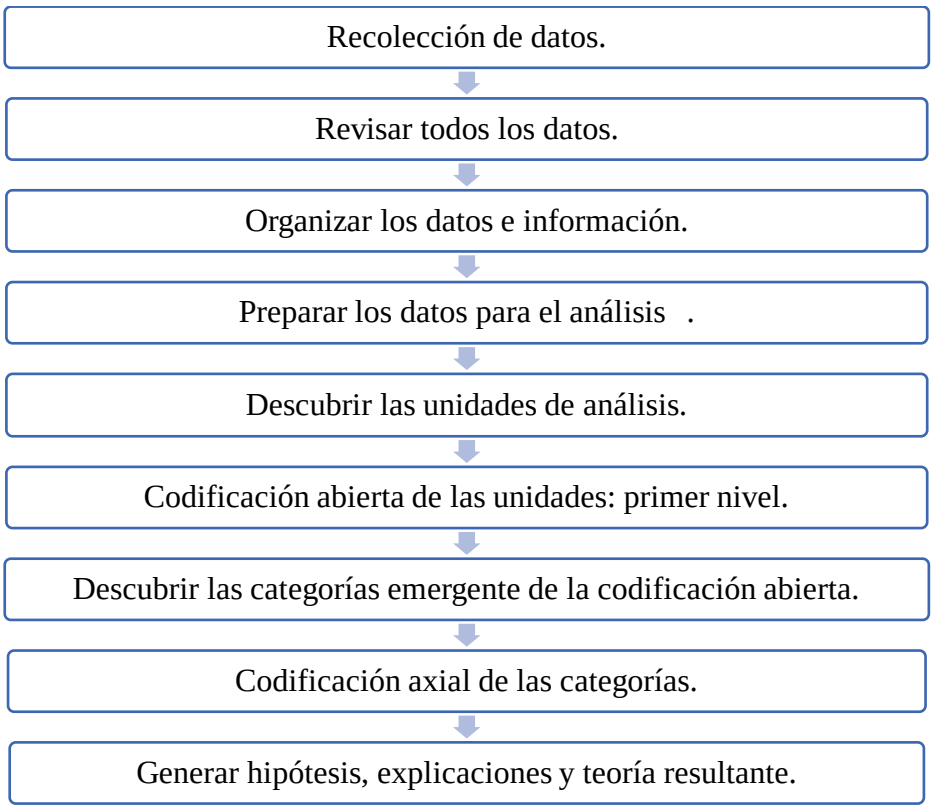
# 4. RESULTADOS Y ANÁLISIS

El corpus de esta investigación pretende proponer un mecanismo legal que garantice la protección de datos personales de la comercialización ilegal de bases de datos y la subsecuente deducción de responsabilidad a los entes comerciales privados que quebranten dicha protección.

El análisis de resultados es el aspecto más importante de la investigación e implica "interpretar los hallazgos relacionados con el problema de investigación, los objetivos propuestos, la hipótesis y/o preguntas formuladas y las teorías o presupuestos planteados en el marco teórico, con la finalidad de evaluar si confirman las teorías o no" (Bernal, 2010, p. 220).

Esta investigación tiene un diseño cualitativo de la teoría fundamentada, por lo que la teoría va surgiendo fundamentada en los datos. Se debe interpretar por separado los resultados que proporciona cada instrumento utilizado. Hernández et al. (2014) indican que en la mayoría de los estudios cualitativos se codifican los datos en dos niveles, la codificación abierta que es en categorías y codificación axial y selectiva, que comparan categorías para agruparlas y encontrar posibles agrupaciones (p. 426).

*Figura 2. Proceso de análisis cualitativo para generar categorías.*




*Fuente: Elaboración propia con base en Hernández et al. (2014, p. 423).*

Definida las metodologías: encuestas, investigación documental, se procedió a aplicar los instrumentos correspondientes y seguidamente a realizar el tratamiento para el análisis de estos.

### 4.1 Análisis de encuestas

Antes de proceder al análisis de encuestas, es menester resaltar que esta investigación tiene un enfoque cualitativo y aunque se ha utilizado las encuestan como instrumento, esta tiene una finalidad descriptiva y no se pretende generalizar los resultados obtenidos en la muestra a una población.

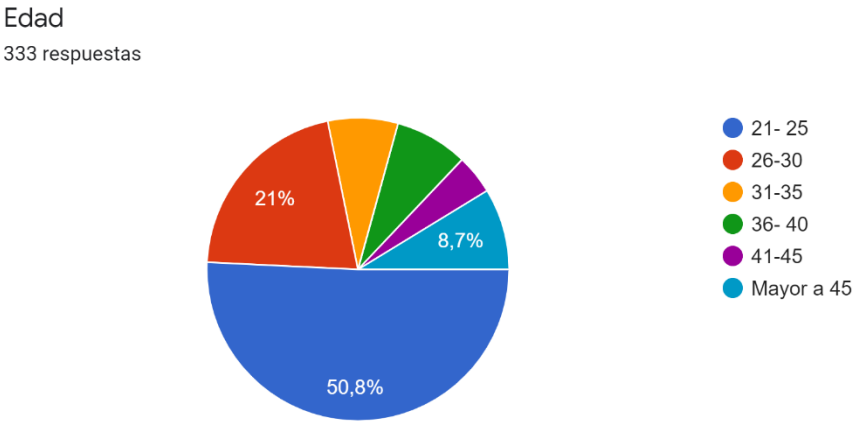
La encuesta fue aplicada a 333 personas a través de la plataforma virtual Google Forms. La encuesta constó de 4 preguntas de perfil de muestra y 8 preguntas con la intención de evaluar la percepción de la población hondureña sobre la protección de su información personal frente a la comercialización no autorizada de sus datos por entes comerciales privados.

A continuación, se procedió a realizar un proceso de análisis descriptivo de los resultados a través de los siguientes gráficos y tablas que sintetizan los datos obtenidos:

### *4.1.1 Análisis individual de las respuestas de la encuesta aplicada*

El perfil de muestra en la encuesta indica que el 57.4% de los encuestados, es decir 191 de estos, fueron representados por mujeres, mientras que el 42.6% (142) por hombres. Es necesario recalcar que este no será un factor que altere los objetivos planteados en esta investigación.

*Figura 3. Edad de los encuestados.*

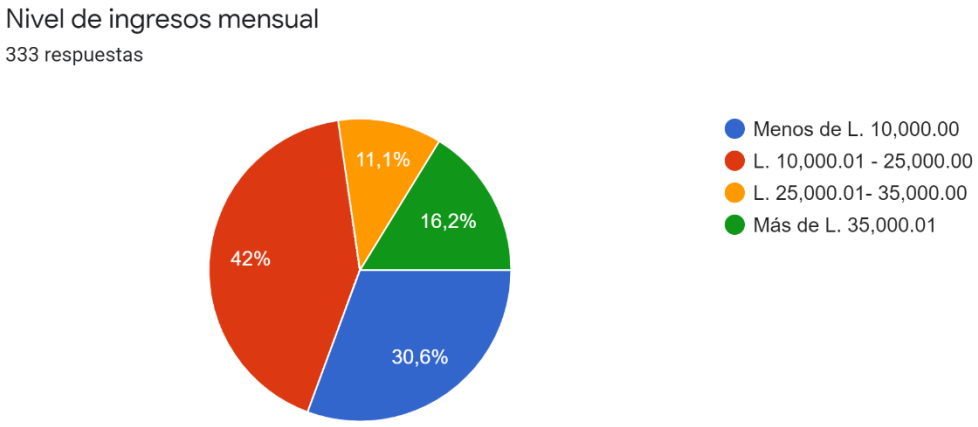



Con relación a la edad de las personas encuestadas, vale la pena aclarar que este instrumento fue dirigido a hondureños mayores de edad. Se aprecia que las edades

comprendidas entre 21- 25 años poseen un 50.8% (169 encuestados), es decir que la mitad de la muestra se concentra en estas edades. En segundo lugar, se ubica con un 21% (70) el grupo con edades entre 26 y 30 años. Le siguen el rango de edades de mayor a 45 con el 8.7% (29), de 36 – 40 con 7.8% (26), de 31- 35 con el 7.5% (25) y por último el rango de 41 – 45 años con el 4.2% (14).

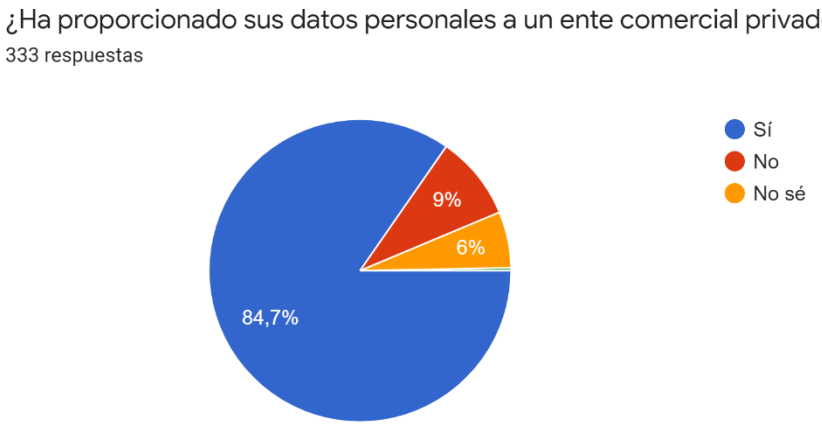
Respecto al nivel educativo de los encuestados, el 61.9% de los encuestados (206) tienen un nivel educativo de pregrado, el 36.3% (121) de postgrado y un 1.8% (6) de primaria.

*Figura 4. Nivel de ingresos de los encuestados.*



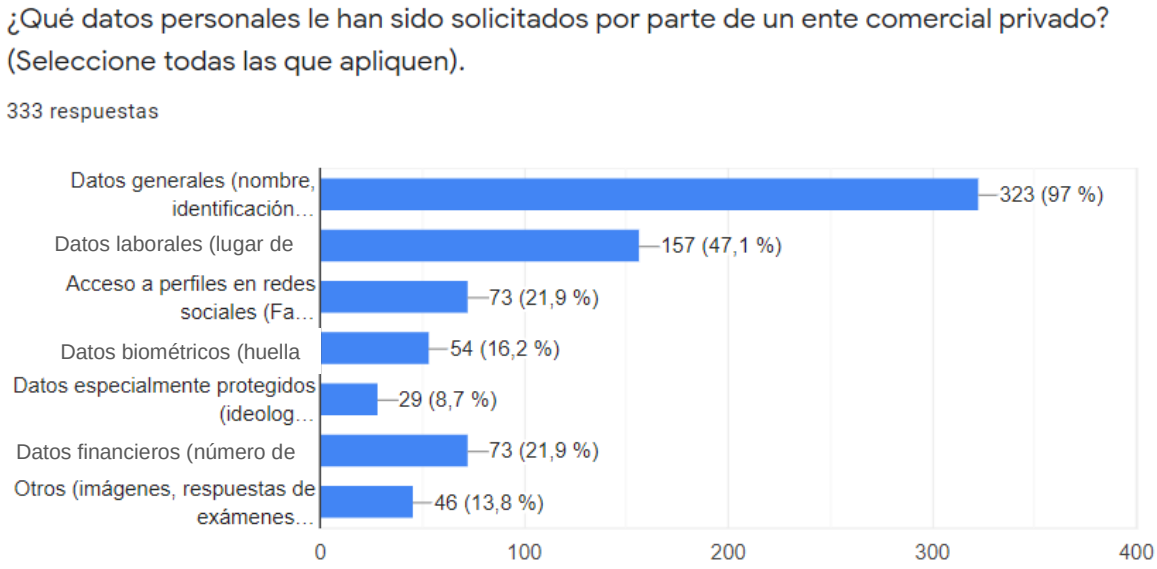

El 42% de los encuestados (140) tiene un ingreso mensual entre L. 10,000.01 y 25,000.00. Mientras que el 30.6% (102) se ubica en el rango de menos de L. 10,000.00. El 16.2% (54) de los encuestados recibe más de L. 35,000.01 al mes y el 11.1% recibe entre L. 25.000.01 y 35,000.00.

*Figura 5. Respuesta de los entrevistados sobre si han proporcionado sus datos personales a un ente comercial privado.*




La primera pregunta muestra que una mayoría considerable del 84.7% (282) de las personas encuestadas han proporcionado sus datos personales a un ente comercial privado, destacando que apenas un 9% (30) que no lo ha hecho. Los resultados también indican que un 6% (20) no sabe, es decir que no están seguras o no se han dado cuenta si en algún momento lo han hecho.

*Figura 6. Datos personales solicitados por entes comerciales privados a los entrevistados.*



Al analizar los datos obtenidos en la pregunta se puede concluir que a una gran mayoría de las personas encuestadas, el 97%, se les han solicitado datos generales como nombre, identificación personal, número de teléfono, correo electrónico, estado civil, domicilio, profesión y/o nacionalidad, entre otros, a entes comerciales privados.

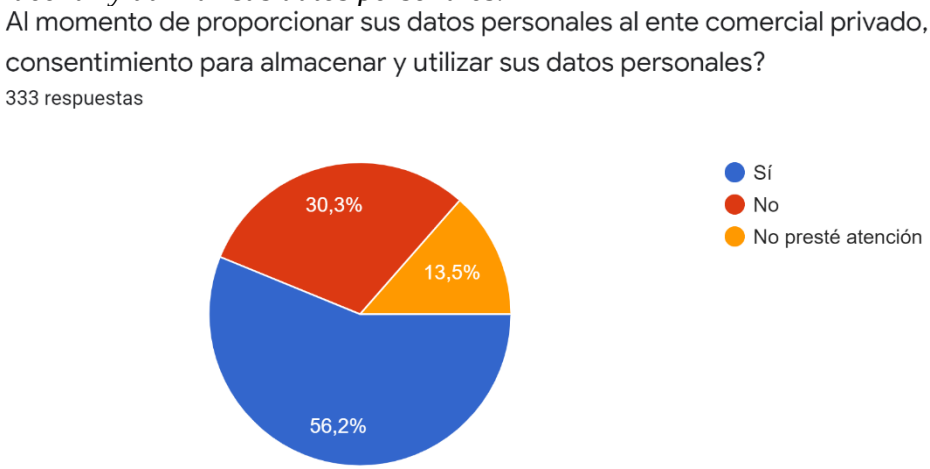
Luego, a un 47.1% le han solicitado datos laborales, por ejemplo, el lugar de trabajo, condiciones, registros, número de seguro social, dirección, etc. Seguidamente, al 21.9% de los encuestados un ente comercial privado les ha solicitado sus datos de acceso en perfiles de redes sociales y a un 21.9% sus datos financieros (por ejemplo, número de tarjeta de crédito/ débito, números de cuenta, ingresos, etc.) a entes comerciales privados.

