PROTECCIÓN Y SANCIONES CONCERNIENTES A LA UTILIZACIÓN DE DATOS DE CARÁCTER PRIVADO EN LA WEB EN ENCARNACIÓN.

José Manuel Morínigo Pérez

Tutor: Abg. Celso Benjamín Ramírez

Tesis presentada en la Universidad Tecnológica Intercontinental como requisito para la obtención del título de Abogado

Encarnación, 2022

CONSTANCIA DE APROBACIÓN DEL TUTOR

Quien suscribe Celso Benjamín Ramírez Benítez, con documento de identidad número 1.762.360, tutor del Trabajo de Conclusión de Carrera titulado “Protección y sanciones concernientes a la utilización de datos de carácter privado en la web en Encarnación” elaborado por el alumno José Manuel Morínigo Pérez para obtener el Título de Abogado, hace constar que el mismo reúne los requisitos formales y de fondo exigidos por la Universidad Tecnológica Intercontinental y puede ser sometido a evaluación y presentarse ante los docentes que fueron designados para conformar la Mesa Examinadora.

En la ciudad de Encarnación, a los 1 días del mes de setiembre de 2022.

Dedico este trabajo a:

mi esposa, por su persistente apoyo,

a mis padres, por ser puntales fundamentales,

y por el ejemplo de trabajo y dedicación.

Agradezco a:

Dios en primer lugar, por todo lo que nos da,

a mis compañeros y docentes por brindarme

el soporte necesario, y por supuesto a tan prestigiosa

casa de estudio a la Universidad Tecnológica

Intercontinental por forjarme como profesional.

Tabla de Contenido

Lista de Tabla

Tabla de Ilustraciones

PROTECCIÓN Y SANCIONES CONCERNIENTES A LA UTILIZACIÓN DE DATOS DE CARÁCTER PRIVADO EN LA WEB EN ENCARNACIÓN.

José Manuel Morínigo Pérez

Universidad Tecnológica Intercontinental

Nota del autor

Carrera de Derecho, Sede XIX
Email: josemorinigo12@gmail.com

Resumen

El propósito de esta investigación fue analizar, si las personas pueden sufrir daños utilizando la web, a consecuencia de introducir sus datos de carácter privados en el internet, y si posteriormente puede exigir una sanción o resarcimiento de los daños y perjuicios, según la doctrina, legislación y jurisprudencia del Paraguay, en la ciudad de Encarnación. El problema formulado radica en el desconocimiento que existe con respecto a la posibilidad de que las personas sean susceptibles de sufrir todo tipo de daños y exigir el castigo de los mismos. La pregunta central de la investigación plantea: ¿A qué consecuencias jurídicas se enfrentan aquellas personas que utilizan los datos privados de las personas en la web en la ciudad de Encarnación? En la investigación el nivel de investigación ha sido el descriptivo. El enfoque que el autor abordo fue el método cuantitativo. La población quedo conformada por familias que habitan en la ciudad de Encarnación. El tipo de muestra ha sido por cuoteo y aleatorio en al barrio Zona alta de la ciudad mencionada. Las principales conclusiones fueron todo lo expuesto se da un margen de porcentaje en el análisis de las tabulaciones, encuadrando como acto delictivo el mal uso del internet, que las personas utilizan la web con datos privados, pero sin saber que pueden ser víctimas de algún tipo de delito, y si ellos son las víctimas de estos inescrupulosas, no saben dónde acudir para reclamar justicia.

Palabras clave: Personas, Datos privados, Internet, Daño, Web, Protección.

Marco Introductorio

Tema de Investigación

La protección de datos de carácter personal en la ciudad de Encarnación**.**

Planteamiento y formulación del problema

El problema que se plantea consiste

Preguntas de investigación. ¿A qué consecuencias jurídicas puede conllevar, la utilización de los datos privados vía web de las personas en la ciudad de Encarnación?

De esta pregunta central de investigación, se desglosan las siguientes preguntas especificas:

- ¿Cuáles son las normas o leyes que protegen este tipo de acto que es el uso de datos personales en el internet en la ciudad de Encarnación?
- ¿A qué instituciones se puede acudir en caso de ser afectado por el uso de los datos e informaciones de uso privado en la ciudad de Encarnación?
- ¿Existe legislación que sancionan la manipulan de los datos privados de las personas en la ciudad de Encarnación?

Objetivo de Investigación

General. Analizar las sanciones a ser impuestas a aquellas personas que infringen en el uso no autorizado de los datos de carácter privado en la ciudad de Encarnación.

Específicos.

- Individualizar las normas o leyes que protegen este tipo de acto ilícito que es el uso no autorizado de datos de carácter personal en la ciudad de Encarnación.

- Identificar instituciones donde se pueda acudir en caso de sufrir atentado en contra del uso de datos no autorizado de carácter privado en la ciudad de Encarnación.
- Averiguar los órganos encargados de sancionar a aquellas personas que hacen uso de información de carácter personal en la ciudad de Encarnación.

Justificación y Viabilidad

Con el tema a ser investigado pretendo dar a conocer los derechos y leyes que hacen a la protección de los datos con énfasis en los datos personales privados en la web, como así también las sanciones referentes al tema esbozado, y por sobre todo hacer conocer el bien jurídico protegido, en vista al desconocimiento que existe al respecto.

Demostrar a la ciudadanía el amparo constitucional que versa sobre el tema escogido y ver si efectivamente el estado ampara a los individuos con relación a la privacidad de datos en la ciudad de Encarnación; y en ese mismo sentido indicar al lector las probables acciones a ser entabladas.

Es de suma importancia e interés los datos a ser recopilados en esta investigación, compilar en un mismo instrumento a fin de facilitar la búsqueda a los lectores referente al tema en cuestión, brindar una herramienta a la sociedad y a todos aquellos que se encuentran en el ejercicio de la profesión.

Es totalmente potable y viable elaborar esta investigación en razón de contar con datos bibliográficos y jurisprudencias en general, además de producir datos de hecho que complementarán esta investigación.

Marco Teórico

Antecedentes de Investigación

A continuación, se exponen los resultados alcanzados a partir de la actividad de búsqueda de informaciones bibliográficas realizada a fin de sistematizar los antecedentes de los estudios previos que se han realizado sobre el tema investigado hemos decidido investigar al respecto en la Universidad tecnológica Intercontinental (UTIC), se ha investigado cuanto sigue.

- Autore**:** Francisco Joel Velázquez Oviedo

Institución: Universidad Tecnológica Intercontinental (UTIC)
Título: Las nuevas tecnologías y su influencia en el Pensamiento Jurídico.
Año: 2016.

- Autora**:** Nidia Aurora Mendieta Cáceres

Institución: Universidad Tecnológica Intercontinental (UTIC)
Título: La Protección Jurídica a la Base de Datos.
Año: 2017.

- Autor**:** Gilberto Flores Rolón

Institución: Universidad Tecnológica Intercontinental (UTIC)
Título: Delitos Informáticos. Seguridad en las Redes locales privadas. Imprevisiones de la Legislación. Observación del Derecho Privado
Año: 2017.

- Autora**:** Claudia Carolina Paniagua de Sarquis

Institución: Universidad Tecnológica Intercontinental (UTIC)
Título: La estafa mediante sistemas informáticos hechos punibles considerando capaz de alterar el equilibrio financiero de la persona física en el orden económico en el régimen democrático.
Año: 2017

Asimismo, ampliamos el campo de búsqueda de los antecedentes en otros países sobre temas relacionados sobre con la protección y sanciones concernientes a la utilización datos de carácter privado la web en Encarnación.

- Carmen Carolina Soto Espinosa, Camilo Andrés Ducuara Cuervo.

  Institución: Universidad Católica de Colombia- Bogotá D.C. (Facultad de Ingeniería).

  Título: Protección de Datos en los servicios de internet

  Año: 2018

  Tipo de Trabajo: Trabajo de Investigación.

- Autores: Jazmín Acuña, Luis Alonzo Fulchi, Maricarmen Sequera.

  Institución: Investigación fue realizada con el apoyo de Privacy International, una organización del Reino Unido que monitorea las invasiones a la privacidad por parte de los gobiernos y corporaciones.

  Título: Sanciones y protección de los datos en redes sociales

  Año: 2017

  Asunción – Paraguay.

- Autor: Carlos Eduardo Saltor.
  Institución: Universidad Complutense de Madrid

  Tema: La protección de datos personales : estudio comparativo Europa-América con especial análisis de la situación Argentina.

  Año: 2013
  Tipo de Trabajo: Tesis Doctoral.
  Madrid.

Bases Teóricas

"En la sociedad de la información y el conocimiento, el manejo e intercambio de datos se ha convertido en una práctica habitual para las empresas de servicios" (Mendoza Enríquez, 2018, p. 23).

El uso de las Tics, están presentes en casi todos los procesos utilizados por el ser humano, lo cual ha optimizado todo tipo de recurso recursos y tiempo. Sin embargo, "también han propiciado una serie de desafíos en torno a la seguridad de la información, la protección de los datos personales y el cumplimiento de la regulación en la materia" (Mendoza Enríquez, 2018, p. 26).

Al hablar de protección de datos, debemos entender primeramente cómo funcionan estos datos, como son utilizados y cómo podemos protegerlos, sabiendo que están almacenados como, común mente lo llamamos las nubes, es importante saber quiénes pueden tener acceso a ellos y de qué manera puede perjudicar a las personas.

El impacto que tiene en la actualidad el uso de las tics con respecto a optimizar tiempo y recursos, se van elevando en grandes porcentajes al estar sometido a la pandemia afectada en el año 2019 y que aun continua sin ser erradicada, se utilizó de manera general en todo el mundo, en colegios, comercios y demás empresas que continuaron a pesar de la pandemia, fue la tecnología lo que nos mantuvo conectado y además mantuvo en un porcentaje la economía del país, mientras todo se paralizó.

Pero así también al utilizar en forma excesiva la tecnología tuvo también sus altibajos, con adicciones al internet y la utilización indebida de los datos privados, que es nuestro tema de investigación.

Datos Privados

Lo privado se define "en principio como oposición a lo común. Desde esta perspectiva, lo privado estaría conectado con el secreto en cuanto consecuencia de una acción de separar un determinado ámbito o conocimiento" (Freund, 1995, p. 238).

Para Freund, puede contemplarse “lo privado desde dos puntos de vista, desde el lado de lo público y desde el del individuo. Si bien desde el primer punto de vista lo privado aparece como la esfera de la interioridad y de la autonomía individuales”, (Freund, 1995, p. 239), visto desde el lado del individuo designa aquello que en el individuo está vuelto hacia el exterior, hacia los otros.