Además, a un 16.2% de los encuestados les han solicitado sus datos biométricos a entes comerciales privados. Los datos biométricos pueden ser la huella dactilar, reconocimiento facial, del iris, de la geometría de la mano, reconocimiento de firma, retina, de escritura, de voz, de la forma de andar, etc. A un 13.8% le han solicitado otros datos como imágenes, respuestas de exámenes, ubicación geográfica, etc.

Destaca que entre los datos que los encuestados menos han otorgado se encuentran los considerados especialmente protegidos, como ser: ideología, afiliación política, sindical, religiosa, creencias, origen racial, salud y/o orientación sexual, entre otros. Estos datos son de gran importancia en la protección de datos personales y vale la pena hacer notar que solo un 8.7% de los encuestados respondió que se le han sido solicitados por un ente comercial privado.

De los resultados de esta pregunta es posible concluir que los datos personales más solicitado por entes comerciales privados son los datos generales, mientras que los menos solicitados son los considerados especialmente protegidos, lo cual se puede considerar positivo al ser estos últimos datos delicados que deberían tener una protección más rigurosa.

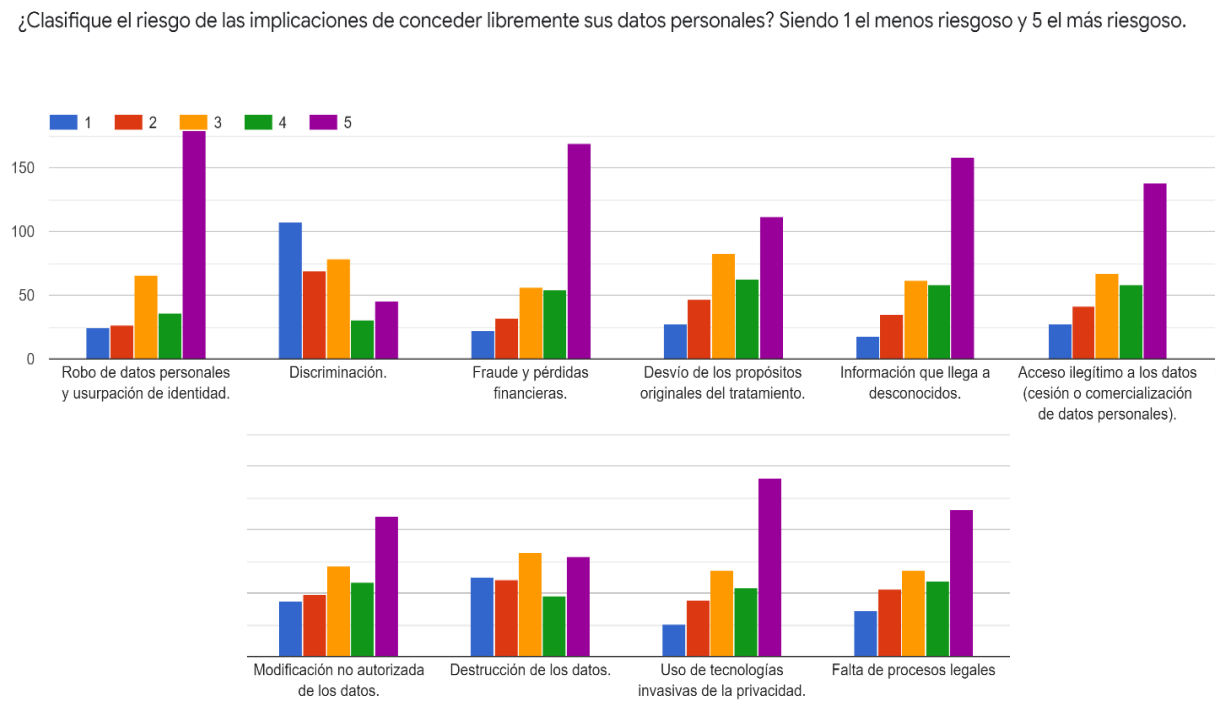
*Figura 7. Respuesta de los entrevistados sobre si se les solicitó o no su consentimiento para almacenar y utilizar sus datos personales.*




Los resultados indican que, a más de la mitad de los encuestados, un 56.2% (187), un ente comercial privado les ha solicitado su consentimiento para almacenar y utilizar sus datos personales al momento de proporcionárselos. Por otro lado, a un 30.3% (101) no les solicitaron su conocimiento.

Sin embargo, vale la pena resaltar que un 13.5% (45) de los encuestados no prestó atención, es decir que no se dio cuenta si el ente comercial privado le solicitó su conocimiento para este fin. Esto muestra que algunas de las personas encuestadas no están conscientes de la importancia de otorgar su consentimiento para almacenar y utilizar sus datos personales, y posiblemente tampoco conozcan los riesgos de esto.

*Figura 8. Respuesta de los entrevistados sobre el nivel de riesgo de las implicaciones de conceder libremente sus datos personales.*




Luego de observar las diversas opciones que ofrece el resultado, la apreciación obtenida fue que: el robo de datos personales y usurpación de identidad fue percibido por los encuestados como la implicación más riesgosa asociada a la libre concesión de sus datos personales, al ser clasificado en categoría 5 de “más riesgoso” por 180 encuestados (54.1%).

El siguiente cuadro resume los resultados de esta pregunta en las dos categorías que se consideraron más relevantes: más riesgos y menos riesgoso.

*Tabla 5. Clasificación de los entrevistados de las implicaciones de conceder libremente sus datos personales en "más riesgosos" y "menos riesgosos".*

| | Más riesgosos | | Menos riesgosos | |
|---|---|---|---|---|
| | **Implicación** | **Encuestados** | **Implicación** | **Encuestados** |
| **1** | Robo de datos personales y usurpación de identidad robo de datos personales y usurpación de identidad. | 180 (54.1%) | Discriminación. | 108 (32.4%) |
| **2** | Fraude y pérdidas financieras. | 169 (50.8%) | Destrucción de datos personales. | 63 (18.9%) |
| **3** | Información que llega a desconocidos. | 159 (47.7%) | Modificación no autorizada de los datos personales. | 44 (13.3%) |
| **4** | Uso de tecnologías invasivas de la privacidad. | 140 (42%) | Falta de procesos legales. | 36 (10.8%) |
| **5** | Acceso ilegítimo a sus datos personales a través de la cesión y/o comercialización de estos. | 138 (41.4%) | Acceso ilegítimo a sus datos personales a través de la cesión y/o comercialización de estos. | 28 (8.4%) |
| **6** | Falta de procesos legales. | 116 (34.8%) | Desvío de los propósitos originales de tratamiento. | 28 (8.4%) |
| **7** | Desvío de los propósitos originales de tratamiento. | 112 (33.6%) | Uso de tecnologías invasivas de la privacidad. | 26 (7.8%) |
| **8** | Modificación no autorizada de los datos personales. | 111 (33.3%) | Robo de datos personales y usurpación de identidad. | 24 (7.2%) |
| **9** | Destrucción de datos personales. | 79 (23.7%) | Fraude y pérdidas financieras. | 22 (6.6%) |
| **10** | Discriminación. | 46 (13.8%) | Información que llega a desconocidos. | 18 (5.4%) |

En la apreciación de “más riesgoso” le siguen respectivamente: fraude y pérdidas financieras siendo escogido 169 veces (50.8% de los encuestados), información que llega a desconocidos con 159 (47.7%), uso de tecnologías invasivas de la privacidad con 140 (42%) y el acceso ilegítimo a sus datos personales a través de la cesión y/o comercialización de sus datos personales con 138 (41.4% de los encuestados).

Los últimos tres lugares en la categoría “más riesgoso” los ocupan respectivamente: falta de procesos legales (116 que representan 34.8%), desvío de los propósitos originales de tratamiento (112 que representan 33.6%), modificación no autorizada de los datos personales (111 que representa 33.3%), destrucción de estos (79 que representa 23.7%) y al final, discriminación (46 que representa el 13.8%).

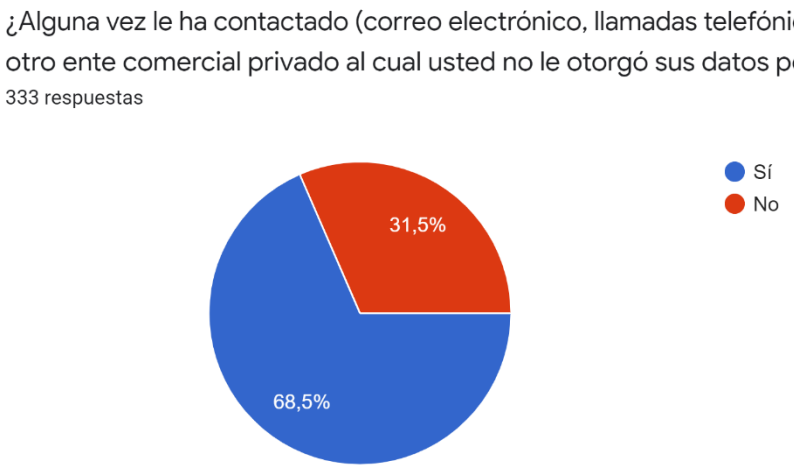
Resulta interesante que los resultados de esta pregunta, en la categoría “menos riesgosa” validan nuevamente los resultados obtenidos en la categoría “más riesgosa”. De esta manera, las tres implicaciones escogidas como “menos riesgosas” por los encuestados, es decir las más votadas, son: discriminación escogido por 108 encuestados (32.4%), destrucción de los datos personales por 63 (18.9%) y modificación no autorizada por 44 (13.3%). Estos resultados corresponden a las tres implicaciones menos escogidas para la categoría “más riesgosa”.

Más aún, las tres implicaciones menos escogidas como “menos riesgosas” por los encuestados son: información que llega a desconocidos por 18 (5.4%), fraude y pérdidas financieras por 22 (6.6%) y robo de datos personales y usurpación de identidad por 24 (7.2%). Aunque en diferente orden, estos resultados corresponden a las tres implicaciones más escogidas para la categoría “más riesgosa”.

Conviene subrayar, que en la categoría “menos votada”, el acceso ilegítimo a sus datos personales a través de la cesión y/o comercialización de estos, obtuvo 28 votos (8.4% de los encuestados), ubicándose en como un riesgo considerado medio por estos. De igual manera, en la categoría “más riesgoso”, esta se ubica como la quinta implicación más riesgosa según el 41.4% (138) de los encuestados.

Complementado lo anterior, la implicación de acceso ilegítimo a sus datos personales a través de la cesión y/o comercialización de estos obtuvo 58 votos (17.4%) en categoría 4, 67 (20.1%) en 3 y 42 (12.6%) en 2.

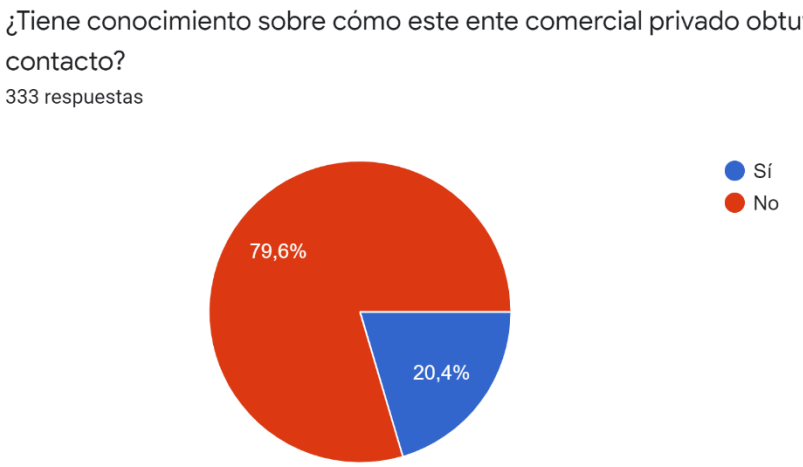
*Figura 9. Respuesta de los entrevistados sobre si han sido contactados por un ente comercial privado al cual no le otorgaron sus datos personales.*




Como se puede observar en la gráfica, al 68.5% (228) de los encuestados los han contactado un ente comercial privado al cual no le otorgaron sus datos de contacto. También se muestra que el 31.5% (105) de las personas encuestados no ha recibido este tipo de contacto.

Es decir, que la mayoría de los encuestados ha recibido correos electrónicos, llamadas, mensajes de texto u otro contacto de entes comerciales privados a los cuales no consintieron proporcionarles sus datos. Esta situación puede haberse producido por una cesión o comercialización de bases de datos por parte de otro ente al cual el usuario le otorgó sus datos anteriormente.

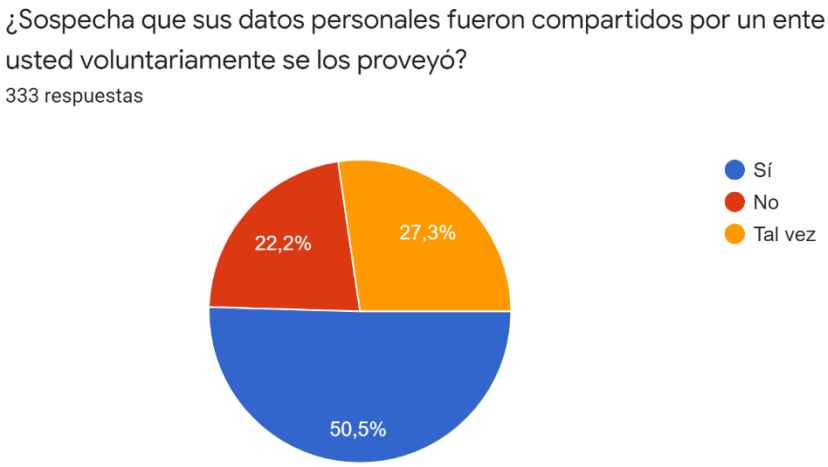
*Figura 10. Respuesta de los encuestados sobre si tienen conocimiento de cómo este ente comercial privado obtuvo sus datos personales.*




Continuando con el análisis de los resultados, en el gráfico se observa cómo el 79.6% de los encuestados (265 de estos) no sabe de qué forma un ente comercial privado obtuvo sus datos personales para contactarlo, quedando un 20.4% (68 encuestados) que si lo saben.