El termino privado también hace referencia a intimo o personal, es decir son palabras que engloban la acción del termino privado, de acuerdo con este termino los datos son de carácter personal, por ello no deben de ser compartidos bajo ninguna circunstancia.

De acuerdo con lo anterior:

> Pudiera sé distinguir entre intimidad en sentido estricto y «privacidad» o lo privado en sentido más amplio como ámbitos diferentes pero consecuentes: lo íntimo sería un concepto estricto de dimensiones propiamente individuales y lo privado sería un ámbito que, abarcando lo íntimo, lo supera. En esta línea, algunos autores han reivindicado la distinción entre lo íntimo y lo privado, no sólo en el plano antropológico, sino también en el jurídico (González Gaitano, 2010).

Dato Personal

Un dato personal es cualquier información concerniente a una persona. “El nombre y apellido, fecha de nacimiento, el teléfono, la dirección postal o el correo electrónico son datos personales. Como también lo son el número de cuenta, la matrícula del coche, los ingresos que se perciben o el historial médico” (Pérez, 2015, p. 21).

Estos datos son proporcionados por una persona, y recogidos en un fichero o base de datos de alguna entidad administrativa ya sea pública o privada, que utilizan estos datos para manejo de personal o cliente u otras cuestiones.

“A través de los datos personales almacenados (bienes adquiridos y lugar de adquisición, perfil en las redes sociales de una persona, así como sus

gustos, aficiones e intereses" (Pérez, 2015, p. 21). Nuestros datos dicen todo de nuestra persona.

Un claro ejemplo de estos datos almacenados son el uso de la identidad electrónica, que hoy en día, se debe registrar en la web, proporcionando todo tipos de datos ligados a bases de datos ya sean esto de policía nacional, registro del automotor, registro civil y las municipalidades, para validar estos datos, están establecidas unas series de preguntas personales que solo puede responder la persona interesada en obtener la identidad electrónica, además de solicitarles fotos de su cedula de ambos lados más una selfis con su cedula de identidad.

Varios son los procesos que se debe seguir para la creación de esta identidad, la cual debe de corroborar que realmente es la persona que está intentando registrar, cabe aclarar que al crear dicha identidad electrónica la persona tendrá acceso a muchos datos de carácter personal como ser, consulta de datos de la cedula de identidad, certificado de antecedente policial, certificado de nacimiento, acta de matrimonio, acta de nacimiento de los hijos, entre otros.

Los datos personales, como el nombre ya lo dice todo, no deben ser divulgados bajo ningún criterio, porque así, se vuelven vulnerables de ataques, estos datos deben ser manejados con absoluta seriedad, por ello los menores de edad, no deberían de utilizar el internet o ninguna red social que les solicite datos de carácter personal. Son muchos los riesgos que circulan en internet, por ellos se recomienda el control del uso de la tecnología en menores, muchas de las plataformas no permiten el acceso de estos, que son detectados al ingresar sus datos de carácter privado.

Sensibilidad de los datos

Esta sensibilidad "está establecida en función del daño que puede causar a una persona la revelación de dicha información. No es lo mismo revelar el teléfono de una persona que su historial médico, teniendo alguna enfermedad que puede provocar su exclusión social" (Pérez, 2015, p. 22).

Ahondamos sobre datos personales, que son los que caracterizan y definen a una persona, siendo esto así, estos datos son sensibles, porque representan la intimidad de cada individuo, porque no también representa su patrimonio, sabiendo que todo son registrado con los datos de la persona.

Normativas vigentes que pueden aplicarse en la ciudad de Encarnación

Antes de hablar de las normativas debemos entender de que manera deben ser respetadas las leyes dentro del territorio paraguayo, es decir cual es la ley máxima de nuestra nación. Según la pirámide se Kelsen, encabezando esta la constitución Nacional, es la normativa por la que rige todo el Paraguay en la cual está establecido en unos de sus artículos sobre el derecho a intimidad, antes de sumergirnos en este artículo, primero vamos a conocer que es el derecho a la intimidad.

Derecho a la intimidad

“La configuración jurídica de la intimidad es relativamente reciente. El primer texto que reconoce y positiva el derecho a la intimidad personal y familiar es la Declaración Universal de Derechos Humanos, de 1948, en su art. 12”. (Martínez de Pisón, 2016, 410).

El art. 8.1 del Convenio Europeo para “la Protección de los Derechos Humanos y las Libertades Fundamentales, de 1950. El art. 17 del Pacto Internacional de Derechos Civiles y Políticos de 1966 acabará por consagrar el reconocimiento de la intimidad como derecho fundamental en el ámbito internacional” (Martínez de Pisón, 2016, 411).

El derecho fundamental a la intimidad tiene este origen cercano y, sin embargo, se le considera uno de los derechos y libertades perteneciente a la primera generación.

El derecho a la intimidad es importante, está protegido por artículo 33 de la constitución nacional, que establece:

ARTICULO 33 - DEL DERECHO A LA INTIMIDAD:

La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, está exenta de la autoridad pública.

Se garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas. (Constitución Nacional, 2005).

Bien jurídico protegido

El bien jurídico cumple funciones “de gran relevancia para las ciencias penales. Entre ellas, la afectación de un bien jurídico permite fundamentar el castigo punitivo de las conductas que lo lesionan o ponen en peligro y constituye un requisito ineludible para el ejercicio del ius puniendi” (Mayer Lux, 2017, p. 10).

El bien jurídico hace referencia a una serie de derechos que tutelan tales como, la salud, la vida, la libertad, el patrimonio, la seguridad, etc.

La constitución nacional del Paraguay el primer bien jurídico que esta protege es el derecho a la vida que se encuentra establecido en su artículo 4to.

Articulo 4 - del Derecho a la Vida:
El derecho a la vida es inherente a la persona humana. Se garantiza su protección, en general, desde la concepción. Queda abolida la pena de muerte. Toda persona será protegida por el Estado en su integridad física y psíquica, así como en su honor y en su reputación. La ley reglamentará la libertad de las personas para disponer de su propio cuerpo, sólo con fines científicos o médicos (Constitución Nacional, 2005, p. 6).

Este derecho es fundamental en ella podemos resaltar otras cuestiones que pueden aplicarse al delito cometido por medios informáticos como el uso indebido de datos de carácter privado, siendo nuestra constitución clara al

establecer que todas las personas están protegidas en su integridad psíquica y en su honor y reputación, al utilizar estos se comete un delito y daña la integridad del ser humano, al ser utilizados con fines ilícitos afectando y desprestigiando a la persona víctima de este delito.

> En comparación con el bien jurídico, el concepto de "delito informático": Ha sido abordado por un número mucho menor de autores, fundamentalmente porque constituye un término relativamente reciente, cuyo surgimiento no es imaginable sin la existencia de computadoras. Se trata, no obstante, de una expresión equívoca, ya que se la emplea para aludir a realidades que no son coincidentes entre sí (Mayer Lux, 2017, p. 10).

El término criminalidad informática “en sentido amplio o criminalidad cometida "mediante" sistemas informáticos, suele utilizarse para referir la comisión de delitos tradicionales a través de computadoras o de internet (v.gr. extorsión o difusión de pornografía infantil)” (MarberthKubicki, 2010, p. 11).

Esta terminología criminalidad informática, está en crecimiento con el uso más frecuentes de las tics, hoy en día se utiliza programas informáticos para optimizar la rapidez y eficacia de los trabajos que deben realizar las empresas o instituciones, por ello también se han creado nuevas formas de delitos y estos son a través de medios informáticos.

> En cambio, la expresión criminalidad informática en sentido estricto: Criminalidad cometida "respecto de" o "contra" sistemas informáticos o, simplemente, criminalidad informática, suele emplearse para aludir a comportamientos delictivos que inciden, directamente, en un sistema informático (v.gr. sabotaje o espionaje informático).
>
> Por su parte, el concepto de "cibercrimen" suele utilizarse para aludir a la criminalidad informática (en sentido amplio o estricto) llevada a cabo a través de internet (MarberthKubicki, 2010, p. 11).

Los delitos informáticos comúnmente que se cometen en la ciudad de Encarnación, son las estafas por redes sociales o, el robo de redes sociales de

uso personal como ser WhatsApp o Facebook, que se denuncian a través de los medios de comunicaciones (*Ver Apéndice B: Denuncian Sistemas Delictivos que roba cuentas de WhatsApp*).

> De acuerdo con la doctrina:
> No toda conducta (delictiva) que recae en un sistema de tratamiento automatizado de información constituye un delito informático en estricto sentido.
>
> Por el contrario, ha de tratarse de comportamientos que incidan en el software o soporte lógico, esto es, en los programas, instrucciones y reglas informáticas que permiten el procesamiento de datos en una computadora.
>
> A diferencia de ellos, las conductas que solo afectan el hardware o soporte físico de un sistema informático, o sea, los componentes que integran la parte material o tangible de una computadora, pueden ser subsumidas, en términos generales, en los delitos (patrimoniales) clásicos y, muy especialmente, en el tipo penal de daños (MarberthKubicki, 2010, p. 11).

Los delitos informáticos “no tutelan un bien jurídico específico y que en ellos "lo informático" no es más que un contexto delictivo o un particular medio de afectación de bienes jurídicos tradicionales, como la intimidad o privacidad, el patrimonio o la fe pública” (Mata, 2017, p. 15).

Pero cual sería la diferencia entre un delito informático y otros delitos, sería el proceder es decir la forma, no así el fondo, en otros delitos también se tiene el uso indebido de datos, alteración de datos, entre otros que afectan a los datos de carácter privado, sería el modo operandi la diferencia entre uno y delito y otro, pero aun así no deja de ser delito, el daño es causado al utilizar estos datos está presente.

Por ello también deben ser denunciados, ahora bien, al ser delitos informáticos la pregunta más frecuente sería donde se puede realizar este tipo de denuncia.

Análisis del bien jurídico protegido

La consideración del Derecho penal como ultima ratio a la hora de solucionar un problema jurídico, impone la necesidad de tener bien claras las razones por las que se debe justificar la intervención coercitiva del Estado.

Ya en el lejano Derecho romano, se entendía que la facultad de castigar del Estado:

De la comunidad misma, debía estar justificada por un precepto imperativo y general, como lo demuestra el aforismo nullum crimen, nulla poena sine lege. Y hoy en día, esta “legalidad del Derecho penal” se ve reforzada por la una nimidad de la doctrina, que resalta por encima de cualquier otra cosa, la función protectora de bienes jurídicos que posee la norma penal (Muñoz Conde, 2015).

Al definir el bien jurídico protegido, que ya lo definimos también como datos personales, va a legitimar la norma penal, siguiendo criterios constitucionalmente sustanciales, como la proporcionalidad, la legalidad o el principio de intervención mínima, por ello la discusión de los datos poder ser protegidos o sancionados a quien de alguna manera se encuentre culpable de vulnerarlos.

Primero se debe partir de entender la importancia del estudio de los datos de carácter privado, sobre todo si estos pueden ser protegidos y sancionados al ser mal utilizados por terceras personas para comer un fin ilícito y quienes son los responsables de proteger estos datos.

El delito de estafa informática. Según expone Galán Muñoz, el delito de estafa informática se caracteriza por:

> Ser un delito protector de un bien jurídico intermedio; siendo considerado un delito de peligro-lesión. Como punto de partida para el desarrollo de la tesis, niega la necesidad de interpretar de forma vinculada el delito de estafa y el de estafa informática. Así, considera que este nuevo tipo delictivo debe entenderse protector no sólo de bienes jurídicos individuales; sino de bienes jurídicos eminentemente colectivos, siendo

> clasificado entre los delitos económicos en sentido amplio. De ahí, la concepción del bien jurídico como intermedio, pues protege, según este sector de la doctrina, intereses de naturaleza muy diversa. El problema que surge en este punto es diferenciar este tipo delictivo frente a los tipos que pueden considerarse como meros delitos pluriofensivos de peligro (Galan Muñoz, 2015, p. 118).

Como se ha visto uno de los delitos a través de la web utilizando datos de carácter privado, es la estafa informática como delito que son cometidos diariamente, a pesar de parecer inofensiva estas estafas también dañan a las víctimas, no solo en su patrimonio, sino también en su intimidad y reputación.

Peligros derivados del uso de las nuevas tecnologías

Una vez asumida la realidad del fenómeno informático, presente en cualquier ámbito del quehacer humano, analizaremos los principales peligros que del mismo se derivan, centrándonos en la protección de los derechos fundamentales en relación con las personas y el uso de las nuevas tecnologías de la información. Así, podemos hablar en primer lugar de los peligros en relación a los derechos de la personalidad del individuo, fundamentalmente los ataques a su intimidad personal. En segundo lugar, los peligros relativos al sistema de garantías y contrapesos que caracteriza a la organización del Estado de Derecho (Castillo Jimenez, 2012, p. 36).

Los aspectos delictivos siempres son un peligros, sin importar la tecnica que utilicen para cometer los actos delictivos contra un individuo, el estado debe de garantizar los derechos y las libertades de utilizar sus datos de carácter ersonal sin temor a que puedan ser vulnerados.

Peligros relacionados con internet

> Los principios básicos de la protección son de naturaleza general y se aplican a todas las tecnologías de la información, por tanto, a todos los

> tipos de redes abiertas o cerradas, incluyendo Internet y sus integrantes, proveedores de acceso, de servicios y usuarios.
>
> Las Leyes de Protección de Datos personales informatizados, que nacen para proteger al titular de la información en lo que se refiere a su intimidad personal, restringen la circulación no autorizada de datos que pueden representar una invasión de la esfera privada.
>
> En Internet, se recomienda ampliamente a los usuarios, operadores y proveedores tomar todas las medidas necesarias antes de divulgar un texto o imagen que pueda suponer una violación del derecho a la intimidad (Castillo Jimenez, 2012, p. 39).

La amenza a la intimidad es algo inminente, al estar en la web nuestros datos personales, y cada ves que ingresamos a utilizar las herramientas utilizadas con acceso a internet como ser correo electronico, redes sociales tales como whatsapp, faceboock, instagram y correos electronicos, todos ellos para ser utilizados requieren del ingreso de datos de carácter personal y privados, por ello toda la intimidad de las personas estan en estas herramientas y del uso que le dan a cada una de ellas.

En la constitución nacional mencionado en los aspectos legales es lo que garantiza la proteccion de dichos datos, que castiga las violacion es del derecho a la intimidad.

Definición de Protección de datos de carácter personal

El núcleo duro del problema de la protección efectiva de los datos personales debe plantearse desde la visión de Guillermo Consentino:

> Cuando afirma que la existencia de bases de datos en el ámbito del Estado llamadas por su ubicación "públicas" y bases de datos en manos de personas u organizaciones privadas o no estatales, denominadas, siguiendo el mismo criterio "privadas ", no necesariamente cambia la condición de los datos personales que puedan contener y no disminuye el nivel de protección que la ley les asigna (Acuña Llamas, 2015, p. 31).

La Protección de Datos de Carácter Personal es un derecho fundamental que tienen todas las personas físicas y también jurídicas, para garantizar su vida privada y supone el control y poder de disposición de la información relativa a su esfera tanto pública como privada. Uno de los medios utilizados en la web para utilizar datos de carácter privado es el Phishing.

El phishing[1]

> Se configura como una de las conductas fraudulentas con más repercusión en la actualidad. Se trata de una práctica encuadrada en el campo de la estafa, que consiste en la adquisición de información confidencial (de carácter económico, personal, o de cualquier otra índole) de forma ilícita, sin consentimiento de su titular; mediante el uso de ingeniería social Sánchez Bernal, 2009, p. 107).

El phishing es uno de los delitos informáticos más comes en internet que, de forma ilícita acceden a los datos de carácter privado, estos datos son vulnerados y son utilizados para fraudes o para dañar a la persona víctima de esta nueva forma des estafa.

El infractor, conocido como phisher, puede simular ser una persona o empresa
de confianza:

> Cometiendo el hecho ilícito mediante una comunicación electrónica aparentemente normal (correo electrónico, mensajería instantánea) o incluso, mediante una llamada telefónica. La persona que lleva a cabo esta actividad delictiva suele camuflarse bajo el nombre de la entidad bancaria habitual u otros servicios contratados por el sujeto engañado con el fin de conseguir códigos, contraseñas, números de tarjetas de

[1] En seguridad informática, la “ingeniería social” es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Se trata de obtener datos, acceso o privilegios en los sistemas de información, que permitan realizar un acto perjudicial para un sujeto, o que lo exponga a un riesgo o abuso. Engloba, por tanto, cualquier manipulación para conseguir información privilegiada.

> crédito u otro tipo de información, especialmente bancaria (Sánchez Bernal, 2009, p. 107).

El autor Sánchez explica la forma en que actúan estos infractores operando a través de la web y como la personas caen en estos tipos de actos delictivos, para ir lejos también están las llamadas, que por medios de engaños estos caen y consiguen extraer plata de sus víctimas, estos con su astucia revelan datos de carácter privado, como nombre de los hijos o del conyugue, en algunos casos direcciones, en la ciudad de Encarnación este tipo de estafa es muy común.

Importancia de la protección de los datos de carácter privado. “Para evitar que sean utilizados con una finalidad distinta para la cual los proporcionaste, evitando con ello se afecten otros derechos y libertades” (Bravo Resendiz, 2021).

Leyes de protección de datos. “tienen por objeto garantizar y proteger, en cuanto al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar” (Bravo Resendiz, 2021).

Para que estos datos sean protegidos se deben establecer diversas obligaciones y responsabilidades que deben ser observadas por las empresas que traten datos personales, además de las personas que utilizan la web como entretenimiento y tener prudencia de las publicaciones personales que realizan. Además, entre ellas se encuentran brindar información suficiente a los titulares sobre el tratamiento de sus datos personales, así como obtener su consentimiento.

Finalidad de la protección de datos de carácter personales. “Garantizar la protección y el buen tratamiento de los datos de carácter personal” (Bravo Resendiz, 2021).

Marco Legal

En este apartado se abordará el desarrollo de los aspectos legales de este trabajo de investigación con respecto al tema investigado protección y sanciones concernientes a la utilización de datos de carácter privado en la web dentro de la ciudad de encarnación, por ello se estará analizando y asentando las leyes y normativas de Paraguay, éstas figuras jurídicas que han sido técnicamente delineadas y profundamente examinadas, que son utilizados en la ciudad de Encarnación para su protección o sanciones al utilizar datos de carácter privado, para dar respuesta a los objetivos establecidos en el presente trabajo de investigación.

Constitución Nacional de la República del Paraguay

En la reforma constitucional del año 1992, se incorporan a la Constitución Nacional (CN) (Asamblea Constituyente, 1992) las siguientes figuras:

> Artículo 33 - Derecho a la Intimidad:
> La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, está exenta de la autoridad pública. Se garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas (Constitución Nacional, 2005, p. 33).

Artículo 36 – Inviolabilidad del patrimonio documental y de la comunicación privada:

> El patrimonio documental de las personas es inviolable. Los registros, cualquiera sea su técnica, los impresos, la correspondencia, los escritos, las comunicaciones telefónicas, telegráficas o de cualquier otra especie, las colecciones o reproducciones, los testimonios y los objetos de valor testimonial, así como sus respectivas copias, no podrán ser examinados, reproducidos, interceptados o secuestrados sino por orden judicial para

> casos específicamente previstos en la ley, y siempre que fuesen indispensables para el esclarecimiento de los asuntos de competencia de las correspondientes autoridades.
>
> La ley determinará modalidades especiales para el examen de la contabilidad comercial y de los registros legales obligatorios. Las pruebas documentales obtenidas en violación a lo prescripto anteriormente carecen de valor en juicio. En todos los casos se guardará estricta reserva sobre aquello que no haga relación con lo investigado (Constitución Nacional, 2005, p. 34).

> Artículo 23 – De la prueba de la verdad:
> La prueba de la verdad y de la notoriedad no serán admisibles en los procesos que se promoviesen con motivo de publicaciones de cualquier carácter que afecten al honor, a la reputación o a la dignidad de las personas, y que se refieran a delitos de acción penal privada o a conductas privadas que esta Constitución o la ley declaran exentas de la autoridad pública.
>
> Dichas pruebas serán admitidas cuando el proceso fuera promovido por la publicación de censuras a la conducta pública de los funcionarios del Estado, y en los demás casos establecidos expresamente por la ley (Constitución Nacional, 2005, p. 31).

La Constitución Nacional, es la norma legal por la cual se rige todo el Paraguay, es decir es utilizada por ende en la ciudad de encarnación, como vemos los artículos examinados, hacen referencia a la utilización de datos de carácter privado y que pueden utilizarse en casos excepcionales, como observaremos en las leyes siguientes que esbozaremos en este apartado.

Derecho a Rectificación

Artículo - 28: Se reconoce el derecho de las personas a recibir información veraz, responsable y ecuánime.

> Las fuentes públicas de información son libres para todos. La ley regulará las modalidades, plazos y sanciones correspondientes a las mismas, a fin de que este derecho sea efectivo.
>
> Toda persona afectada por la difusión de una información falsa, distorsionada o ambigú a tiene derecho a exigir su rectificación o su aclaración por el mismo medio y en las mismas condiciones que haya sido divulgada, sin perjuicio de los demás derechos compensatorios (Constitución Nacional, 2005, p. 32).