Esta falta de conocimiento acerca de cómo un ente que les contactó obtuvo sus datos personales podría deberse a que sus datos personales fueron compartidos, cedidos y/o comercializados en una base datos por parte de un ente al cual se los proporcionaron libremente. Esta actividad sería incorrecta si se realizó sin el consentimiento de los encuestados.

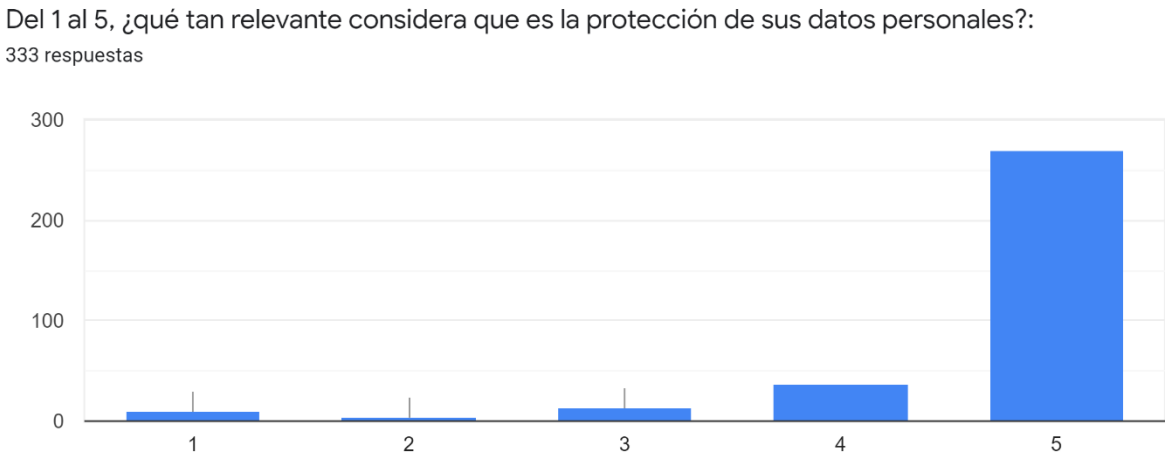
*Figura 11. Respuesta de los entrevistados sobre si sospechan que sus datos personales fueron compartidos por un ente comercial privado.*




El 50.5% de los encuestados, es decir 168 de estos, sospecha que sus datos personales fueron compartidos por un ente comercial privado al cual se los proveyeron voluntariamente. Además, el 27.3% (91 de los encuestados), considera que esta es una posibilidad al responder "tal vez". En cambio, 74 de los encuestados (22.2%) no sospecha que sus datos fueron compartidos por un ente comercial privado.

Este resultado muestra que existe en más de la mitad de los encuestados la sospecha de que los entes comerciales privados a los que les han dado sus datos personales comercializan o ceden sus bases de datos, y que de esta manera otros entes de este tipo logran contactarlos.

*Figura 12. Relevancia de la protección de datos personales para los entrevistados.*




Finalmente, este ítem tiene implícito parte de las aspiraciones de esta investigación, ya que señala la importancia que le dan los encuestados a la protección de sus datos personales. El 80.8% de los encuestados (269 de los 333) le dio la calificación máxima de 5, indicando que consideran muy importante la protección de sus datos personales. El 11.1% (37 encuestados) lo calificó en 4, el 3.9% (13) en 3 como importancia media, el 1.2% (4) en 2 y un 3% (10) lo calificó en 1.

Este resultado muestra que existe un a conciencia general en los encuestados respecto a la importancia de proteger sus datos personales al ubicarse la gran mayoría de las respuestas en una calificación alta para su relevancia.

### *4.1.2 Síntesis general de los resultados de la encuesta*

La encuesta aplicada tiene el objetivo de mostrar la percepción de los encuestados respecto a la protección de sus datos personales para evitar la comercialización ilegal de bases de datos por parte de entes comerciales privados.

Los resultados indican que una gran proporción de los encuestados (casi el 90.7% de estos) ha otorgado sus datos personales a entes comerciales privados y que prácticamente los datos que más otorgan son sus datos generales que incluyen los datos de contacto.

Con respecto a esto, llama la atención, que un poco más de la encuestados contestó que si se les pidió consentimiento para almacenar y utilizar sus datos personales. Sin embargo, el hecho que el 13.5% haya contestado que no prestó atención muestra que algunos entrevistados no están conscientes del riesgo que implica otorgar libremente sus datos personales.

Asimismo, los resultados indican que, a más de mitad de los encuestados, al 68.5%, los ha contactado un ente comercial privado al cual no le dieron sus datos personales, que el 79.6% no tiene idea de cómo este ente que los contactó obtuvo sus datos de contacto y que la mitad sospecha que sus datos fueron provistos por otro ente comercial privado al cual si le otorgaron sus datos personales. Este resultado es interesante al considerar que el 43.8% de los encuestados contestó que no le solicitaron su consentimiento o no prestaron atención al momento de otorgar sus datos personales.

El 80.8% de los entrevistados considera que es importante que estos datos estén protegidos y en cuanto al riesgo, la implicación de acceso ilegítimo a sus datos personales a través de la cesión y/o comercialización se ubicó prácticamente como un riesgo considerado medio por los entrevistados. Siendo las implicaciones más riesgosas: Robo de datos personales y usurpación de identidad, fraude y pérdidas financieras e información que llega a desconocidos.

## 4.2 Análisis de la investigación documental

La investigación de documentos es una herramienta valiosa en los estudios cualitativos que permite conocer los antecedentes. Para la investigación, es conveniente realizar una triangulación de datos que implica tener varias fuentes y métodos para recolectar los datos (Hernández et al., 2014, pp. 417–418).

### *4.2.1 Análisis del marco jurídico vigente*

El análisis del marco teórico de esta investigación indica que la legislación vigente que regula la protección de datos personales en Honduras se encuentra en la Constitución de la República, tratados internacionales, la Ley sobre Justicia Constitucional, la Ley de Transparencia y Acceso a la Información Pública, la Ley de Instituto de Acceso a la Información Pública.

Para el caso concreto de la presente investigación, solamente se analizará de manera comparativa, el marco jurídico hondureño vigente que regula la responsabilidad de entes comerciales privados frente a la comercialización no autorizada de bases de datos.

Se ha tomado en cuenta, la Constitución de la República (1982), que es la carta magna de Honduras, de donde emana todo el sistema jurídico del país, específicamente, donde se plasma primero el Derecho a la Protección de Datos Personales. En el caso de Honduras, se reconoce el derecho a la intimidad personal, a la inviolabilidad de las comunicaciones y la garantía del Hábeas Datas, por lo que se clasifica como un texto constitucional que no reconoce expresamente este derecho, pero que tiene disposiciones relacionadas que han permitido a los tribunales reconocer este derecho fundamental (Rodríguez, 2015, p. 61).

Los artículos de la Constitución aplicables son el 76, el 100 y el 182. La comercialización ilegal de datos personales en bases de datos implica una violación al derecho a la intimidad personal y a la inviolabilidad de las comunicaciones.

Por otro lado, la garantía del Hábeas Data se refiere directamente al derecho de acceso a la información pública y privada, sirviendo como un mecanismo procedimental que una autoridad jurisdiccional puede aplicar de forma inmediata para hacer cesar cualquier violación contra el honor, intimidad personal o familiar y la propia imagen (López, 2014). En este sentido, el Hábeas Data es la garantía que se aplica en caso de una violación al Derecho a la Protección de Datos Personales, como lo es la comercialización ilegal de datos personales.

Adicionalmente y considerando que el texto de los Tratados Internacionales pasa a formar parte del derecho interno al ser ratificado, se han tomado en cuenta 3 tratados internacionales de derechos humanos de los cuales Honduras es parte: el Pacto Internacional de Derechos Civiles y Públicos (1966), la Declaración Americana de los Derechos y Deberes del Hombre (1948) y la Convención Americana sobre Derechos Humanos (1969). En todos estos instrumentos, se reconoce junto al derecho a la intimidad, a la honra y a la dignidad, el Derecho a la Protección de Datos Personales, como un derecho fundamental y un derecho humano al ser uno personalísimo que todas las personas adquieren al nacer (Villan, 2018). Incluso se llama a la protección por parte de las autoridades en caso de inherencias en la vida privada. Sin embargo, esta, al igual que la constitución, no trata directamente el tema de la comercialización ilegal de datos personales, siendo estas, regulaciones generales.

Se consideró la Ley sobre Justicia Constitucional (2004), ya que esta desarrolla las garantías constitucionales enunciadas en la Constitución de la República. Esta ley reguló la acción de Hábeas Data junto al Hábeas Corpus, expresando en artículo 13, que se aplica a registros públicos y privados, como los de los entes comerciales privados; y que del Hábeas Data solo puede conocer la Sala de lo Constitucional, lo cual Tomé (2019, p. 3) critica, ya que esto limita el acceso de la población a este recurso (p. 3). Brewer-Carías, (2016) considera que esta garantía busca asegurar "el acceso a la información; impedir su transmisión o divulgación, rectificar datos inexactos o errores; actualizar información; exigir confidencialidad y la eliminación de información falsa (…)" (p. 66). Esta normativa no regula ni trata la comercialización de datos personales en bases de datos.

Finalmente, se analizaron las disposiciones contenidas en el Código Penal (Congreso Nacional, 2019) como parte de la normativa ordinaria de Honduras. Este código en su capítulo II regula los delitos de violación y divulgación de secretos, determinando los supuestos del delito y sus respectivas penas.

Primero tipifica en el artículo 272, el delito de "descubrimiento y revelación de secretos" para quienes acceden por cualquier medio a datos (entre otros), para conocer los secretos o vulnerar la intimidad de otro sin su consentimiento, determinando una pena de prisión por uno (1) a tres (3) años más una multa de 360 a 720 días. Luego, agrega en este mismo delito a quienes sin autorización y perjudicando a un tercero, se apoderan, altera o utiliza datos personales en cualquier registro público o privado y sin importar la forma, determinando una pena de prisión de dos (2) a tres (3) años y la misma multa. Este artículo también determina un castigo más severo para quienes difundieron, revelaron o cedieron los

datos, con una pena de prisión por dos (2) a cuatro (4) años y una multa mayor de 360- 1,000 días. Incluso incluye a quienes, sin saber del origen ilícito de los datos, participan del delito, determinando una pena menor de prisión por seis (6) meses a un (1) año y multa de 100- 500 días.

Adicionalmente, el Código Penal (Congreso Nacional, 2019) en el mismo capítulo indica los agravantes específicos aplicables al artículo mencionado, determinando un aumento de un tercio (1/3) cuando la conducta es realizado por los responsables de los datos, afectan datos sensibles, afectan a un menor de 18 años o persona discapacitada y cuando se realizan con fines lucrativos, como lo es la comercialización de bases de datos personales.

A consecuencia de este objeto de estudio, se ha excluido del presente análisis la Ley de Transparencia y Acceso a la Información Pública y la Ley del Instituto de Acceso a la Información Público, las cuales son eminentemente del ámbito público. Estás regulaciones obligan a los tres poderes del Estado, así como Organizaciones No Gubernamentales, Organizaciones Privadas de Desarrollo y personas naturales y jurídicas que administren o reciban fondos públicos (López, 2014), más no a entes comerciales privados que no estén recibiendo o administrando estos fondos.

El siguiente cuadro sirve de resumen para lo explicado anteriormente:

*Tabla 6. Cuadro resumen sobre el marco jurídico vigente en Honduras que regula la responsabilidad de entes comerciales privados para evitar la comercialización ilegal de datos personales.*

| Legislación | Artículos | Análisis y/o comentarios |
|---|---|---|
| **Constitución de la República de Honduras (1982)** | Artículo 76: "Se garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen" (p.67). | Reconoce el derecho a la intimidad personal y a la inviolabilidad de las comunicaciones. La comercialización ilícita de bases de datos implica una violación a la intimidad personal.<br><br>El Hábeas Data es la garantía que se aplica en caso de una violación a la intimidad, incluida a la Protección de Datos Personales, como lo es la comercialización ilegal de datos personales. |
| | Artículo 100: "Toda persona tiene derecho a la inviolabilidad y al secreto de las comunicaciones, en especial de las postales, telegráficas y telefónicas, salvo resolución judicial" (p. 71). | |
| | Artículo 182: (…) Hábeas Data. Toda persona tiene el derecho de acceso a la información sobre si misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros Públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o suprimirla. No podrá afectarse el secreto de las fuentes de información periodística. (p.87). | |
| **Pacto Internacional de Derechos Civiles y Públicos (1966)** | Artículo 17: 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.<br>2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques. | Como en la Constitución, en estos se reconoce el Derecho a la Protección de Datos Personales, como un derecho fundamental y un derecho humano al ser uno personalísimo que todas las personas adquieren al nacer (Villan, 2018).<br><br>Incluso se llama a la protección por parte de las autoridades en caso de inherencias en la vida privada.<br><br>Junto a la Constitución, representan disposiciones generales, no específicas |
| **Declaración Americana de los Derechos y Deberes del Hombre (1948)** | Artículo V: "toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar". | |
| **Convención Americana** | Artículo 11: Protección de la Honra y de la Dignidad. | |