Hablando con anterioridad a la privacidad, el único "antecedente de protección en nuestro país corresponde a la época del régimen totalitario de Alfredo Stroessner y se encontraba en la Constitución del 1967, enmendada en 1977. En su artículo 50 hablaba de la protección del honor y la reputación" (Pappalardo Zaldívar, 1992, p. 15)

Garantía Constitucional de Hábeas Data

> El artículo 135 Hábeas Data dispone lo siguiente:
> Toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Además, la persona podrá requerir la actualización, rectificación o destrucción de los datos personales, que fueran erróneos o que afecten de forma ilegítima sus derechos ante las autoridades competentes (Constitución Nacional, 2005, p. 58).

Información de Carácter Privado – Ley 1682/2001 y modificaciones

Como se desarrolló con anterioridad los datos de carácter privado y personal, son datos sensibles lo cual en esta ley menciona al respecto que el titular de los datos personales que se concibe como persona natural respecto de la cual se predica cierta información puede acudir a un tribunal para ejercer

sus derechos constitucionales a través de habeas data u otras de amparo ante infracciones cometidas en su contra.

La ley 1682 y sus modificaciones, menciona que los datos son de libre acceso y que las personas tienen el derecho para almacenarlo y al mismo tiempo utilizarlo, así como lo hacen los bancos y otras entidades públicas, pero lo central en la discusión es la necesidad o no de que el Estado adopte una Institucionalidad que vele el cumplimiento de la normativa sobre tratamiento de datos personales y que no quede sólo a la gestión de agentes intervinientes. Es decir, que el Estado genere mecanismos y garantías para la gestión de los datos personales.

En Paraguay los datos personales están regulados por la Ley N.º 1682/2001 “Que reglamenta la información de carácter privado” y su posterior modificación por la Ley 1969 del año 2002 y 5.543/2015, estableciéndose en su artículo primero lo siguiente:

Artículo 1°- “Toda persona tiene derecho a recolectar, almacenar y procesar datos personales para uso estrictamente privado” (LEY N° 1.682, 2012, p. 1).

Así mismo en artículo segundo de la misma ley establece que los datos son libres, para todos.

> Artículo 2°- Las fuentes públicas de información son libres para todos. Toda persona tiene derecho al acceso a los datos que se encuentren asentados en los registros públicos, incluso los creados por la Ley Nº 879 del 2 de diciembre de 1981, la Ley Nº 608 del 18 de julio de 1995, y sus modificaciones (LEY N° 1.682, 2012, p. 1).

Dicha Ley asume que la acción de protección recae en la persona afectada, siendo más cercana a la doctrina norteamericana que implica dejar el cumplimiento de la normativa a las partes involucradas y evitar la intervención del Estado, salvo en cuanto al rol que compete a los tribunales de justicia.

Artículo 3°- Es lícita la recolección, almacenamiento, procesamiento y publicación de datos o características personales, que se realicen con fines

científicos, estadísticos, de encuestas y sondeos de la opinión pública o de estudio de mercados, siempre que en las publicaciones no se individualicen las personas o entidades investigadas.

El artículo tercero estable que es lícita solo para casos que el estado así lo requiera y deba utilizar esos datos con fines de recolección de información, estudio de mercado y demás, pero solo en estos casos son lícitos.

La Ley 1682/2001 (y sus modificaciones) tiene un enfoque meramente economicista, como ya se mencionó solo le permite al estado la utilización de esos datos que están guardados en la web o mejor dicho en una base de datos utilizadas por entes públicos, ya que regula casi exclusivamente los sistemas de información crediticia en las entidades bancarias y financieras, sin cubrir enfoques social y comunitario de la información personal.

Es de suma importancia realizar el análisis de esta ley vigente, que hace alusión a al tema principal, datos de carácter privado, utilizamos los principios propugnados por el sistema europeo de protección de datos personales, para el esclarecimiento del tema investigado, sobre la protección y sanciones al utilizar datos de carácter privado en la web en la ciudad de Encarnación.

Código Penal – Ley N° 1160/97

Capítulo VII los hechos punibles contra el ámbito de vida y la intimidad de la persona.

Entre ellos se encuentran: Artículo 143.- Lesión de la intimidad de la persona:

1º El que, ante una multitud o mediante publicación en los términos del artículo 14, inciso 3º, expusiera la intimidad de otro, entendiéndose como tal la esfera personal íntima de su vida y especialmente su vida familiar o sexual o su estado de salud, será castigado con pena de multa.

2º Cuando por su forma o contenido, la declaración no exceda los límites de una crítica racional, ella quedará exenta de pena.

> 3º Cuando la declaración, sopesando los intereses involucrados y el deber de comprobación que según las circunstancias incumba al autor, sea un medio adecuado para la persecución de legítimos intereses públicos o privados, ella quedará exenta de pena.
> 4º La prueba de la verdad de la declaración será admitida sólo cuando de ella dependiera la aplicación de los incisos 2º y 3º (Código Penal, 2004, p. 164).

Dentro de nuestro código penal se encuentra penado la lesión a la intimidad de la persona, y esta lesión se produce cuando una persona es vulnerada en su intimidad al utilizar sus datos de carácter privado en la web, para algún hecho delictivo u otros fines.

Lesión del derecho a la comunicación y a la imagen.

Artículo 144.- Lesión del derecho a la comunicación y a la imagen

> 1º El que sin consentimiento del afectado: 1. escuchara mediante instrumentos técnicos; 2. grabara o almacenará técnicamente; o 3. hiciera, mediante instalaciones técnicas, inmediatamente accesible a un tercero, la palabra de otro, no destinada al conocimiento del autor y no públicamente dicha, será castigado con pena privativa de libertad de hasta dos años o con multa.
> 2º La misma pena se aplicará a quien, sin consentimiento del afectado, produjera o transmitiera imágenes: 1. de otra persona dentro de su recinto privado; 2. del recinto privado ajeno; 3. de otra persona fuera de su recinto, violando su derecho al respeto del ámbito de su vida íntima.
> 3º La misma pena se aplicará a quien hiciera accesible a un tercero una grabación o reproducción realizada conforme a los incisos 1º y 2º.
> 4º En los casos señalados en los incisos 1º y 2º será castigada también la tentativa.
> 5º La persecución penal del hecho dependerá de la instancia de la víctima, salvo que el interés público requiera una persecución de oficio. Si la víctima muriera antes del vencimiento del plazo para la instancia sin haber renunciado a su derecho de interponerla, éste pasará a sus parientes.

La violación del secreto de la comunicación y el artículo 143.- Lesión a la intimidad de la persona, que estuvimos resaltando con anterioridad, hace alusión directa a la exposición pública de la intimidad de la persona, de su vida familiar, sexual y su estado de salud.

"El código penal también se utiliza para forzar a las empresas a que implementen mecanismos informáticos que eliminen de manera automática la información de los datos no publicables, conforme a la Ley 1682/01 y modificaciones" (Acuña, Fulchi, & Sequera, 2017, p. 24).

Código de Organización Judicial

La ley 1682/01 modificada por la Ley 1969/02, en su artículo 2 establece: Toda persona tiene derecho a recolectar, almacenar y procesar datos personales para uso estrictamente privado.

Las fuentes públicas son de libre acceso para todos. Toda persona tiene derecho al acceso a los datos que se encuentran asentados en los registros, incluso los creados por la Ley 879 del 2 de diciembre de 1981 la Ley N° 608 del 18 de julio de 1995, y sus modificaciones (LEY Nº 1969 , 2010, p. 1).

Ley Nº 642/95 de Telecomunicaciones

Dicha ley regula todo tipo de emisión y propagación de las señales de comunicación electromagnéticas que son de dominio público del Estado. Asimismo, crea al ente regulador denominado Comisión Nacional de Telecomunicaciones (CONATEL) que deberá velar por el cumplimiento de la ley.

La misma incluye aspectos de tratamientos de datos y estos son de carácter en su mayoría privado en el Título IX

Régimen de protección a abonados y usuarios.

Artículo 91.-Es obligación de los titulares de la explotación de servicios públicos de telecomunicaciones publicar y distribuir en forma gratuita las

> guías y nómina de sus respectivos usuarios abonados, de conformidad con las normas reglamentarias correspondientes. Los usuarios tendrán derecho a la no inclusión de sus nombres en dichas guías y nóminas (Ley Nº 642/95, 2015).

Dichos servicios públicos requieren de datos de carácter personal para poder ser utilizados, que al mismo tiempo también son publicados con esos datos que llamamos también sensibles que en manos equivocadas son vulnerados y mal utilizados afectando a la persona cual dato está siendo utilizado de forma ilícita.

Resolución 1350/2002 Por el cual se establece la Obligatoriedad de registro de detalles de llamadas por el plazo de seis (6) meses

La Resolución 1350/2002 de Conatel[2] contradice la Ley 642/95 de Telecomunicaciones expresados en los artículos 89 y 90 sobre la inviolabilidad de la correspondencia de las telecomunicaciones y el Decreto del Poder Ejecutivo 14135/96[3]. Esta Resolución otorga facultades a las compañías operadoras de servicios de telefonía a almacenar por un periodo de seis meses el registro de detalles de llamadas de todos los usuarios en Paraguay:

> Artículo. 1.- Establecer el plazo de seis (6) meses, como periodo obligatorio de conservación del registro de detalles de llamadas entrantes y salientes de todas las líneas que conforman la cartera de clientes de las diferentes operadoras del servicio de telefonía móvil celular (STMC) y/o Sistema de Comunicación Personal (PCS) (Resolución Nº 1350, 2002, p. 2).

Estos plazos son indispensables para tener un repositorio de evidencias si los datos de la CONATEL son vulnerados, como las famosas llamadas pinchadas o intervenidas, sirven de prueba, ahora, el tiempo de guardado tal

[2] Comisión Nacional de Telecomunicaciones (CONATEL). RESOLUCIÓN Nº 1350/2002.- Por la cual se establece la obligatoriedad de registro de detalles de llamadas por el plazo de seis meses. (Comisión Nacional de Telecomunicaciones (CONATEL), s. f.)
[3] Por el cual se aprueba las normas reglamentarias («Ley No 642/95 “De telecomunicaciones”.», s. f.).

vez no sería lo suficiente, pero al ser grandes cantidades de datos y todo estos de carácter personal, siendo que las llamadas entre una persona y otra son muy personales, también son tipificados como delitos.

Ley N° 5.830/17 “Que prohíbe la publicidad no autorizada por los usuarios titulares de telefonía móvil”

Antes de adentrarnos a esta ley primeramente conoceremos cuál es su objeto lo cual se encuentra establecido en su artículo primero, protegiendo los datos de carácter privado utilizando teléfonos móviles.

Objeto de la ley.

Artículo 1° Objeto. El objeto “de la presente ley es proteger a los titulares o usuarios autorizados de los servicios de telefonía, en cualquiera de sus modalidades, de los abusos del procedimiento de contacto, publicidad, oferta, venta y regalo de bienes o servicios no solicitados” (LEY N° 5.830, 2012, p. 1).

Inscripción.

Artículo 4° Inscripción:

> Las inscripciones y bajas en el Registro Nacional serán gratuitas y podrán ser realizadas tanto de manera personal ante la Secretaría de Defensa del Consumidor y el Usuario (SEDECO), como por otras vías que dicha Institución reglamente. En todo caso se deberá dejar constancia de la identidad del titular o usuario autorizado y del número de teléfono móvil.
>
> A fin de corroborar que los datos personales proveídos por los interesados sean verídicos, la Secretaría de Defensa del Consumidor y el Usuario (SEDECO), deberá contar con las bases de datos necesarios para ello, los cuales serán brindados por las empresas proveedoras de telefonía móvil, conforme a la reglamentación de la presente ley[4].

[4] Aprobado el Proyecto de Ley por la Honorable Cámara de Diputados, a los seis días del mes de diciembre del año dos mil dieciséis, y por la Honorable Cámara de Senadores, a los dieciocho días del mes de mayo del año dos mil diecisiete, queda sancionado, de conformidad con lo dispuesto en el artículo 204 de la Constitución Nacional.

> La periodicidad con que se actualizará el Registro Nacional será reglamentada por la Secretaría de Defensa del Consumidor y el Usuario (SEDECO) (LEY N° 5.830, 2012, p. 1).

Por otra parte, tenemos el artículo 4to que hace alusión a la inscripción, para utilizar una telefonía móvil, se deben solicitar los datos personales tal como lo establece dicho artículo, estos datos son guardados en un servidor web, por ende, dichos datos pueden ser vulnerados por expertos en la materia y utilizar dichos datos para fines ilícitos o realizar estafas.

Se observa claramente que en todo lo que hacemos siempre están comprometido nuestros datos para cualquier tipo de diligencia que realicemos.

Marco Conceptual

En este apartado se realice la sistematización y exposición de los conceptos que son relevantes y fundamentales para el desarrollo de la investigación, que aboca el tema protección y sanciones a la utilización de datos de carácter privado en la web, dentro de la ciudad de Encarnación. Según la RAE se establece los siguientes conceptos:

Protección

"Acción y efecto de proteger" (RAE, 2021).

Datos[5]

"Información sobre algo concreto que permite su conocimiento exacto o sirve ara deducir las consecuencias derivadas de un hecho" (RAE, 2021).

Es importante estos dos conceptos que agrupados hacen la conjunción del tema investigado, del cual se conceptualizara de la siguiente manera:

Protección de datos

"Sistema legal que garantiza la confidencialidad de los datos personales de las administraciones públicas u otras organizaciones. Agencia de protección de datos" (RAE, 2021).

Carácter[6]

"Conjunto de rasgos, cualidades o circunstancias que indican la naturaleza propia de una cosa o la manera de pensar y actuar de una persona o una colectividad, y por los que se distingue de las demás" (RAE, 2021).

---

[5] Además, la Rae lo califica de la siguiente manera:
Información dispuesta de manera adecuada para su tratamiento por una computadora.

[6] Según la Rae además se refiere a Datos como:
Estilo o forma de los signos de la escritura o de los tipos de la imprenta. Carácter redondo.

Personal[7]

"Que es propio o característico de una determinada persona" (RAE, 2021).

Ley[8]

"Regla o norma establecida por una autoridad superior para regular, de acuerdo con la justicia, algún aspecto de las relaciones sociales" (RAE, 2021).

Sanción[9]

"Pena establecida para el que infringe una ley o una norma legal" (RAE, 2021).

Principio[10]

"Punto de donde parte, nace o surge una cosa" (RAE, 2021).

Internet

"Red informática de nivel mundial que utiliza la línea telefónica para transmitir la información" (RAE, 2021).

Web[11]

Conjunto de información que se encuentra en una dirección determinada de internet. Es una palabra inglesa que significa red o telaraña. Se designa como 'la web' al sistema de gestión de información más popular para la trasmisión de datos a través de internet. (RAE, 2021).

---

[7] Personal: Perteneciente o relativo a la persona**.**

[8] Ley: En el régimen constitucional, disposición votada por las Cortes y sancionadas por el jefe del estado.

[9] Sanción: Mal dimanado de una culpa o yerro y que es como su castigo o pena**.**

[10] Principio: Norma o idea fundamental que rige el pensamiento o la conducta**.**

[11] Además, la palabra web viene del inglés web (red, malla) y se refiere a la Internet, o sea, la red electrónica que conecta a todas las computadoras. De ahí tomamos las siglas www (wide world web = red a lo ancho del mundo).

Código

"Conjunto ordenado de leyes de un país" (RAE, 2021).

Privacidad

"Es aquello que una persona lleva a cabo en un ámbito reservado (vedado a la gente en general), por lo tanto, tiene derecho a mantener su privacidad fuera del alcance de otras personas, asegurándose la confidencialidad de sus cosas privadas" (RAE, 2021).

Público

"Que se realiza ante un grupo de personas atentas a lo dicho o hecho o para que sea difundido y conocido por la gente" (RAE, 2021).

Derecho

"Conjunto de normas que imponen deberes y normas que confieren facultades, que establecen las bases de convivencia social y cuyo fin es dotar a todos los miembros de la sociedad de los mínimos de seguridad, certeza, igualdad, libertad y justicia" (RAE, 2021).

Información[12]

"Noticia o dato que informa acerca de algo" (RAE, 2021).

Software[13]

"Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas" (RAE, 2021).

---

[12] RAE: Además, puede conceptualizarse como la Acción y efecto de informar.

[13]Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

Hardware[14]

“Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático” (RAE, 2021).

Hechos punibles

“Es aquel acontecimiento que, de cometerse este asociado a una pena, definida en una ley penal cualquiera. Es lo que está establecido en el tipo penal” (RAE, 2021).

Telecomunicaciones[15]

“Sistema de comunicación a distancia que se realiza por medios eléctricos o electromagnéticos” (RAE, 2021).

Daño[16]

“El daño se define como el menoscabo que, a consecuencia de un acaecimiento o evento determinado, sufre una persona, ya en sus bienes vitales naturales, ya en su propiedad, ya en su patrimonio” (RAE, 2021).

Electrónica

“Parte de la física que estudia los cambios y los movimientos de los electrones libres y la acción de las fuerzas electromagnéticas y los utiliza en aparatos que reciben y transmiten información” (RAE, 2021).

[14] Equipo (‖ conjunto de aparatos de una computadora).
[15] Asimismo, puede conceptualizarse como el, sistema de transmisión y recepción a distancia de señales de diversa naturaleza por medios electromagnéticos.
[16] RAE: Delito consistente en causar daños de manera deliberada en la propiedad ajena. Estos daños también pueden darse en la utilización incorrecta de los datos de carácter privado.

Jurisprudencia[17]

"Conjunto de sentencias o resoluciones judiciales emitidas por órganos judiciales y que pueden repercutir en sentencias posteriores. En algunos países, la jurisprudencia puede ser una fuente del Derecho, directa o indirecta" (RAE, 2021).

Víctima[18]

"Persona física que directa o indirectamente ha sufrido daño o el menoscabo de sus derechos producto de una violación de sus derechos" (RAE, 2021).

[17]Criterio sobre un problema jurídico establecido por una pluralidad de sentencias concordes
[18] Persona que padece daño por culpa ajena o por causa fortuita.

Definición de operacionalización de las variables

Variable	Datos privados	Sanciones
Definiciones Conceptuales	Es toda la información que te identifica, te hace identificable y te distingue de los demás. Asimismo, es "toda información sobre una persona física identificada o identificable".	se denomina la pena que establece una ley o norma para quien la viole o la incumpla. En Derecho, se puede decir que la sanción es la consecuencia que tiene una conducta que constituya una infracción para la norma jurídica.
Definiciones operacionales	De acuerdo a las bibliografías consultadas datos son, Nombre, origen étnico y racial, lengua materna, domicilio, teléfono, correo electrónico, firma, contraseñas, RFC, CURP, fecha de nacimiento, edad, nacionalidad, estado civil	De acuerdo a las bibliografías consultadas, estas sanciones se dan por el uso ilícito de los datos personales de acuerdo a nuestra investigación. Asimismo, su el objetivo principal no es el castigar la falla, el objetivo principal es el generar un cambio de conducta.

Marco Metodológico

En este apartado se presenta la metodología utilizada para la sustentación de la investigación realizada para la obtención del título de grado.

Tipo de Investigación

Este trabajo investigativo de acuerdo con el fin fue una investigación básica, según el alcance temporal fue seccional, de acuerdo con el enfoque ha sido cuantitativo, según el marco en el cual se desarrolló fue de campo (Barón, 2021, p. 19).

Cualitativo. “Se fundamenta en un esquema deductivo y lógico que busca formular preguntas de investigación e hipótesis para posteriormente probarlas” (Sampieri, 2010).

El tipo de investigación que utilizaré para la recolección de datos será del tipo cuantitativo, ya que, dentro del ambiente en el cual muchas veces se da la violación o el uso incorrecto de la información de carácter personal, podría obtener descripciones detalladas de situaciones, eventos, personas, interacciones, conductas observadas y testimonios.

Diseño de investigación

Al ser un estudio no experimental, implica no manipular de forma intencional las variables independientes debido a que ya sucedieron, ni asignar aleatoriamente a los participantes. En este tipo de investigación se observan los fenómenos, es decir el estudio de investigación protección y sanciones concernientes a la utilización de datos de carácter privado en la web.

No experimental. Podría definirse como la investigación que se realiza sin manipular deliberadamente variables. Es decir, se trata de estudios donde no hacemos variar en forma intencional las variables independientes para ver su efecto sobre otras variables. (Sampieri, 2010).

El diseño de esta investigación será no experimental porque me estaré basando en casos ya existentes, personas que fueron afectadas por el uso no autorizado de sus datos personales en la web en la ciudad de Encarnación, así también me estaré basando en los documentos, testimonios y jurisprudencias ya ocurridos por lo tanto no será experimental.