| | | |
|---|---|---|
| **sobre Derechos Humanos (1969)** | 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.<br>2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.<br>3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques. | sobre la responsabilidad de entes comerciales privados frente a la comercialización de datos personales en bases de datos. |
| **Ley sobre Justicia Constitucional (2004)** | Artículo 13. (…)<br>2.El Hábeas Data:<br>Toda persona tiene el derecho a acceder a la información sobre si misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o enmendarla.<br>Únicamente conocerá de la garantía de Hábeas Data la Sala de lo Constitucional de la Corte Suprema de Justicia. (p. 109) | Regula mínimamente la acción de Hábeas Data indicando que se aplica a registros privados, como los de los entes comerciales privados; y que del Hábeas Data solo puede conocer la Sala de lo Constitucional, lo cual Tomé (2019, p. 3) critica, ya que esto limita el acceso de la población a este recurso (p. 3).<br>Además, indica las formalidades y el procedimiento a seguir para interponer la acción de Hábeas Data.<br>Esta normativa no regula ni trata la responsabilidad de entes comerciales privados frente a la comercialización ilegal de datos personales en bases de datos. |
| | Artículo 40. De la substanciación de la acción de Hábeas Data. - Aplicación Supletoria.<br>El recurso de Hábeas Data será interpuesto ante la Sala de lo Constitucional de la Corte Suprema de Justicia cuando se haya agotado el trámite administrativo correspondiente.<br>En la sustanciación del recurso que observará el procedimiento establecido para el Hábeas Corpus o exhibición personal.<br>Las disposiciones que regulan el recurso de exhibición personal o Hábeas Corpus, se aplicarán, en lo pertinente al procedimiento de Hábeas Data. (p. 116). | |
| **Código Penal (2019)** | Artículo 272.- Descubrimiento y Revelación De Secretos. Debe ser castigado con las penas de prisión de uno (1) a tres (3) años y multa de trescientos sesenta (360) a setecientos veinte (720) días, quien para conocer los secretos o <u>vulnerar la intimidad de otro y sin su consentimiento, desarrolla alguna de las conductas siguientes:</u><br>1) <u>Accede, por cualquier medio</u>, a sus documentos, papeles, <u>datos,</u> información en cualquier soporte o efectos personales; | Regula la responsabilidad penal de:<br>- Quienes acceden por cualquier medio a datos para conocer los secretos o vulnerar la intimidad de otro sin su consentimiento, (pena de prisión por uno (1) a |

| | | |
|---|---|---|
| | 2) Intercepta sus telecomunicaciones; o,<br>3) Usa artificios técnicos de escucha, transmisión, grabación o reproducción del sonido, la imagen o secuencia de imágenes.<br>Debe ser castigado con las penas de dos (2) a tres (3) años de prisión y multa de trescientos sesenta (360) a setecientos<br>veinte (720) días quien, en perjuicio de terceros y sin estar autorizado, accede, se apodera, altera o utiliza datos personales incorporados a ficheros, soportes, registros informáticos, electrónicos, telemáticos o a cualquier otro tipo de archivo o registro público o privado.<br>Quien difunde, revela o cede a terceros los secretos o imágenes captados conforme a los párrafos anteriores, debe ser castigado con las penas de prisión de dos (2) a cuatro (4) años y multa de trescientos sesenta (360) a mil (1,000) días.<br>Debe ser castigado con la pena de prisión de seis (6) meses a un (1) año y multa de cien (100) a quinientos (500) días quien, no habiendo participado en su descubrimiento, pero conociendo su origen ilícito, realiza la conducta recogida en el párrafo anterior. (p. 67). | tres (3) años más una multa de 360 a 720 días).<br>- Quienes sin autorización y perjudicando a un tercero, se apoderan, altera o utiliza datos personales en cualquier registro público o privado y sin importar la forma (pena de prisión de dos (2) a tres (3) años y la misma multa.<br>- Quienes difundieron, revelaron o cedieron los datos (pena de prisión por dos (2) a cuatro (4) años y una multa mayor de 360- 1,000 días).<br>- quienes, sin saber del origen ilícito de los datos, participan del delito (prisión por seis (6) meses a un (1) año y multa de 100- 500 días).<br>Los agravantes específicos (1/3) incluyen cuando se realizan con fines lucrativos, como lo es la comercialización no autorizada de bases de datos personales.<br><br>Quienes difunden, entregan o venden las bases de datos personales tienen la pena mayor, siendo la finalidad de lucro un agravante. |
| | Artículo 276.- Agravantes Específicas.<br>Las penas de los artículos anteriores se deben aumentar en un tercio (1/3), cuando concurra las circunstancias siguientes:<br>1) La conducta se realiza por las personas encargadas o responsables de los ficheros, soportes informáticos, archivos o registros;<br>2) Se afecta a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial<br>o vida sexual;<br>3) La víctima es un menor de dieciocho (18) años o una persona con discapacidad necesitada de especial protección; o,<br>4) Los hechos se realizan con fines lucrativos. (pp. 67-68). | |

### *4.2.2 Análisis sobre la eficacia para evitar la comercialización ilegal de bases de datos de la regulación actual en Honduras*

Se considera el derecho europeo sobre Protección de Datos Personales como un referente en la materia, ya que cuenta con estándares altos y modernos que están sirviendo como base para esta regulación a nivel mundial (López-Torres, 2014, p. 103). Es por esta razón que para esta investigación se ha decidido utilizar las disposiciones en el Reglamento General de Protección de Datos o RGPD (2016) como estándar para determinar la eficacia de la aplicación de la actual normativa hondureña sobre protección de datos personales para evitar la comercialización ilegal de bases de datos.

Según el RGPD, para que la comercialización de datos personales en bases de datos se considere legal, se debe demostrar que la información se obtuvo conforme a los siguientes criterios:

1. Consentimiento previo, específico e inequívoco del titular, que debe de incluir la posibilidad de transmitir estos datos a otro destinatario con los fines de la transmisión, así como asegurarse que los datos están actualizados.
2. Considerar los intereses del tratamiento, que deben ser legítimos.
3. Notificar al dueño de los datos en la primera comunicación que se obtuvieron sus datos para tales fines (Comisión Europea, n.d.).

Respecto al segundo requisito, según el artículo 5 del RGPD (2016), el interés del interesado se considera legítimo si cumple una o más de las siguientes seis condiciones de licitud para el tratamiento o cesión:

- que la cesión sea necesaria para la ejecución o desarrollo del contrato,
- que constituya una obligación legal para el cedente,
- que obedezca intereses legítimos del responsable o terceros a los que se le comunican los datos, y/o
- que sirva para salvaguardar el interés vital del interesado u otros (p. 36).

Para determinar la eficacia de la regulación actual, y considerando la ausencia de una legislación especial sobre el tema, se analizaron las políticas de cesión de datos que estipulan 10 entes comerciales privados en Honduras en sus políticas de privacidad, con el fin de determinar si esta aplicación cumpliría con los 3 requisitos que exige el RGPD europeo para considerar una cesión lícita.

Se escogieron 2 entes comerciales privados del rubro de telecomunicación, 2 de distribución, 2 farmacias, 2 supermercados, 1 universidad y 1 servicio de envíos.

La información fue organizada en un cuadro matriz donde se nombra el ente comercial privado; las disposiciones de su política sobre cesión de datos que fueron consideradas; el cumplimiento de los tres requisitos del RGPD y finalmente una columna para comentarios del investigador sobre el cumplimiento o incumplimiento de estos requisitos.

*Tabla 7. Cuadro de análisis sobre las Políticas de Privacidad de entes comerciales privados hondureños según la regulación del RGPD europeo.*

| # | Ente Comercial Privado | Disposición Considerada | Consentimiento previo, específico e inequívoco del titular (1) | Interés legítimo del tratamiento (2) | Obligación de notificar al titular sobre la obtención (3) | Comentarios |
|---|---|---|---|---|---|---|
| **1** | **TIGO Honduras (**Navega S.A. de C.V., Dinelsa S.A. y Telefónica Celular S.A. de C.V.) (2021) | 5. ¿Con quién compartimos sus datos personales?<br>Tigo puede comunicar o transferir sus datos personales a terceros proveedores (por ejemplo, para almacenamiento y/o análisis de datos), a otras entidades de Tigo, o en caso de una fusión, adquisición, venta de activos de la compañía o transición del servicio a otro proveedor. (…)<br>El uso, comunicación y transferencia de la información proporcionada se realizará respetando su confidencialidad. | No Cumple | Cumple | No Cumple | (1) No solicita el consentimiento específico e inequívoco del usuario para tratar los datos.<br>(2) Ejecución del contrato. Cumple, pero se considera una redacción muy amplia.<br>(3) No se encontró evidencia de este requisito. |
| **2** | **Claro Honduras (**Empresa | Uso de Información Personal.<br>La Información Personal recopilada por CLARO será administrada y utilizada para | No Cumple | Cumple | No cumple | Menciona expresamente que no |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Hondureña de Telecomunicaciones S.A.) (2017) | prestar a los Usuarios los Servicios que ofrece CLARO y que aquellos soliciten. Asimismo, CLARO y sus subsidiarias y/o afiliadas harán uso de los datos personales del Usuario para informar a este sobre los Servicios disponibles. CLARO y sus subsidiarias y/o afiliadas no podrán enajenar ni arrendar a terceros sus BASES DE DATOS de Usuarios. Sin embargo, en determinadas ocasiones CLARO y sus subsidiarias y/o afiliadas podrá contactar a los Usuarios en nombre de ciertos sitios Web relacionados con CLARO y sus subsidiarias y/o afiliadas para informarles sobre el lanzamiento de ofertas que pudieran ser de su interés. En dicho supuesto, la información personal del Usuario por ningún motivo será proporcionada a terceros. Asimismo, CLARO y sus subsidiarias y/o afiliadas podrán poner ciertos datos a disposición de sitios relacionados con CLARO y sus subsidiarias y/o afiliadas para facilitar la elaboración de análisis estadísticos, para el envío de correo electrónico o Newsletter. | | | | comercializará las bases de datos con terceros.<br><br>(1) No solicita el consentimiento específico ni inequívoco del usuario para tratar los datos.<br>(2) Ejecución del contrato. Indica claramente los propósitos en caso de cesión.<br>(3) No se encontró evidencia de este requisito. |
| **3** | **Jetstereo** (Jetstereo S.A.) (2015) | 4. La información de nuestros usuarios es importante para nosotros.<br>El acceso a tus datos puede estar disponible a terceros que proveen el soporte técnico para el mantenimiento y | No Cumple | Cumple | No Cumple | (1) No solicita el consentimiento específico ni |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | operación del sitio. Podemos divulgar la información que poseemos en casos relacionados al cobro de valores que se adeudan a nuestra empresa.<br>Queda autorizado JETSTEREO para compartir información con empresas del grupo ILP, así mismo en los caso que sea requerida por autoridad competente y/o cuando sea necesaria o apropiado la aclaración para proteger los derechos de JETSTEREO.<br>5. Usamos software de seguridad para proteger la confidencialidad de tus datos personales.<br>Nuestras prácticas son revisadas periódicamente para asegurarnos que sean acorde con las políticas de seguridad y confidencialidad. Las mismas se regulan y limitan el acceso de parte de los empleados a información confidencial, y restringen el uso y la divulgación de estos datos a personal no autorizado.<br>En caso que se requiera el servicio de envío se proporcionará información necesaria al agente encargado de realizar la entrega del producto(s) solicitado. | | | | inequívoco del usuario para tratar los datos.<br>(2) Ejecución del contrato, obligación legal y obedece intereses legítimos del responsable. Cumple, pero se considera una redacción muy amplia al no expresar los fines de compartir los datos con el grupo ILP.<br>(3) No se encontró evidencia de este requisito. |