Nivel de conocimiento esperado

Correlacional. "Este tipo de estudio tiene como finalidad conocer la relación o grado de asociación que exista entre dos o más conceptos, categorías o variables en un contexto en particular" (Sampieri, 2010)**.**

El nivel de conocimiento esperado es el correlacional, ya que a través de esta investigación estaré analizando las variables, como primera variable estaré analizando a las personas como víctimas del uso no autorizado de sus datos en el internet, así mismo al o los que de manera deliberada utilizan sin ningún consentimiento los datos privados de los habitantes de esta ciudad, también las causales y motivos que provocan.

Población. Muestra, muestreo

Población. "Conjunto de todos los casos que concuerdan con determinadas especiaciones. Delimitar la población que va a ser estudiada y sobre la cual se pretende generalizar los resultados" (Sampieri, 2010).

La población está compuesta por las familias que habitan en la ciudad de Encarnación.

Muestra. "Es un subconjunto de elementos que pertenecen a ese conjunto definido en sus características al que llamamos población" (Sampieri, 2010).

La muestra está constituida por el barrio zona alta de la ciudad de Encarnación.

Muestreo. “Busca encontrar una muestra que sea representativa del universo o población con cierta posibilidad de error (se pretende minimizar) y nivel de confianza (maximizar), así como probabilidad” (Sampieri, 2010).

El muestreo esta compuesto, por 150 familias que habitan en el barrio Zona Alta de la ciudad de Encarnación.

La población o universo delimitado serán relacionados a aquellos casos que surgen en la ciudad de Encarnación específicamente en el barrio Zona Alta. Personas que guarden relación con el uso indiscriminado de los datos de carácter privado.

Técnica e instrumento de recolección de datos

Análisis de documentos. “Son aquellas que sirven al investigador para conocer los antecedentes de un ambiente, las experiencias, vivencias o situaciones y su funcionamiento cotidiano. Veamos el uso de los principales documentos, registros, materiales y artefactos como datos cualitativos” (Sampieri, 2010).

El análisis de documentos, será la fuente de información, estas podrían facilitarme informaciones sumamente importantes, ayudaría a entender el tema principal de nuestra investigación en cuanto al uso inadecuado de información de carácter privado en la ciudad de Encarnación, e incluso acceder a los expedientes Judiciales y analizar sus historias, la manera en la que se llevaron a cabo los procesos en diferentes instancias judiciales.

Descripción del procedimiento de análisis de datos

Se considero que es necesario conocer la percepción de diversos aspectos desde un punto de vista de la muestra seleccionada.

“Una vez que los datos se han codificado, transferido a una matriz, guardado en un archivo y limpiado de errores, el investigador procede a analizarlos” (Sampieri, 2010).

Luego de haberse completado la recolección de datos empíricos conseguido mediante el trabajo de campo, se ha procedido a la correspondiente sistematización a partir de la cual se realizó la producción de datos en forma de tablas. Téngase presente que la investigación ya dispuso de los materiales en forma de tabulados impresos y digitales.

La presentación de las informaciones dentro de la investigación y elaboración del Marco Analítico de la tesis, se llevó a cabo mediante tablas de frecuencias y esquemas, posteriormente se realizó la descripción de los referidos datos, a la luz de enfoque correspondiente, finalmente fueron interpretados las informaciones previamente sistematizadas en función de los objetivos formulados, y las preguntas planteadas.

Tal como quedó especificado en los párrafos que anteceden, en la presente investigación se recurrió en cuanto al tratamiento de los datos al enfoque cuantitativo, por tanto, se recurrió a las tablas de frecuencias (absolutas y relativas porcentuales) y gráficos de distribución porcentual de los datos tabulados a partir de información producidos por el propio tesista.

Marco Analítico

Presentación y análisis de los Resultados

Se presenta a continuación los resultados de la aplicación del formulario de encuesta a 150 familias que habitan en la ciudad de Encarnación, específicamente en el barrio Zona Alta, acerca de la protección y sanciones concernientes a la utilización de datos de carácter privado.

De la población mencionada se procedió a trabajar con la muestra que ha sido por cueteo y aleatorio, lo cual se ha seleccionado de la ciudad de Encarnación un barrio al azar, el cual aleatoriamente ha sido la Zona alta.

En los datos expuestos en la tabla número uno, se encontró que la encuesta fue aplicada a familias, que fijan residencia en el barrio Zona Alta, distrito de Encarnación de los cuales respondieron de la siguiente manera.

Una fuente de datos importantes es la que se puede obtener a través de una muestra representativa, la encuesta sirve para crear fundamentos que soportan y ayuden a la investigación para la sustentación. Para confirmar lo que se ha dicho, se realizó un estudio de campo en la ciudad de Encarnación específicamente en el barrio Zona Alta.

Los resultados cuidadosamente analizados a través de tablas de frecuencia, para poder obtener la información certera de los resultados para luego plasmarlos en un gráfico.

Mediante estos gráficos los resultados pueden ser interpretadas las tablas numéricas, es decir se puede observar solo el resultado final de las pregu7ntas realizadas en la técnica aplicada para obtener más información sobre la investigación que es concerniente a protección y sanciones en la utilización de datos de carácter privado en la web en la ciudad de Encarnación.

Encuesta a Familias del Barrio Zona Alta.

A la interrogante planteada en la primera pregunta del cuestionario de encuesta aplicada Usted ¿Conoce que son los datos de carácter privado?, lo cual arrojo los siguientes resultados:

Se encontró que, el 100% de las Familias encuestadas respondieron Conocer que son los datos de carácter privado.

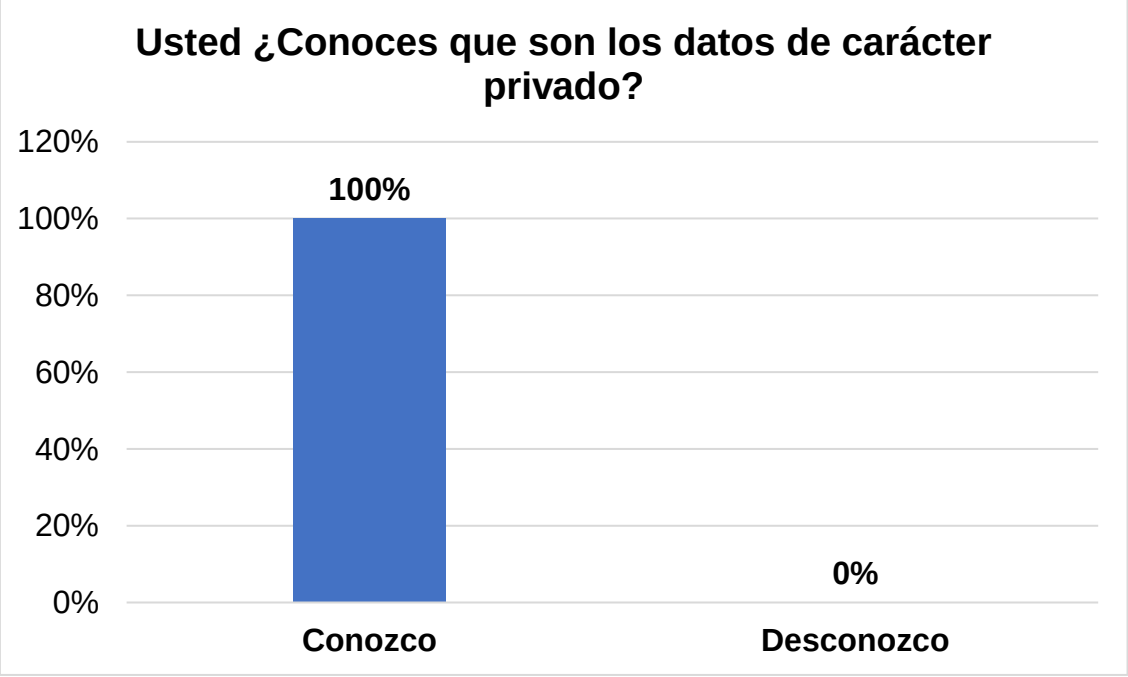
Tabla 1 *¿Conoces que son los datos de carácter privado?*

Muestra	Frecuencia	Frecuencia relativa	%
Conozco	150	1	100%
Desconozco	0	0	0%
Sumatoria	**150**	**1**	**100%**

Fuente: Elaboración propia del tesista en base a los datos generados mediante la realización del trabajo de campo.

Se detalla en la siguiente ilustración los porcentajes resultantes de la primera pregunta del cuestionario aplicado a las familias del barrio Zona Alta.

Ilustración 1 *¿Conoces que son los datos de carácter privado?*



Fuente: Elaboración propia del tesista en base a los datos generados mediante la realización del trabajo de campo.

En base a la observación de los datos expuestos en la Tabla número dos, se ha encontrado que la encuesta aplicada a las familias, que fijan residencia en el barrio Zona Alta, de lo cual respondieron a la siguiente interrogante: Usted ¿Utiliza para almacenar dados personales, la web?, la cual arrojó los siguientes resultados:

Familias que utilizan la web para almacenar datos personales alcanzan un 75% de los encuestados.

Y familias que utilizan poco la web para almacenar datos son de un 25%.

Concluyendo así, que se utiliza con mayor frecuencia la web para almacenar datos de carácter privado.

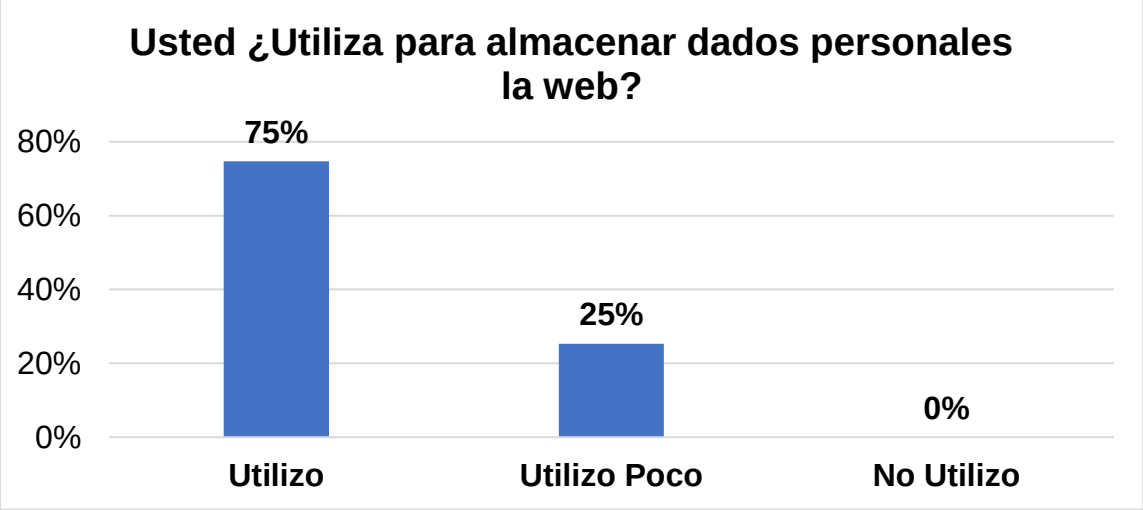
Tabla 2 *¿Utiliza para almacenar dados personales, la web?*

Muestra	Frecuencia	Frecuencia relativa	%
Utilizo	112	0,7	75%
Utilizo Poco	38	0,3	25%
No Utilizo	0	0	0%
Sumatoria	150	1	100%

Fuente: Elaboración propia del tesista en base a los datos generados mediante la realización del trabajo de campo.

Se detalla en la siguiente ilustración los porcentajes resultantes de la segunda pregunta del cuestionario aplicado a las familias del barrio Zona Alta.

Ilustración 2 *¿Utiliza para almacenar dados personales la web?*



Fuente: Elaboración propia del tesista en base a los datos generados mediante la realización del trabajo de campo.

En la Tabla número tres, se ha encontrado que la encuesta aplicada a las familias, que fijan residencia en el barrio Zona Alta, de lo cual respondieron a la siguiente interrogante: Usted ¿Qué tipo de herramienta o aplicación utiliza para almacenar sus datos personales?, la cual arrojó los siguientes resultados:

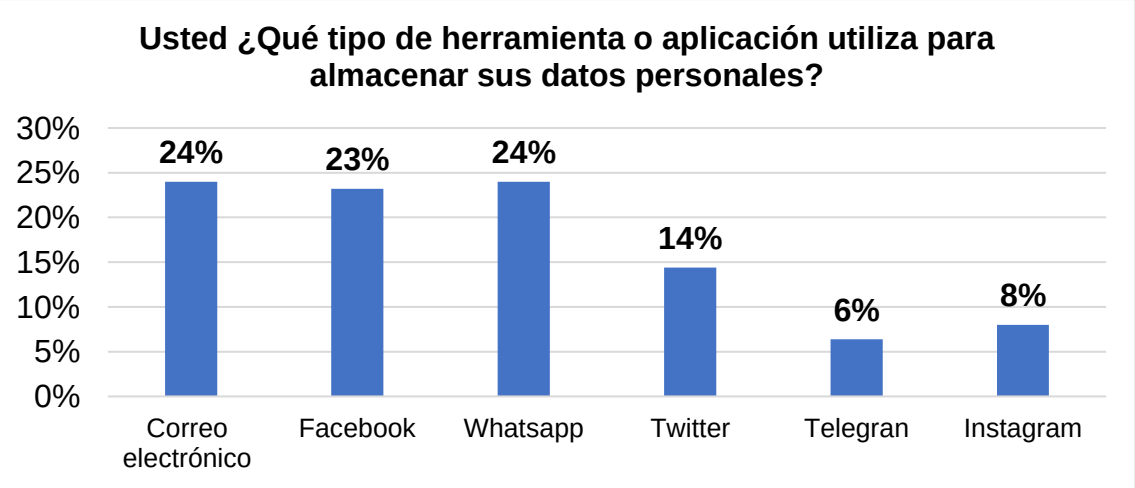
Familias que utilizan correo electrónico como herramienta para almacenar datos personales alcanzan un 24% de los encuestados. Y las que respondieron Facebook, son un 23%; las que respondieron WhatsApp, un 24%; Twitter en un 14%; Telegram en un 5% y los que respondieron Instagram en un 8%. Concluyendo así, que se utiliza con mayor frecuencia las herramientas para almacenar datos de carácter privado el Correo electrónico y el WhatsApp en un 24%.

Tabla 3 *¿Qué tipo de herramienta o aplicación utiliza para almacenar sus datos personales?*

Muestra	Frecuencia	Frecuencia relativa	%
Correo electrónico	150	0,2	24%
Facebook	145	0,2	23%
WhatsApp	150	0,2	24%
Twitter	90	0,1	14%
Telegram	40	0,1	6%
Instagram	50	0,1	8%
Sumatoria	**625**	**1**	**100%**

Fuente: Elaboración propia del tesista en base a los datos generados mediante la realización del trabajo de campo.

Ilustración 3 *¿Qué tipo de herramienta o aplicación utiliza para almacenar sus datos personales?*



Fuente: Elaboración propia del tesista en base a los datos generados mediante la realización del trabajo de campo.

En base a la observación de los datos expuestos en la Tabla número cuatro, se ha encontrado que la encuesta aplicada a las familias, que fijan residencia en el barrio Zona Alta, de lo cual respondieron a la siguiente interrogante: Usted ¿Conoce las normas que regulan la protección del uso de los datos personales en nuestro país?, la cual arrojó los siguientes resultados:

Familias que conocen las normas que regulan la protección del uso de los datos personales alcanzan un 47% de los encuestados. Y familias que desconocen las normas que regulan la protección del uso de los datos en nuestro país son de un 53%. Concluyendo así, que las familias desconocen de la existencia de las normas que regulan la protección del uso de los datos en nuestro país en un 53%, por no creer que el uso indebido de datos es un delito.

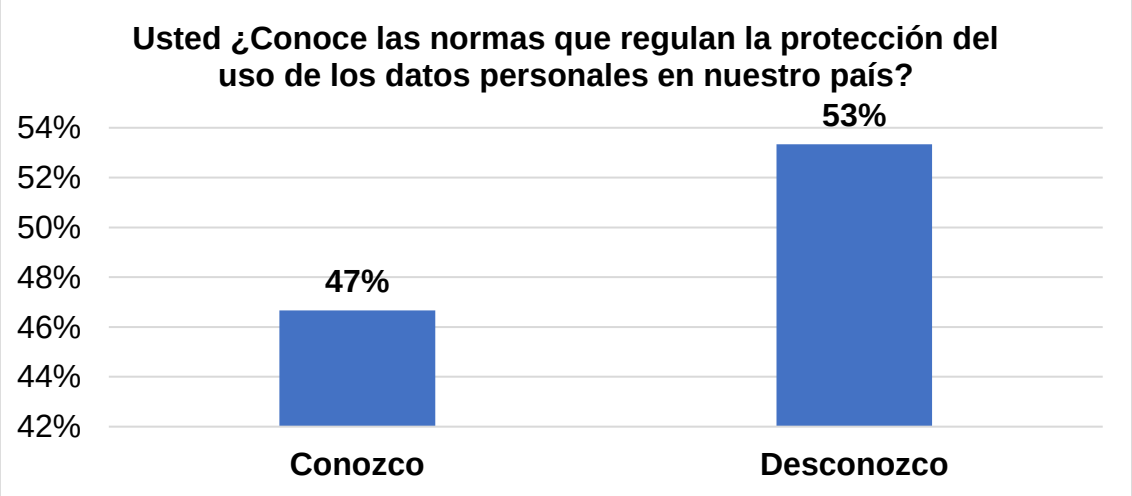
Tabla 4 *¿Conoce las normas que regulan la protección del uso de los datos personales en nuestro país?*

Muestra	Frecuencia	Frecuencia relativa	%
Conozco	70	0,47	47%
Desconozco	85	0,53	53%
Sumatoria	150	1	100%

Fuente: Elaboración propia del tesista en base a los datos generados mediante la realización del trabajo de campo.

Se detalla en la siguiente ilustración los porcentajes resultantes de la cuarta pregunta del cuestionario aplicado a las familias del barrio Zona Alta.

Ilustración 4 *¿Conoce las normas que regulan la protección del uso de los datos personales en nuestro país?*



Fuente: Elaboración propia del tesista en base a los datos generados mediante la realización del trabajo de campo.

En base a la observación de los datos expuestos en la Tabla número cinco, se ha encontrado que la encuesta aplicada a las familias, que fijan residencia en el barrio Zona Alta, de lo cual respondieron a la siguiente interrogante: Usted ¿Conoce las consecuencias jurídicas que conllevan la utilización de datos privados que se encuentran en la web?, la cual arrojó los siguientes resultados:

Familias que conocen las consecuencias jurídicas conllevan la utilización de datos de carácter privado alcanzan un 43% de los encuestados. Y familias que desconocen las consecuencias jurídicas son de un 57%. Concluyendo así, que las familias desconocen las consecuencias jurídicas que conllevan la utilización de datos de carácter privado en un 57%, solo que estas no lo usan por no creer que el uso indebido de datos es un delito.

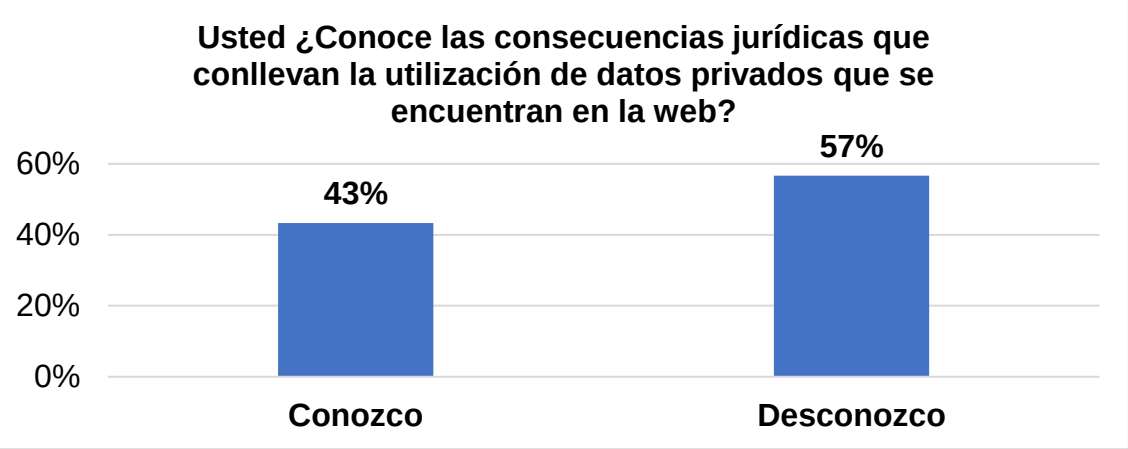
Tabla 5 *¿Conoce las consecuencias jurídicas que conllevan la utilización de datos privados que se encuentran en la web?*

Muestra	Frecuencia	Frecuencia relativa	%
Conozco	65	0,43	43%
Desconozco	85	0,57	57%
Sumatoria	**150**	**1**	**100%**

Fuente: Elaboración propia del tesista en base a los datos generados mediante la realización del trabajo de campo.

Se detalla en la siguiente ilustración los porcentajes resultantes de la quinta pregunta del cuestionario aplicado a las familias del barrio Zona Alta.