| | | | | | | |
|---|---|---|---|---|---|---|
| **4** | **Diunsa** (Distribuciones Universales S.A.) (2019) | Esta compañía no venderá, cederá ni distribuirá la información personal que es recopilada sin su consentimiento, salvo que sea requerido por un juez con un orden judicial. | Cumple | Cumple | Cumple | (1) Expresa que en caso de ser necesario ceder los datos personales, se solicitará consentimiento al titular.<br>(2) Obligación legal.<br>(3) Indica que se solicitará consentimiento previo a la cesión, lo que lleva implícita una notificación. |
| **5** | **Farmacia Simán** (Súper Farmacia Simán S.A.) (2021) | 6. Información Protegida<br>(…)<br>Los datos personales que usted ingrese en la página web se consideran en todo momento información confidencial y privada.<br>Farmacia Simán respetará la confidencialidad de los datos de carácter personal aportados por el usuario. | No Cumple | No Cumple | No Cumple | (1) No solicita el consentimiento específico ni inequívoco del usuario para tratar los datos.<br>(2) No se encontró |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | evidencia del interés que tendría la cesión del tratamiento de datos personales.<br>(3) No se encontró evidencia de este requisito. |
| **6** | **Farmacias del Ahorro** (Doguería y Farmacias "Del Ahorro" S.A.) (n.d.) | Esta compañía no venderá, cederá ni distribuirá la información personal que es recopilada sin su consentimiento, salvo que sea requerido por un juez con un orden judicial. | Cumple | Cumple | Cumple | (1) Expresa que en caso de ser necesario ceder los datos personales, se solicitará consentimiento al titular.<br>(2) Obligación legal.<br>(3) Indica que se solicitará consentimiento previo a la cesión, lo que lleva implícita |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | una notificación. |
| **7** | **Hugo Honduras** (Hugo Technologies S.A. de C.V.) (2020) | El USUARIO autoriza que la INFORMACION PERSONAL sea compartida con terceros, según se indicará a continuación, de conformidad con lo establecido en los Términos y Condiciones del SITIO WEB y la APP. A dichos terceros se les exigirá los mismos estándares de seguridad que sigue HUGO y que son requeridos por la LEYES APLICABLES. Podemos compartir la información que recopilamos sobre el USUARIO con:<br>• Hugo Drivers para que puedan prestar los SERVICIOS que el USUARIO solicita. Por ejemplo, compartimos su nombre, número de teléfono, y las ubicaciones de entrega;<br>• Nuestro personal de atención al cliente, para dar respuesta a las preguntas y quejas de los USUARIOS con relación a nuestros SERVICIOS;<br>• El público en general si envía el contenido a un foro público, por ejemplo, comentarios en blogs, mensajes de redes sociales u otras opciones de nuestros SERVICIOS a disposición del público en general, en cuyo caso el USUARIO asumirá el riesgo y liberará de toda responsabilidad a HUGO, por cualquier | Cumple | Cumple | No cumple | (1) Establecen que, al aceptar la Política de Privacidad, el usuario emite formal consentimiento informado para el tratamiento de sus datos.<br>(2) Cesión por obligación contractual y legal. Aunque es amplia, detalla claramente con quien y para que se cediesen los datos.<br>(3) No se encontró evidencia de este requisito. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | uso indebido, no autorizado o ilegal de la información por parte de terceros;<br>• Con terceros con quienes HUGO tenga relaciones comerciales (pero de tal forma que estos terceros no podrán identificar a ningún USUARIO individual con dicha información);<br>• Con empleados, oficiales, subsidiarias, afiliadas, proveedores, asesores, agentes, socios de marketing y otros proveedores o contratistas que razonablemente necesiten acceder a dicha información para los fines descritos en esta política;<br>• En caso de que la INFORMACION PERSONAL deba ser divulgada por orden judicial o de alguna autoridad competente con facultades suficientes para requerirla a HUGO o para establecer, ejercer o defender los derechos de HUGO; o en caso de que HUGO deba denunciar a las autoridades competentes algún tipo de actividad ilegal por parte del USUARIO en relación con Los SERVICIOS brindados través de nuestro SITIO WEB o la APP.<br>• Con cualquiera de las subsidiarias, afiliadas o miembros del mismo grupo de interés económico, en los países en que operamos, en forma tal que las subsidiarias no podrán identificar a un USUARIO en específico, que | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | razonablemente necesiten para los fines descritos en esta política;<br>• Con terceros en virtud de una eventual negociación o formalización de una fusión, adquisición, financiamiento, cesión u otras transacciones análogas. En estos casos, HUGO entregará únicamente la información estrictamente necesaria y en cumplimiento de los lineamientos legales establecidos por la legislación aplicable sobre la transferencia de datos personales.<br>• Para cualquier otro uso no descrito expresamente en la presente POLITICA, que sea previamente notificado y aceptado por el USUARIO. Los DATOS DE LOS USUARIOS no serán cedidos, comunicados ni trasferidos a terceros salvo por lo indicado en la presente POLÍTICA.<br>La información y los datos recolectados por HUGO serán tratados con absoluta privacidad, confidencialidad y seguridad, según estipule la legislación vigente y aplicable en la materia. | | | | |
| **8** | **Universidad Tecnológica Centroamericana** (n.d.) | Los datos personales (los datos) divulgados por esta Institución tienen como finalidad que los datos personales y/o datos sensibles que, en su caso sean recabados por virtud del presente Aviso de Privacidad, puedan ser utilizados para la debida operación y fines de la | No Cumple | Cumple | No Cumple | (1) No solicita el consentimiento específico ni inequívoco del usuario |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | Institución (y todas sus áreas), incluyendo su transmisión dentro y fuera del país a: filiales y subsidiarias de Laureate Education, Inc., instituciones educativas, socios comerciales u otros terceros y a las autoridades gubernamentales que así lo requieran. Lo anterior, con el objeto de que los mismos puedan ser utilizados para efectos académicos, administrativos, comerciales, mercadológicos, ventas, estadísticos y otros que puedan ser de interés y/o en beneficio del Titular.<br><br>Hacemos de su conocimiento que, para cumplir con las finalidades previstas en este Aviso de Privacidad y la Ley aplicable, podrán ser recabados y tratados datos personales sensibles, los cuales pueden relacionarse a su esfera más íntima, tales como aspectos de origen racial o étnico, estado de salud, creencias religiosas, filosóficas y morales, opiniones políticas, entre otras.<br>Con base en lo anterior, nos comprometemos a que los mismos serán tratados bajo estrictas medidas de seguridad y garantizando su confidencialidad.<br><br>Nuestro programa publicitario de notificación de promociones, ofertas y servicios a través de correo electrónico, se realiza mediante mensajes promocionales | | | | para tratar los datos.<br>(2) Interés legítimo de cesión por ejecución de contrato, obligación legal y que obedece a interés legítimo del responsable. Aunque es amplia, detalla claramente con quien y para que se pudiesen ceder los datos.<br>(3) No se encontró evidencia de este requisito. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | de la Institución y, ocasionalmente, podrán incluirse ofertas de terceras partes que sean nuestros socios comerciales. Los correos electrónicos solo serán enviados a los usuarios y a aquellos contactos registrados. | | | | |
| **9** | **Supermercados La Colonia** (Supermercados La Colonia S.A. de C.V.) (2020) | Finalidad y Transferencia de Uso de Datos<br>Los datos referidos en estos términos y condiciones que incluyen dirección de correo electrónico, número telefónico, número de identidad o algún otro documento de identificación oficial, tendrán como finalidad validar los pedidos y mejorar la labor de información y comercialización de los productos y servicios ofrecidos por Supermercados La Colonia, en ningún caso serán traspasados a terceros. | No cumple | Cumple | No cumple | (1) No se encontró evidencia de este requisito.<br>(2) Interés legítimo de ejecución del contrato.<br>(3) No se encontró evidencia de este requisito. |
| **10** | **Pricemart Honduras** (PriceSmart Honduras S.A. de C.V.) (2020) | Si usted nos proporciona Datos Personales, no procederemos a vender, licenciar, transmitir, o divulgar la misma fuera del grupo de empresas afiliadas a PriceSmart salvo que (i) usted nos autorice expresamente a hacerlo, o (ii) nos facilite proveer productos y servicios a Usted, o (iii) deba ser divulgada a entidades que prestan servicios de marketing en nuestro nombre o a otras entidades con las cuales tenemos acuerdos de mercadeo conjunto, o (iv) según sea | Cumple | Cumple | Cumple | (1) Expresa que en caso de ser necesario ceder los datos personales, se solicitará consentimiento al titular.<br>(2) Interés legítimo de ejecución del contrato y |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | requerido o permitido por la ley o una orden judicial.<br>En los términos anteriores, PriceSmart podría divulgar su información personal con la empresa matriz, filial o subsidiaria de PriceSmart. PriceSmart también podría dar los nombres y las direcciones de sus socios a terceras personas, con el propósito de que estos les envíen información promocional.<br>También podríamos compartir su información personal con nuestro(s) banco(s) afiliado(s) para el programa de tarjeta de crédito PriceSmart, con el fin de que le faciliten ofertas de la tarjeta de crédito y formularios, así como otras promociones relacionadas con el programa de tarjeta de crédito conjunta.<br>Si usted aplica para o solicita ciertos productos, ofertas o servicios, la información personal que usted nos brinde podría ser compartida directamente con terceros que ofrezcan los productos, ofertas o servicios solicitados. La empresa Matriz, filial o subsidiaria de PriceSmart con quienes compartamos información, están en la obligación de no utilizar la información compartida con fines diferentes al ofrecimiento del servicio que les solicitemos. | | | | obligación legal.<br>(3) Indica que se solicitará consentimiento previo a la cesión, lo que lleva implícita una notificación. |

El siguiente cuadro sirve de resumen para interpretar los resultados anteriores. Para indicar que cumple el requisito, se utilizó la puntuación 1, y de no cumplir el 0, logrando un total máximo de 3 puntos para cada uno de los entes comerciales privados escogidos.

*Tabla 8. Cuadro resumen sobre el análisis de la efectividad para evitar la comercialización ilegal de bases de datos en las políticas de privacidad de entes comerciales privados de Honduras según el RGPD.*

| ***Ente Comercial Privado*** | **Consentimiento del titular** | **Interés legítimo del tratamiento** | **Obligación de notificar al titular sobre la obtención** | **Total** |
|---|---|---|---|---|
| ***1.*** *Tigo Honduras* | 0 | 1 | 0 | 1 |
| ***2.*** *Claro Honduras* | 0 | 1 | 0 | 1 |
| ***3.*** *Jetstereo* | 0 | 1 | 0 | 1 |
| ***4.*** *Diunsa* | 1 | 1 | 1 | 3 |
| ***5.*** *Farmacia Simán* | 0 | 0 | 0 | 0 |
| ***6.*** *Farmacias del Ahorro* | 1 | 1 | 1 | 3 |
| ***7.*** *Hugo Honduras* | 1 | 1 | 0 | 2 |
| ***8.*** *UNITEC* | 0 | 1 | 0 | 1 |
| ***9.*** *La Colonia* | 0 | 1 | 0 | 1 |
| ***10.*** *PriceSmart Honduras* | 1 | 1 | 1 | 3 |
| *TOTAL* | 4 | 9 | 3 | 16/30 |

El cuadro muestra que, de 10 entes comerciales privados, solamente tres cumplirían con los tres requisitos exigidos por el RGPD para considerar legítima su cesión o comercialización a un tercero de su base de datos. Uno no cumpliría ninguno de los requisitos y otro cumpliría dos. La mitad de estos solamente cumpliría con un requisito.

Por un lado, solamente 4 de estos cumplen con el consentimiento previo, específico e inequívoco solicitado, ya que en su mayoría las políticas de privacidad expresaban que con el simple hecho de dar sus datos o entrar al servicio estaban aceptando sus políticas de tratamiento de datos personales. Apenas 3 entes cumplen con la notificación de la cesión,

siendo este el requisito menos cumplido. Por otro lado, de forma positiva, 9 de los entes considerados establecen fines de tratamiento legítimo en sus políticas de privacidad.

A la luz del RGPD y considerando que para que, según este, para que la cesión se considere legítima, se deben cumplir los 3 requisitos, solamente 3 empresas podrían comercializar o ceder legalmente sus bases de datos. En este sentido, es claro que la legislación actual es insuficiente e ineficaz para cumplir con estos estándares, evidenciando la posible necesidad de una legislación sectorial que regule el tema.

### 4.3 Análisis de las entrevistas no estructuradas

Para poder determinar aciertos y vacíos en la regulación estipulada para evitar la comercialización ilegal de bases de datos en el Anteproyecto de Ley de Protección de Datos Personales y Acción del Hábeas Data, se entrevistó a dos abogados con conocimientos sobre la protección de datos personales y la comercialización de bases de datos. La transcripción de ambas entrevistas se puede encontrar en el Anexo 1. Entrevista 1 y Anexo 2. Entrevista 2.

Entre los aciertos que tiene el Anteproyecto de Ley fue mencionado que esta iniciativa podría considerarse “la mejor de América” y que incluso Uruguay ha copiado e implementado varias de las figuras jurídicas consideradas en el Anteproyecto.

Otros aciertos son que la implementación de este Anteproyecto de Ley en Honduras haría el trámite de los derechos ARCO más expedito al volverlo un trámite administrativo y desjudicializarlo. De esta manera, las personas que consideren que sus datos personales han sido comercializados o cedidos ilegalmente, podrían hacer valer sus derechos de manera más expedita. Además, otro acierto es que, bajo esta ley, el trámite también sería gratuito por

tratarse de un derecho humano. Así, estas mismas personas que se consideraran vulneradas por una cesión o comercialización ilegal de sus datos, no dependerían de un abogado para hacer valer sus derechos.

Finalmente, durante la entrevista se mencionó que el Anteproyecto contempla todos los principios de protección de datos personales que se incluyen en el derecho internacional, especialmente los mencionados por la Organización de Estados Americanos. Esto indica que se trata de un cuerpo legal muy completo.

Un comentario adicional fue que la responsabilidad per se de los entes comerciales privados frente a la comercialización ilegal de bases de datos se encuentra regulada en el Código Penal, el cual en su última versión incluye específicamente, la responsabilidad de personas jurídicas, contribuyendo a sancionar penalmente esta acción.

Por otro lado, durante las entrevistas también se mencionaron algunos desaciertos o vacíos en el Anteproyecto de Ley de Protección de Datos Personales y Acción de Hábeas Data. Entre estos vacíos está que no se subsumió una regulación para la implementación de placas, sticker electrónico, expediente clínico y del acceso a redes sociales. Estos son datos de gran importancia y susceptibles a ser comercializados ilegalmente por su valor.

Uno de los entrevistados hizo la sugerencia de implementar las mismas disposiciones del Reglamento General de Protección de Datos europeos, especialmente sobre el consentimiento expreso por párrafo. También sugirió contar con un ente competente y eficiente con poder coercitivo para aplicar la regulación y las sanciones, alegando que el

Instituto de Acceso a la Información no es la institución más adecuada para esto, como indica el Anteproyecto de Ley.

Finalmente, ambos abogados entrevistaron coincidieron en que es necesario contar con una legislación sectorial sobre protección de datos personales en Honduras. Entre las razones que citaron está, que la ausencia de regulación abre la puerta a que entes comerciales privados hostiguen a los usuarios que no quieren recibir y para que defraudadores tomen la información y cometan fraudes, así como la vulneración de datos personales expone al Estado de Honduras a potenciales demandas por vulneración de un derecho humano y por el uso irracional de bases de datos por parte de instituciones.

# CAPÍTULO V

# 5. PROPUESTA DE INNOVACIÓN

La siguiente propuesta de innovación es el resultado de la validación de la hipótesis plantada y el trabajo de campo realizado a través de la aplicación de los diferentes instrumentos para esta investigación.

La regulación actual en Honduras sobre protección de datos personales resulta ineficaz para evitar la comercialización ilegal de bases de datos por parte de entes comerciales privados al no cumplir con estándares internacionales; adicionalmente, gran parte de la población considera que se encuentra en riesgo al exponerse a que sus datos personales sean comercializados sin su autorización por estos entes.

En ese sentido, Honduras no cuenta con una legislación sectorial que regule la protección de datos personales para evitar la comercialización ilegal de bases de datos por parte de entes comerciales privados. Sin embargo, si existe el Anteproyecto de Ley de Protección de Datos Personales y Acción de Hábeas Data que fue ampliamente trabajado y presentado al Congreso Nacional en el 2014. Este anteproyecto de ley no ha sido aprobado por el Congreso Nacional y dada la normativa parlamentaria nacional, la iniciativa deberá de volver a presentarse y someterse a votación al poder legislativo. Esto representa una oportunidad de mejora al posibilitar revisar y actualizar la propuesta de ley para garantizar la protección de datos personales de los hondureños y evitar la comercialización ilegal de bases de datos.

Se realizó una revisión del contenido sobre cesión de datos en Anteproyecto de Ley de Protección Personales y Acción del Habeas Data tomando en consideración como estándar internacional, los requisitos que el Reglamento General de Protección de Datos (RGPD) europeo exige para considerar legal una cesión de datos:

1. Consentimiento previo, específico e inequívoco del titular, que debe de incluir la posibilidad de transmitir estos datos a otro destinatario con los fines de la transmisión, así como asegurarse que los datos están actualizados.
2. Considerar los intereses del tratamiento, que deben ser legítimos (que la cesión sea necesaria para la ejecución o desarrollo del contrato, que constituya una obligación legal para el cedente, que obedezca intereses legítimos del responsable o terceros a los que se le comunican los datos, y/o que sirva para salvaguardar el interés vital del interesado u otros).
3. Notificar al dueño de los datos en la primera comunicación que se obtuvieron sus datos para tales fines (Comisión Europea, n.d.; Reglamento general de protección de datos, 2016, p. 36).

Durante esta revisión se encontraron algunos detalles que podrían fortalecerse en el contenido del Anteproyecto para lograr una regulación más clara y eficiente en evitar la comercialización ilegal de datos personales por entes comerciales privados, que cumpla los estándares internaciones de la Unión Europea como referente en el tema y uno de los principales mercados.

Se identificaron tres aspectos puntuales que valdría la pena mejorar en el Anteproyecto de Ley de Protección de Datos Personales y Acción de Hábeas Data. Primero,

que en el apartado del Aviso de Privacidad donde se exige que se debe de incluir la posibilidad de la cesión, también se exija que este aviso indique la finalidad que tendría dicha cesión ya que con esta información el titular puede decir más claramente si proporcionar o no sus datos y las consecuencias de esta cesión, logrando un consentimiento más específico.

Segundo, que en los deberes del responsable del Tratamiento se le exija comunicar al titular cuando haga una cesión de datos personales, para que el titular esté informado o pueda actuar sobre su información personal.

Finalmente, el Anteproyecto regula, específicamente en el Título VIII la Cesión de Datos. En este título se indica cuando una cesión puede considerarse legal, sin embargo, no se especifica, como lo hace el RGPD, los fines legítimos que puede tener la cesión. Aunque si se pueden encontrar estos fines en el contenido, estos están esparcidos, por lo que valdría la pena dejarlos de manera expresa y taxativamente para garantizar que los entes comerciales privados y los usuarios sepan claramente bajo que finalidades pueden ceder los datos personales a terceros.

### 5.1 Formulación de la Propuesta de Innovación

La propuesta de innovación consiste en reformar tres artículos del Anteproyecto de Ley de Protección de Datos Personales, con el objetivo de actualizar y detallar claramente la regulación de datos personales para evitar la comercialización ilícita de bases de datos por entes comerciales privados.

Con estas mejoras se pretende lograr un consentimiento más específico, más información y control sobre los datos personales y aclarar los fines legítimos que puede tener una cesión de datos personales.

*Tabla 9. Mejoras al Anteproyecto de Ley de Protección de Datos Personales y Acción de Hábeas Data.*

| **Mejoras al Anteproyecto de Ley de Protección de Datos Personales y Acción de Hábeas Data** | |
|---|---|
| **Contenido Actual** | **Propuesta de mejora al texto** |
| **Artículo 7. Contenido del Aviso de Privacidad.** El aviso de privacidad deberá contener, al menos, la siguiente información:<br><br>a. (…); b. (…);<br><br>c. La posibilidad de que los datos recolectados sean cedidos o comunicados a un tercero y la identidad y domicilio de dicho cesionario;<br><br>d. (…); e. (…). | **Artículo 7. Contenido del Aviso de Privacidad.** El aviso de privacidad deberá contener, al menos, la siguiente información:<br><br>a. (…); b. (…);<br><br>c. La posibilidad de que los datos recolectados sean cedidos o comunicados a un tercero, **la finalidad de esta cesión** y la identidad y domicilio de dicho cesionario;<br><br>d. (…); e. (…). |
| **Artículo 24. Deber del Responsable del Tratamiento.** El Responsable del Tratamiento deberá cumplir los siguientes deberes, sin perjuicio de las demás | **Artículo 24. Deber del Responsable del Tratamiento.** El Responsable del Tratamiento deberá cumplir los siguientes deberes, sin perjuicio de las demás |

| | |
|---|---|
| disposiciones previstas en la presente Ley y su Reglamento:<br><br>a.(…); b. (…); c. (…); d. (…); e. (…); f. (…); g. (…); h. (…); i. (…); j. (…); k. (…); l. (…); m. (…). | disposiciones previstas en la presente Ley y su Reglamento:<br><br>a. (…); b. (…); c. (…); d. (…); e. (…);f. (…); g. (…); h. (…); i. (…); j. (…); k. (…); l. (…); m. (…);<br><br>**n. Notificar al titular de cualquier cesión o comunicación que haga de sus datos, incluyendo el cesionario y la finalidad.** |
| **Artículo 35.- Cesión de datos a terceros.**<br>Los datos personales objeto del tratamiento sólo podrán ser cedidos a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, con el previo consentimiento expreso del Titular de los datos. | **Artículo 35.- Cesión de datos a terceros.**<br>Los datos personales objeto del tratamiento sólo podrán ser cedidos a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, con el previo consentimiento expreso del Titular de los datos. **Estos fines lícitos pueden ser por:**<br>**a. que el interesado dio su consentimiento para esos fines específicos,**<br>**b. que la cesión sea necesaria para la ejecución o desarrollo de un** |

| | |
|---|---|
| | **contrato en el que el interesado es parte,**<br>**c. que la cesión sea necesaria para cumplir una obligación legal para el cedente,**<br>**d. que obedezca intereses legítimos del responsable o terceros a los que se le comunican los datos, y/o**<br>e. **que sirva para salvaguardar el interés vital del interesado u otros.** |

*Fuente: (Instituto de Acceso a la Información Pública & Agencia Española de Cooperación Internacional para el Desarrollo AECID, 2014).*

La aprobación del anteproyecto de ley, incorporando las mejoras sugeridas en esta propuesta de mejora supondría un avance progresivo en la protección de datos personales para evitar la comercialización ilegal de bases de datos por entes comerciales privados, fortaleciendo el derecho fundamental a la intimidad personal y a la inviolabilidad de las comunicaciones.

Esta propuesta de mejora sería presentada al Instituto Hondureño de Acceso a la Información Pública (IAIP) como el ente público que ha formulado el Anteproyecto de Ley. El impacto de esta propuesta de mejor consiste en la mejora significativa de la posible futura regulación sobre protección de datos personales, beneficiando a los hondureños y hondureñas que cada vez más frecuentemente, otorgan sus datos personales a entes comerciales privados.

# CAPÍTULO VI

# 6. CONCLUSIONES Y RECOMENDACIONES

## 6.1 Conclusiones

**PRIMERA.** La protección de datos personales es un tema que ha logrado importancia en el mundo 2frente a las nuevas tecnologías y el uso masivo de datos personales que pueden perjudicar a los usuarios. Con relación a la primera pregunta de investigación, sobre la percepción de los hondureños, el instrumento aplicado evidencia que los hondureños consideran que su información personal se encuentra en riesgo de ser comercializada ilegalmente por entes comerciales privados.

Tomando en consideración el diseño cualitativo de esta investigación que se basa en la teoría fundamentada, los resultados de las 333 encuestas aplicadas en esta investigación muestran que, para la gran mayoría de los entrevistados, es relevante el tema de protección de datos personales. La mitad de los entrevistados también indicó que sospechan que entes comerciales privados a los que les han otorgado voluntariamente sus datos personales, comercializan o ceden sus bases de datos a otros entes sin autorización, y que de esta manera otros entes de este tipo logran contactarlos. La comercialización o cesión ilegal de datos personales es considerado por los entrevistados como un riesgo intermedio, posicionándose en el número 5 de 10 en las implicaciones más y menos riesgosas de conceder libremente los datos personales.

**SEGUNDA**. Honduras se clasifica como un país en el que el texto Constitucional no reconoce expresamente el Derecho a la Protección de Datos Personales, pero que posee

disposiciones sobre la materia que han permitido a los Tribunales Constitucionales reconocer este derecho fundamental. Adicionalmente, Honduras no cuenta con una regulación sectorial que regule el tema, especialmente que regule la cesión de bases de datos por parte de entes comerciales privados.

La legislación vigente que regula de manera general la protección de datos por parte de entes comerciales privados en Honduras es: de manera general la Constitución de la República y Tratados Internacionales sobre derechos humanos (el Pacto Internacional de Derechos Civiles y Públicos, la Declaración Americana de los Derechos y Deberes del Hombre y la Convención Americana sobre Derechos Humanos) que reconocen el derecho ligado a la intimidad y privacidad; la Ley sobre Justicia Constitucional que amplía sobre la garantía del Hábeas Data como mecanismo que se aplica en caso de trasgresión a este derecho; y el Código Penal, siendo el único que regula específicamente sobre la cesión ilegal y comercialización de datos personales al considerarlo un delito y regular la responsabilidad penal de cometerlo para los involucrados.

**TERCERA.** Honduras no cuenta con una normativa sectorial que regule el uso de datos personales por parte de entes comerciales privados. En este sentido, el instrumento aplicado indica que Honduras no cuenta con una regulación eficaz en protección de datos personales para evitar que entes comerciales privados cedan ilegalmente o comercialicen bases de datos de los usuarios por lo que es necesario contar con mayor regulación, específicamente, una legislación sectorial sobre el tema.

El estudio comparativo con el Reglamento General de Protección de Datos de Europa, considerado un referente mundial en la materia, muestra que solamente tres de las diez

políticas de privacidad de los entes comerciales privados hondureños escogidos, cumplirían con los tres requisitos que exige el RGPD para que su cesión de datos se considerara legal. Estos resultados muestran que la legislación actual no es suficiente y resulta ineficaz para cumplir estándares internacionales de protección de datos, evidenciando la necesidad de contar con una legislación adicional.

**CUARTA.** El Anteproyecto de Ley de Protección de Datos Personales y Acción de Hábeas Data presentado en el 2014 muestra el interés social por contar con una regulación sectorial sobre este tema, sin embargo, a la fecha este no ha sido aprobado por el Congreso Nacional. Siendo esta una investigación cualitativa, las entrevistas no estructurales realizadas con dos abogados expertos en el tema de protección de datos, sirven para conocer aciertos y vacíos de este anteproyecto de ley con relación a su aplicabilidad para evitar la comercialización ilegal de datos por parte de entes comerciales privados.

En ese sentido, las entrevistas practicadas revelan entre los aciertos, que el Anteproyecto de Ley se puede considerar muy completo y "la mejor (regulación) de América", que, a través de esta iniciativa, el trámite de derechos ARCO sería gratuito y más expedito al desjudicializarlo. Con la aprobación y entrada en vigor de esta regulación, los usuarios tendrían mayor control y facilidades sobre la cesión de sus datos personales. Sobre los vacíos, los expertos entrevistados indican que faltó incluir regulaciones específicas como placas, expediente clínico y acceso a redes sociales, y por otro lado se sugirió designar a un ente con poder coercitivo para aplicar la regulación y sanciones de esta legislación.

### 6.2 Recomendaciones

A partir de la presente investigación se sugiere:

- Ampliar la investigación aplicando una metodología similar a otras circunstancias de riesgo que implica conceder libremente datos personales. Se podría investigar la situación puntual para el caso de robo de datos personales y usurpación de identidad, fraude y pérdidas financieras e información que llegan a desconocidos, las cuales, según los resultados de los instrumentos aplicados en la presente investigación, son las tres implicaciones más riesgosas de conceder libremente los datos personales.
- Aprobar la Ley de Protección de Datos Personales y Acción de Hábeas Data en el Congreso Nacional de la República. Para esto es necesario revisar el anteproyecto del 2014 para actualizar y agregar regulaciones sobre temas actuales como las placas y sticker electrónicos, redes sociales, DNI, etc.; luego volver a recolectar las firmas o que sea propuesto por algún diputado y que se discutan nuevamente en el Congreso todos los artículos. Es necesario contar lo más pronto posible con una legislación sectorial que regule la protección de datos personales en Honduras dado el uso irracional de bases de datos por parte de entes comerciales privados y las posibles violaciones de derechos fundamentales y humanos que podrían derivar de la falta de regulación.
- Socializar periódicamente con los entes comerciales privados sobre la importancia de contar con una política de privacidad y su aplicación. Es importante ir preparando a estos entes, para garantizar a los usuarios el derecho fundamental a la intimidad y privacidad de las comunicaciones, así como facilitar la posible entrada en vigor de una legislación sectorial de protección de datos personales. De igual manera, una gran cantidad de países están comenzando a implementar regulaciones sectoriales de protección de datos personales y exigen que las empresas con las que comercializan

cumplan ciertos estándares, por lo que es importante que los entes comerciales privados vayan desarrollando estas buenas prácticas que facilitarán el comercio internacional.

- Concientizar a la población hondureña en espacios de la sociedad civil, sobre las implicaciones riesgosas que implica conceder libremente los datos personales a entes comerciales privados. Promoviendo una cultura de protección hacia los propios datos personales, que motive a los ciudadanos a asegurarse de la necesidad y de los fines que tendrá el tratamiento de sus datos personales al momento de cederlos.

# Bibliografía

Álvarez, D. (2020). La protección de datos personales en contextos de pandemia y la constitucionalización del derecho a la autodeterminación informativa. *Revista Chilena de Derecho y Tecnología*, *9*(1), 1–4. https://doi.org/10.5354/0719-2584.2018.57777

Andrés, G. (2019). *El consentimiento y el reglamento de protección de datos—LegalToday*. Legal Today. https://www.legaltoday.com/practica-juridica/derecho-publico/proteccion-datos/el-consentimiento-y-el-reglamento-de-proteccion-de-datos-2019-10-04/

Arroyo, V., & Sierra Castro, H. (2019, March 20). Honduras necesita un debate urgente sobre datos personales y libertad de expresión. *Access Now*. https://www.accessnow.org/honduras-igf/

Asamblea Nacional Constituyente. (1982). *Constitución Política: Vol. Diario Oficial La Gaceta No. 23, 612* (Decreto No. 131). Editorial OIM. http://www.poderjudicial.gob.hn/CEDIJ/Leyes/Documents/Constituci%C3%B3n%20de%20la%20Rep%C3%BAblica%20de%20Honduras%20%28Actualizada%202014%29.pdf

Bernal, C. A. (2010). *Metodología de la investigación administración, economía, humanidades y ciencias sociales* (3era ed.). Pearson Educación.

Brewer-Carías, A. R. (2016). Derecho del Sistema de Justicia Constitucional. In *Comentarios a la Ley sobre Justicia Constitucional: El sistema de Justicia Constitucional en Hondruas*. Editorial OIM.

Castellanos, Á., Alejos, D., Samour, O., Aragón, F., Paz Morales, J. R., Betancourt, C., Taboada, R., Quesada Bianchini, M., & Álvarez, A. C. (2020, June 30). *La pandemia por COVID-19 dispara el uso del comercio electrónico en Centro América*. Consortium Legal. https://consortiumlegal.com/la-pandemia-por-covid-19-dispara-el-uso-del-comercio-electronico-en-centro-america/

Castro, C. M. (2015). Las Tecnologías de la Información y la Comunicación (TIC'S) en el Derecho Procesal Civil Hondureño. *Revista Chilena de Derecho*, *43*(2), 759–782.

CLARO. (2017). *Claro—Personas | Documentos de Legal y Regulatorio*. CLARO HN. http://www.claro.com.hn/personas/legal-regulatorio/

Comisión Europea. (n.d.). *¿Podemos utilizar datos recibidos de un tercero para mercadotecnia?* [Text]. Comisión Europea - European Commission. Retrieved March 1, 2021, from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/can-data-received-third-party-be-used-marketing_es

Comisión Nacional de Bancos y Seguros. (2020). *Resumen Ejecutivo: Buenas prácticas para la protección de datos del usuario financiero*. Comité Fintech e Innovaciones Tecnológicas. https://www.cnbs.gob.hn/wp-content/uploads/2020/11/RESUMEN-EJECUTIVO-BUENAS-PRACTICAS-DE-PROTECCION-FINAL-editado.pdf

Congreso Nacional. (2019). *Código Penal*. Diario Oficial La Gaceta No. 34,940, Decreto 130-2017. https://www.tsc.gob.hn/web/leyes/Decreto_130-2017.pdf

Corte Suprema de Justicia. (2004). *Ley sobre Justicia Constitucional*. Diario Oficial La Gaceta No. 30, 792, Decreto 244-2003. http://www.oas.org/juridico/pdfs/mesicic4_hnd_justicia.pdf

Cubillos, Á. (2017). La Explotación de los datos personales por los gigantes de internet. *Biblioteca Jurídica Virtual Del Instituto de Investigaciones Jurídicas de La UNAM*, *3*, 27–55.

Diunsa. (2019). *Politica-de-privacidad – Diunsa*. https://www.diunsa.hn/politica-de-privacidad

Enríquez, L. (2017). Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales. *Revista de Derecho*, *27*, 43–61.

Farmacia Simán. (2021). *Términos y Condiciones*. Farmacia Simán. https://farmaciasiman.com/

Farmacias del Ahorro. (n.d.). *Política de Privacidad*. Retrieved February 25, 2021, from https://delahorro.app/politicas/Pol%C3%ADtica-de-Privacidad.pdf

Fernández de Heredia, L. (2018, April 16). La gestión de riesgos de la privacidad de datos personales, esencia del nuevo reglamento. *El blog de UHY FAY & CO. Madrid*. https://www.elblogdetusasesores-consultores.com/ciberseguridad-y-accesibilidad-de-la-informacion/la-gestion-riesgos-la-privacidad-datos-personales-esencia-del-nuevo-reglamento/

Gallardo, M. (2018). *GDPR: Comunicación de datos a terceros*. Expansión. https://www.expansion.com/especiales/2018/GDPR/comunicacion-de-datos-a-terceros.html

Gil, E. (2015). *Big Data, Privacidad y Protección de Datos*. Agencia Española de Protección de Datos.

González, V. (2017). La compraventa de Bases de Datos es ilegal según la LOPD | El Jurista. *El Jurista*. https://www.eljurista.eu/2017/12/18/la-compraventa-de-bases-de-datos-es-ilegal-segun-la-lopd/

Gregorio, C. G. (2019). *Protección de Datos Personales en América Latina- Juan Pérez ante una disyuntiva de progreso y bienestar*. Instituto de Investigación para la Justicia. https://www.researchgate.net/publication/334576727_Datos_personales_marketing_digital_y_los_derechos_de_los_ciudadanos_de_America_Latina

Hernández, R., Fernández, C., & Baptista, M. del P. (2014). *Metodología de la Investigación* (6th ed.). Mc Graw Hill Education. https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Huerta, P. P. (2017). *La génesis del derecho fundamental a la protección de datos personales*. Universidad Complutense de Madrid. https://eprints.ucm.es/43050/1/T38862.pdf

Hugo App. (2020). *Política de Privacidad y Seguridad*. Hugo App. https://hugoapp.com/politica-privacidad/

Jetstereo. (2015). *Política de Privacidad | Jetstereo—Cuando quieras lo mejor*. https://www.jetstereo.com/politica-de-privacidad

Kluwer, W. (2018). *Riesgo y alto riesgo (Protección de Datos)*. Guías Jurídicas. https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1jTAAAkNjEwtTM7Wy1KLizPw8WyMDQwsDM0NDkEBmWqVLfnJIZUGqbVpiTnEqADwHElc1AAAAWKE

LatinAlliance. (2020). *Aspectos Legales de la Transformación Digital de mi Negocio: La Protección de Datos*. https://latinalliance.co/wp-content/uploads/2020/08/Proteccion-de-Datos-Honduras.pdf

López, D. (2014, April 22). Análisis del Anteproyecto hondureño de Ley de Protección de Datos Personales y el desarrollo del habeas data. *Daniel López Carballo*. http://dlcarballo.com/2014/04/22/analisis-del-anteproyecto-hondureno-de-ley-de-proteccion-de-datos-personales-y-el-desarrollo-del-habeas-data/

López, D. A. (2014). Tratamiento de Datos Personales y Habeas Data en la Legislación Hondureña. *Observatorio Iberoamericano de Protección de Datos*. http://oiprodat.com/2014/04/25/tratamiento-de-datos-personales-y-habeas-data-en-la-legislacion-hondurena/

López-Torres, J. (2014). Antecedentes Internacionales en Materia de Privacidad y Protección de Datos Personales. *EAFIT Journal of International Law*, *5*(2), 103–117.

Mailrelay: Email Marketing. (2018). *Comprar bases de datos de emails: ¿Estrategia o fraude?* https://www.youtube.com/watch?v=ud8guvagz7s

Maqueo, M. S., Moreno, J., & Recio, M. (2017). Protección de datos personales, privacidad y vida privada: La inquietante búsqueda de un equilibrio global necesario. *Revista de Derecho (Valdivia)*, *XXX*(1), 77–96.

Martínez, R. (2017). Cuestiones de ética jurídica al abordar proyectos de Big Data. El contexto del Reglamento general de protección de datos*. *Dilemata*, *24*, 151–164.

Mejía, N. (2006). ¿Metodología para investigar en el derecho? *Estado Del Arte En Metodología de La Investigación Jurídica 1999-2003*.

Mok, S. C. (2010). Privacidad y protección de datos: Un análisis de legislación comparada. *Diálogos: Revista electrónica de historia*, *11*(1), 4.

Olvera, J. (2015). *Metodología de la Investigación Jurídica para la Investigación y la elaboración de tesis de licenciatura y posgrado* (1st ed.). Universidad Autónoma del Estado de México.

Organización de Estados Americanos. (1948). *Declaración Americana de los Derechos y Deberes del Hombre* [Text]. OEA. http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp

Organización de Estados Americanos. (1969). *Convención Americana sobre Derechos Humanos*. https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm

Organización Internacional de las Naciones Unidas. (1966). *Pacto Internacional de Derechos Civiles y Políticos*. Oficina Del Alto Comisionado de Los Derechos Humanos de Las Naciones Unidas. https://www.ohchr.org/sp/professionalinterest/pages/ccpr.aspx

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la

Directiva 95/46/CE (Reglamento general de protección de datos), Pub. L. No. 32016R0679, 119 OJ L (2016). http://data.europa.eu/eli/reg/2016/679/oj/spa

Pedraza, Ó. (2001). La Matriz de Congruencia Una Herramienta para Realizar Investigaciones Sociales. *Economía y Sociedad*, *6*(10), 311–316.

Polo, A. (2020). El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado. *Revista Derecho Político*, *108*, 165–193.

Ponce, L. (1996). La Metodología de la Investigación Científica del Derecho. *Biblioteca Jurídica Virtual Del Instituto de Investigaciones Jurídicas de La UNAM*, *205–206*, 61–83.

PriceSmart. (2020). *Políticas y retornos*. https://www.pricesmart.com/site/hn/es/politicas-y-retornos#politica_confidencialidad_datos_personales

Red Iberoamericana de Protección de Datos. (2020). *Legislación* |. Red Iberoamericana de Protección de Datos. https://www.redipd.org/es/legislacion?nid=83

Richter, M. (2015). La Protección de Datos de Carácter Personal como Derecho Humano. *Revista Auctoritas Prudentium*, *12*, 18–29.

Rodríguez, E. (2015). El nacimiento de un nuevo derecho fundamental: El derecho a la protección de datos personales. Una aproximación a su origen. *Revista de La Facultad de Derecho*, *67–70*, 45–88.

Ruiz, B. Y. (2016). *Regulación en materia de protección de datos personales o habeas data en Colombia*. Universidad Católica de Colombia. https://repository.ucatolica.edu.co/bitstream/10983/13794/4/Regulaci%c3%b3n%20e

n%20materia%20de%20protecci%c3%b3n%20de%20datos%20personales%20o%20habeas%20data%20en%20Colombia%20%281%29.pdf

Sánchez Zorrilla, M. (2011). La Metodología de la Investigación Jurídica: Características peculiares y pautas generales para investigar en el derecho. *Revista Telemática de Filosofía Del Derecho*, *14*, 317–358.

Sarmiento, Y. (2016, May 17). ¿Cómo legisla Honduras la protección de sus datos? *Revista IT NOW*. https://revistaitnow.com/como-legisla-honduras-la-proteccion-de-sus-datos/

Supermercados La Colonia. (2020). *Políticas de privacidad*. https://www.lacolonia.com/politicas-de-privacidad

TIGO. (2021). *Aviso de Privacidad para la Protección de Datos Personales*. Tigo Honduras. https://ayuda.tigo.com.hn/hc/es/articles/360027370653-Aviso-de-Privacidad-para-la-Protecci%C3%B3n-de-Datos-Personales

Tomé, E. (2019). *Estudio Centroamericano de Protección de Datos, Honduras*. Ipandetec. https://www.ipandetec.org/wp-content/uploads/2019/01/EDP_Honduras.pdf

Travieso, J. A. (2016). Protección de datos personales y tecnología. En busca del paraíso perdido. *Revista Tribuna Internacional*, *5*(9), 109–122. https://doi.org/10.5354/rti.v5i9.41962

Unión Europea. (2000). *Carta de Derechos Fundamentales*. Lex Europa. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A12016P%2FTXT

UNITEC. (n.d.). *Política de Privacidad*. Retrieved February 25, 2021, from https://www.unitec.edu/politica-de-privacidad/

Vargas, Z. R. (2009). La investigación aplicada: Una forma de conocer las realidades con evidencia científica. *Revista Educación*, *33*(1), 155–165.

Vera, M. A., & Vivero, M. B. (2019). ¿Vida Privada o Muerte a la Privacidad?: Protección de datos personales en la relación empresa-cliente en Ecuador. *USFQ Law Review*, *IV*. https://doi.org/10.18272/lr.v6i1.1397

Villabella Armengo, C. M. (2015). Los Métodos en la Investigación Jurídica. Algunas Precisiones. *Biblioteca Jurídica Virtual Del Instituto de Investigaciones Jurídicas de La UNAM*, 921–953.

Villan, M. A. (2018). *Datos personales, marketing digital y los derechos de los ciudadanos de América Latina*. Universidad Argentina de Negocios.

# Anexos

## Anexo 1. Entrevista 1

Realizada el 26 de febrero del 2021.

Abogado hondureño con maestría en Derecho Civil y Comercial de la Universidad Internacional de Florida, maestría en Derecho Constitucional de la Universidad de Valencia y Especialización en Derecho Internacional y Estudios Jurídicos Internacionales; con conocimiento sobre la protección de datos personales y sobre el Reglamento General de Protección de Datos de Europa (RGPD).

**Investigadora:** Buenas tardes abogado, me gustaría comenzar la entrevista preguntándole, ¿qué conocimiento tiene respecto a la regulación de la Protección de Datos Personales para evitar la comercialización ilegal de Bases de Datos por entes comerciales privados en Honduras?

**Abogado entrevistado 1:** Hay varios temas. Anteriormente el que guardaba toda la información era el Registro Nacional de las Personas, tenían las bases de datos personales a nivel nacional, que obviamente, por su función era la institución correcta para almacenar esta información. Antes no era común que empresas privadas tuvieran mis datos, mis números de teléfono, correos y que estuvieran llamando.

Es de conocimiento público, aunque no existe una investigación que lo establezca, pero el Registro Nacional de las Personas vendió la información de las personas a las empresas privadas. Justamente, con un fin lucrativo de hacer negocio y ganar dinero. Esto fue una violación de privacidad a nivel nacional porque en ningún momento el Registro

Nacional de las Personas nos consultó, o me preguntaron a mí, si podían vender mis datos. Eso, por un lado.

La forma correcta de hacerlo es como lo hizo la Farmacia Kielsa, ellos crearon su propia base de datos. Cuando uno iba a comprar algo, ellos decían me regala su nombre, número de identidad y correo, así uno respondía si quería o no. Ellos pedían mi autorización para mandarme correos, anuncios y llamadas, lo que sea, pero bajo mi autorización porque la solicitaban.

En el caso del RNP, esto no sucedió así, y ahora esto se ha hecho algo viral porque ahora muchas empresas consiguen los datos personales y pasan llamando u ofreciendo productos sin que les haya dado mis datos y autorización.

**Investigadora:** Okay, ¿usted considera que para lograr que las empresas soliciten la autorización para comercializar las bases de datos se necesita una regulación sectorial?

**Abogado entrevistado 1:** Es necesario. Es necesario porque el hecho de tener información de los ciudadanos y cederla, abre la puerta a que estos entes hostiguen a los usuarios con anuncios que uno no quiere saber y no quiere tener, y también para que defraudadores agarren la información y cometan fraudes. Lo digo por la cantidad de gente que llega a donde yo trabajo porque los han defraudado, es increíble. ¿Por qué? Porque consiguen información en internet o porque las empresas privadas están regando los nombres y contactos de todo mundo. Personalmente, dos intentos he tenido de que me han querido vender algo sabiendo que son del crimen organizado. Fácilmente se puede engañar a alguien, por eso es necesario regular esto.

**Investigadora:** Específicamente, ¿de qué forma cree que se podría regular?

**Abogado entrevistado 1:** En Europa tiene el Reglamento General de Protección de Datos, que es muy estricto. Yo creo que se debería de implementar aquí. Todos notamos que cuando se creó e implementó este nuevo reglamento, un montón de empresas internacionales comenzaron a enviar correos solicitando aceptar las nuevas condiciones de privacidad porque el nuevo reglamento lo exigía. Entonces sucedió que, al modificar el reglamento, la empresa privada necesitaba una autorización con consentimiento expreso, no como sucede ahorita que las empresas mandan un documento con 500 páginas que no leemos, solo damos scroll hasta abajo para aceptar. Según el nuevo reglamento los usuarios tienen que ir párrafo por párrafo dándole check a cada uno para expresar que estaban de acuerdo y si no lo hacían la empresa era susceptible a una demanda de daños y perjuicios y una sanción del Estado por irrespetar la privacidad de los ciudadanos.

Incluso esta normativa establece a una persona encargada de la protección de los datos, lo que es esencial porque esta persona debe de saber que los datos personales que tiene de su cliente no los pueden tener los demás empleados de la empresa, solo la persona encargada los puede resguardar.

Aplicar esto en Honduras implica modificar la normativa actual y tener un órgano competente y eficiente, hago énfasis en esto, para aplicar la normativa y las sanciones en caso de que corresponda.

**Investigadora:** El Anteproyecto de Ley de Protección de Datos Personales designa como entidad encargada al Instituto de Acceso a la Información Pública, ¿qué opina al respecto?

**Abogado Entrevistado 1:** Haré énfasis nuevamente en que debe de ser un ente competente y eficiente que se encargue de aplicar la regulación y las sanciones como se debe. ¿Qué es lo que pasa? Está bien que se designe esta entidad, pero ¿cuál es el poder coercitivo que tiene esta institución? ¿Qué poder coercitivo va a tener sobre los ciudadanos? ¿Va realmente a ser una institución tiene esas facultades de forma eficiente o va a ser, por ejemplo, como el CNA? Que el CNA me presenta donde trabajo un "oficio" solicitándome información y yo le digo "nos vemos, vaya a volar", porque no tienen la potestad de venir a pedirme información y si yo quiero se las puedo dar, si no quiero no les doy nada.

**Investigadora:** ¿Usted considera que sería más eficiente crear una nueva institución?

**Abogado entrevistado 1:** Podría crearse una nueva institución, pero el problema con la creación de instituciones aquí es que estamos inundados de instituciones públicas que no hacen su trabajo. En teoría a quien debería de designarse es al Ministerio Público porque es el órgano de investigación, pero la verdad no podría decir cosas buenas del Ministerio Público. Podríamos hablar de una institución pública tirando a sanciones administrativas, por ejemplo, el SAR. El SAR se encarga de este tipo de investigaciones y sanciones administrativas, que serían multas que irían a las arcas del Estado.

**Investigadora:** ¿Algún comentario que agregar respecto a la regulación jurídica de la responsabilidad de entes comerciales privados frente a la comercialización de datos personales?

**Abogado entrevistado 1:** La responsabilidad que tienen las empresas está regulado sobre todo en el Código Penal que se ha ampliado en nuestro nuevo Código Penal, incluyendo a las personas jurídicas. Quizás no se busca tanto al individuo, que obviamente si comete un delito va a la cárcel, pero ahora también está la responsabilidad social. Las empresas tienen responsabilidad no solamente social, si no también ambiental, económica, y dentro de las responsabilidades civiles está la privacidad de sus clientes. La información que manejan de sus clientes es algo muy delicado. Tal vez uno piensa que si compra algo y les dice donde vive no es algo importante porque lo puede averiguar cualquiera, pero uno puede hacer muchas cosas con esa información, un criminal puede hacer muchas cosas con esa información. Entonces si es importante las empresas privadas tomen esto en cuenta y le den importancia al momento de tratar los datos personales de sus clientes.

**Anexo 2. Entrevista 2**

Entrevista realizada el 5 de marzo del 2021.

Abogado hondureño del Instituto de Acceso a la Información Pública con especialidad obtenida en el 2019 del Instituto Español de Protección de Datos Personales, con maestría y doctorado en Derechos Humanos y experiencia en el ejercicio de sus funciones.

**Investigadora: ¿**Qué sabe sobre el Anteproyecto de Ley de Protección de Datos Personales y Acción del Hábeas Data en Honduras?

**Abogado entrevistado 2:** El anteproyecto de ley se construye como una demanda ciudadana y con fondos de la Cooperación Español por la imperativa necesidad de las falencias de una normativa que regula el tema en Honduras. Se presenta ante el Congreso Nacional de Honduras como una iniciativa ciudadana con 7,900 firmas y el objetivo de formar una ley que hasta la fecha no existe.

**Investigadora:** ¿Usted participó en la formulación del contenido de este Anteproyecto de Ley?

**Abogado entrevistado 2:** En efecto, estuvimos reunidos una semana entera con un ex magistrado de la Corte Suprema de España, el abogado Puyol; él estuvo presente aquí en Honduras y estuvimos reunidos toda una semana en el Hotel Clarión trabajando con expertos de info tecnología, su servidor y el equipo legal trabajando en jornadas maratónicas, viendo jurisprudencia de países de América. Utilizamos jurisprudencia de Uruguay, Colombia, Costa Rica, México y España. Empezamos con la jurisprudencia administrativa y judicial para poder darle forma a la ley.

Acá le voy a agregar un comentario que nos hizo el magistrado Puyol, él nos manifestaba que la Ley de Honduras iba a ser la mejor de América, porque era la que contenía todas las figuras, que aun la ley de España no tiene. Por ejemplo, las disposiciones que regula sobre la manipulación genética, los mecanismos de seguridad por retina y el uso y limitación de drones a través de un registro porque cualquiera tiene un dron que puede

vulnerar su privacidad. Incluso Uruguay nos copió varias figuras contenidas en el Anteproyecto, ya hasta las están implementando y nosotros aún no.

**Investigadora:** Muy interesante, no sabía eso. Hablando ya del tema de cesión y comercialización ilegal de datos, ¿cómo se regula en el Anteproyecto de Ley?

**Abogado entrevistado 2:** Nosotros en el Anteproyecto tenemos 4 figuras jurídicas: Acceso, Rectificación, Cancelación y Oposición, que en sus siglas se denominan los derechos ARCO. Iniciamos con el Acceso, analizando las diferentes formas de accesos que tienen las empresas privadas a diferentes bases de datos. Cuando hablamos de bases de datos de empresas jurídicas, por ejemplo, Banco Atlántida; Banco Atlántida y Seguros Atlántida son dos personas jurídicas diferentes, pero el simple hecho de poseer una razón social similar no autoriza para que mis datos como cliente habiente de Banco Atlántida sean cedidos a Seguros Atlántida. Yo le estoy dando mis datos a la persona jurídica Banco Atlántida, no a la persona jurídica Seguros Atlántida. Así se malinterpreta esa cesión de datos que ocurre dentro de personas jurídicas con la misma denominación social, pero que no son la misma persona jurídica.

**Investigadora:** En mi investigación hice una pequeña revisión de las políticas de privacidad de unas cuantas empresas hondureñas y una mayoría expresa que va a ceder los datos personales con las demás empresas de su grupo. En este caso, ¿sería esta disposición correcta?

**Abogado entrevistado 2:** Ahí estaría bien. A raíz de estos elementos, en el 2009 una gran mayoría de empresas que no tenía la política de cesión de datos. Ellos de forma

unilateral determinaban hacer esa cesión de datos. A raíz de todas estas pláticas se les empezó a recomendar que la incluyeran al momento que el usuario llegara a su entidad porque así no estarían cometiendo la irregularidad de la cesión de datos y sería una cesión legal de datos personales. Cuando yo como cliente suscribo la autorización, automáticamente le estoy diciendo a la empresa que estoy de acuerdo con que les ceda mis datos a sus demás empresas y no hay problema. Esto fue uno de los avances y en honor a la verdad, muchas instituciones lo implementaron después de todas estas conversaciones previas que tuvimos. No esperaron que estuviera la ley, sino que lo tomaron como una buena práctica.

**Investigadora:** Si encontré algunas empresas que no lo regulaban en su política de privacidad.

**Abogado entrevistado 2:** Si, como no es obligatorio algunos no lo hacen, pero las instituciones grandes si lo hacen.

**Investigadora:** ¿Qué tres aciertos mencionaría en las disposiciones sobre cesión de datos que se determinan en este Anteproyecto de Ley?

**Abogado entrevistado 2:** Número 1, realizaba más expedita el trámite de los derechos ARCO, ya que lo convertía en un trámite administrativo y desjudicializaba el proceso de la Corte y lo subsumía a una denuncia ante el IAIP, quien estaba obligado a dar respuesta en un periodo no máximo de 10 días hábiles. Entonces hacía muy ágil el proceso.

Número 2, vuelve el proceso de forma gratuita ya que, por ser un derecho humano, e acceso de denuncia debe de estandarizarse. Ante la Corte Suprema de Justicia en Amparo, usted solo se puede ir a través de apoderado de legal y los abogados en causa propia. ¿Pero

con pasa con todas aquellas personas que no son abogados o que no pueden pagar un abogado? Automáticamente se les bloqueaba el acceso a presentar el Habeas Data. En cambio, en el Anteproyecto de Ley se determinaba que cualquier persona, natural, jurídica, a título de representante o privado, podía presentar la denuncia ante el IAIP.

Número 3, el Anteproyecto de Ley contemplaba los Principios de Protección de Datos de Derecho Internacional. Agarraba todos los Principios de la OEA, ¿no sé si usted los ha leído?

**Investigadora:** Si los he leído, incluso leí los propuestos en el Anteproyecto de Ley, comparándolos con los que están incluidos en el Reglamento General de Protección de Datos y son más completos los del Anteproyecto de Ley.

**Abogado entrevistado 2:** Exactamente, el Anteproyecto de Ley contempla todos los principios de Protección de Datos. Estos son tres aspectos importantísimos que el Anteproyecto de Ley destaca.

**Investigadora:** ¿Qué tres aspectos considera que pudieron determinarse mejor en las disposiciones sobre cesión de datos que se determinan en este Anteproyecto de Ley?

**Abogado entrevistado 2:** Okay, habríamos, y esto si no se profundizó lo suficiente porque no se había perfeccionado, lo de las placas y el sticker electrónico que entregan con las placas, no se había subsumido en el Anteproyecto. Este es un elemento que ya debe de ser objeto de reforma para que sea incluido porque estas bases de datos son manejados y administrados por los entes del Estado y deben de ser regulados. Este es uno de los elementos que se quedaron por fuera.

Otro elemento que se quedó por fuera es el acceso a las redes sociales, en donde no se profundizó también. En determinar dónde termina la libertad de expresión y el abuso o intromisión a la dignidad de la persona a quien yo me refiero.

El otro elemento que lastimosamente quedó fuera, aunque el IAIP lo está retomando, no quedó en el Anteproyecto de Ley, es el expediente clínico. Es unificar un solo expediente clínico, que con su número de identidad el médico que lo atienda tiene acceso a su expediente clínico desde su nacimiento. Era regular las consultas y acceso y unificar el expediente. Este es un proyecto sumamente importante que el IAIP ya está regulando.

**Investigadora:** El Anteproyecto de Ley es muy completo y extenso, tal vez no lo noté. En el Reglamento General de Protección de Datos Europeo regulan que la persona a quien se le ceden los datos tiene que notificar al usuario como y de quien recibió los datos en la primera comunicación. Quisiera consultar, ¿si complementaron este tipo de disposición en el Anteproyecto de Ley?

**Abogado entrevistado 2:** Existen 2 figuras: quien administra el dato y a quien se le cede el dato, que es el DBO. Esas dos figuras están contempladas dentro del Anteproyecto de Ley. Por ejemplo, vamos a suponer con un ejemplo que en la actualidad se está dando. El CENISS, el Centro de Información del Estado, es uno de los principales recolectores de datos personales. Tiene una ficha única de registro de participantes, es el recolector de datos y automáticamente se convierte en el administrador de esa base de datos. Hay algunos proyectos que por la naturaleza tienen que hacerle una cesión de datos. Por ejemplo, ahora con esta pandemia, el Estado tuvo que proporcionar internet a zonas que no tenían. Entonces el CENISS tuvo que hacer una cesión temporal de ciertos datos a CONATEL para poder

determinar los beneficiados. CENISS hace una cesión de datos a CONATEL, este último genera un receptor y un administrador. CONATEL per se, cómo persona jurídica parte del Estado recibe los datos y es responsable, pero dentro del responsable también hay un encargado que es el DBO, quien verificar quien cuando y donde entran a hacer una revisión de esa base de datos.

**Investigadora:** En ese caso, ¿la institución qué recibe los datos, notifica al usuario que recibió sus datos personales?

**Abogado entrevistado 2:** Tiene que. En el Anteproyecto de Ley se determina que tiene que notificarle. Esto se regula en la parte del encargado y responsable que queda por el artículo cincuenta y algo. Ahí se determina la obligatoriedad de la institución de notificar a la persona porque en ese punto la persona puede decirle a la entidad que no quiere que los ceda, que no quiere el beneficio y que se opone al uso de sus datos.

**Investigadora:** Gracias abogado, ya para finalizar me gustaría saber: ¿qué tan necesaria considera que es para Honduras contar con una regulación sectorial sobre Protección de Datos Personales?

**Abogado entrevistado 2:** No es necesario, es vital. Es de vida o muerte porque la vulneración de datos personales es tan grande que está exponiendo al Estado de Honduras a potenciales demandas en el Sistema Interamericano de Derechos Humanos por vulneración de un derecho humano y por el uso irracional de bases de datos por parte de instituciones.

Por ejemplo, instituciones financieras que son fáciles de regular. Es mucho más difícil regular las instituciones de media o baja tabla, todas esas que tienen bases de datos manuales, ellos son complicados de regular.

**Investigadora:** En el caso de las entidades financieras, ya cuentan con una regulación, ¿no?

**Abogado entrevistado 2:** La AHIBA (Asociación Hondureña de instituciones Bancarias) ha emitido una regulación que tomaron, bueno también estuvimos en esas reuniones, de Equifax y TransJunior, que son de las bases de datos más completas que hay en el país. Uno es estadounidense y el otro colombiano. La AHIBA emitió unos lineamientos en el cual más o menos adaptaron el Anteproyecto de Ley para ser aplicable únicamente al sistema financiero.

Entonces, le digo no es importante, es vital que el Estado de Honduras apruebe este Anteproyecto de Ley. Lastimosamente por la norma parlamentaria tocaría volver a recolectar las firmas o que un diputado introduzca el Anteproyecto de Ley como iniciativa de ley y volver a tratar el tema, para que se discutan nuevamente todos los artículos.