Ilustración 5 *¿Conoce las consecuencias jurídicas que conllevan la utilización de datos privados que se encuentran en la web?*



Fuente: Elaboración propia del tesista en base a los datos generados mediante la realización del trabajo de campo.

En base a la observación de los datos expuestos en la Tabla número seis, se ha encontrado que la encuesta aplicada a las familias, que fijan residencia en el barrio Zona Alta, de lo cual respondieron a la siguiente interrogante: Usted ¿Conoce a que institución debe recurrir en caso de uso indebido de sus datos privados en la ciudad de Encarnación?, la cual arrojó los siguientes resultados:

Familias que conocen las instituciones donde deben recurrir en caso de uso indebido de sus datos en la ciudad de Encarnación alcanzan un 49% de los encuestados. Y familias que desconocen las instituciones donde recurrir son de un 51%. Concluyendo así, que las familias desconocen donde acudir en caso de uso indebido de sus datos de carácter privado en un 51%, sería importante dar informaciones sobre los lugares que deben acudir las personas víctimas de uso indebido de sus datos personales.

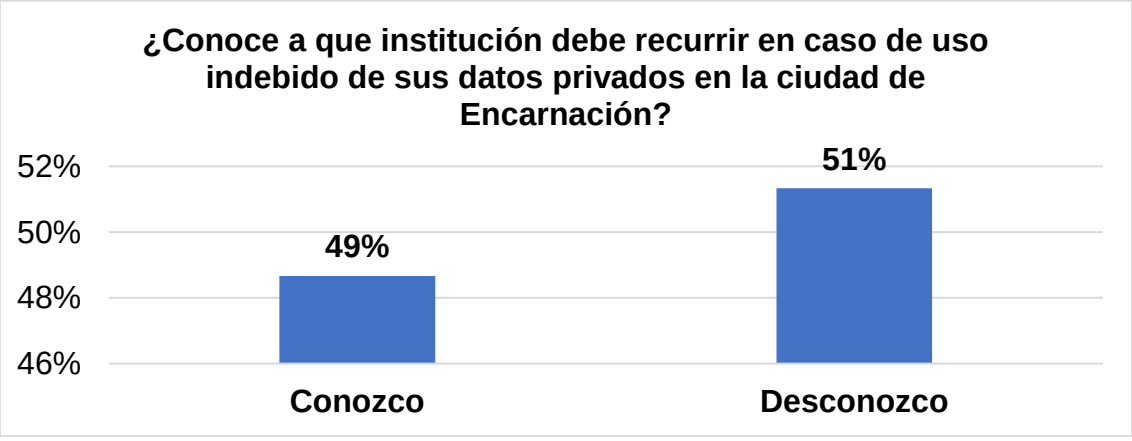
Tabla 6 *¿Conoce a que institución debe recurrir en caso de uso indebido de sus datos privados en la ciudad de Encarnación?*

Muestra	Frecuencia	Frecuencia relativa	%
Conozco	73	0,49	49%
Desconozco	77	0,51	51%
Sumatoria	150	1	100%

Fuente: Elaboración propia del tesista en base a los datos generados mediante la realización del trabajo de campo.

Se detalla en la siguiente ilustración los porcentajes resultantes de la sexta pregunta del cuestionario aplicado a las familias del barrio Zona Alta.

Ilustración 6 *¿Conoce a que institución debe recurrir en caso de uso indebido de sus datos privados en la ciudad de Encarnación?*



Fuente: Elaboración propia del tesista en base a los datos generados mediante la realización del trabajo de campo.

En base a la observación de los datos expuestos en la Tabla número siete, se ha encontrado que la encuesta aplicada a las familias, que fijan residencia en el barrio Zona Alta, de lo cual respondieron a la siguiente interrogante: Usted ¿Conoce si existen legislaciones que sancionen la utilización indebida de datos almacenados en la web?, la cual arrojó los siguientes resultados:

Familias que conocen las legislaciones que sancionan el uso indebido de sus datos almacenados en la web, alcanzan un 27% de los encuestados. Y familias que desconocen las legislaciones que sancionan, son de un 73%. Concluyendo así, que las familias desconocen las legislaciones y sanciones cuando se usa indebidamente sus datos de carácter privado en un 73%, sería importante dar informaciones sobre las legislaciones y sanciones en el caso que se utilice indebidamente sus datos de carácter privado.

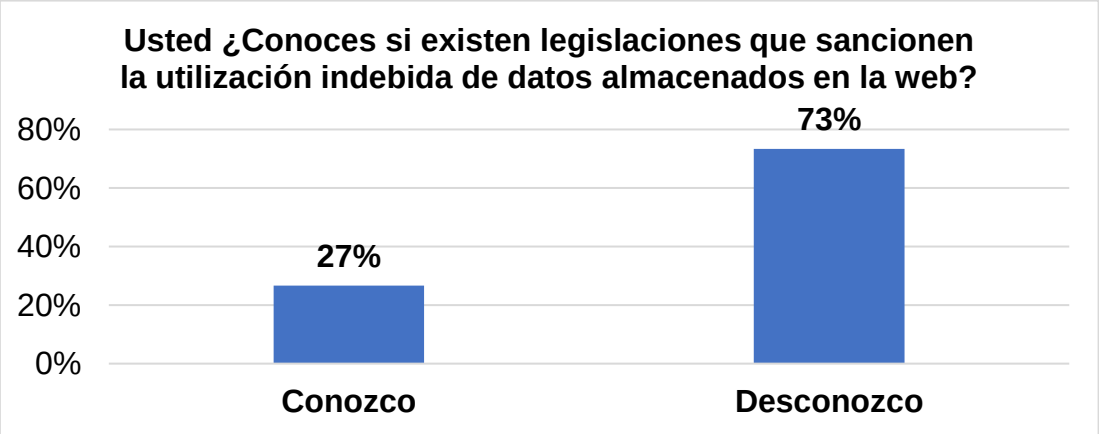
Tabla 7 *¿Conoce si existen legislaciones que sancionen la utilización indebida de datos almacenados en la web?*

Muestra	Frecuencia	Frecuencia relativa	%
Conozco	40	0,27	27%
Desconozco	110	0,73	73%
Sumatoria	150	1	100%

Fuente: Elaboración propia del tesista en base a los datos generados mediante la realización del trabajo de campo.

Se detalla en la siguiente ilustración los porcentajes resultantes de la séptima pregunta del cuestionario aplicado a las familias del barrio Zona Alta.

Ilustración 7 *¿Conoces si existen legislaciones que sancionen la utilización indebida de datos almacenados en la web?*



Fuente: Elaboración propia del tesista en base a los datos generados mediante la realización del trabajo de campo.

Comentarios y recomendaciones

En el siguiente apartado se procede a la presentación de las redacciones de los cometarios en base a los resultados obtenidos de la investigación realizada en base a las bibliografías consultadas y la encuesta elaborado en base a los resultados en obtenidos en el estudio de campo, previamente se ha realizado la evaluación e interpretación de dicho estudio empírico, poniendo énfasis en la pregunta central la cual se estableció lo siguiente ¿A qué consecuencias jurídicas puede conllevar, la utilización de los datos privados vía web de las personas en la ciudad de Encarnación?, consiguientemente con esta pregunta centralizada se puede responder el objetivo general de la investigación que se estableció de la siguiente manera: Analizar las sanciones a ser impuestas a aquellas personas que infringen en el uso no autorizado de los datos de carácter privado en la ciudad de Encarnación.

Para responder esta pregunta debemos analizar la actualidad, las tendencias de la utilización de la web para entretenimiento o realizar transacciones o compras es la nueva modalidad utilizada, por ellos también se platean nuevas formas delictivas se han centrado en la usurpación de datos personales a la hora de realizar operaciones bancarias en línea (consulta de saldos, transferencias, pagos vía Internet, etc.). se maneja mucha información en la web después de la pandemia, algunas de ellas fuimos mencionando, además de las herramientas web, como se detalla en la tercera pregunta realizada en la encuesta donde se detalla que el 24% utilizan correos electrónicos, así también en un 24% el WhatsApp y en un 23% utiliza Facebook y el porcentaje restante utiliza las demás herramientas en menor porcentaje.

Aunque la técnica habitual por parte de los phishers, que fue definido dentro del marco teórico, consiste en realizar envíos masivos de correos fraudulentos, se ha demostrado con las referencias bibliográficas consultadas que son también capaces de establecer, previamente a quien van a estafar,

ello y de forma selectiva, con qué banco opera un cliente y una vez obtenida esa información, crear el señuelo a la víctima, la cual siempre es engañada.

La unidad Especializada de Delitos Informáticos, son los responsables de detectar a estos infractores. Esta Unidad Especializada que está en la ciudad de Encarnación, fue creada para combatir los hechos punibles en la web, cometidos a través del uso de la tecnología que a su vez requieran un tratamiento especializado, desde la investigación, recolección, manejo de evidencia y prueba digital.

En este contexto, se expresan los objetivos específicos, formulados en el marco introductorio del trabajo de investigación, considerando que respondidos en su totalidad quedando evidenciados al completar la encuesta realizando un análisis punto por uno a través de la tabulación de los datos respondiendo a los siguientes:

Primer objetivo; Individualizar las normas o leyes que protegen este tipo de acto ilícito que es el uso no autorizado de datos de carácter personal en la ciudad de Encarnación; las normas y las leyes fueron individualizados en el marco legal de la investigación donde se menciona la constitución nacional, leyes de protección de datos tales como: Ley Nº 5.830; Resolución 1350/2002; Ley Nº 642/95 de Telecomunicaciones; Código Penal – Ley Nº 1160/97; Ley 1682/2001 Información de carácter Privado, además del Código de Organización judicial.

Asimismo, en la encuesta se realizó la siguiente pregunta, si conocen las normas que regulan la protección del uso de los datos personales en nuestro país lo cual arrojo que 53% desconoce, que existen las normas que regulan la protección, por ello no saben que utilizar datos de carácter privado extraído de la web son protegidos y al mismo tiempo sancionados al darle un uso incorrecto.

Segundo objetivo; Identificar instituciones donde se pueda acudir en caso de sufrir atentado en contra del uso de datos no autorizado de carácter privado en la ciudad de Encarnación; como se mencionó en párrafo anteriores

las institución o órgano encargado donde se puede acudir es a La unidad Especializada de Delitos Informáticos.

Así mismo se consultó a la población encuestada, si conocen donde deben recurrir en caso de uso indebido de sus datos en la ciudad de Encarnación, estos un 51% desconocen, donde acudir en caso de ser víctima de este tipo de delitos, por ello sería importante impartir informaciones sobre este tema para ayudar a las víctimas, que desconocen que el uso indebido de sus datos son un delito y están dentro de la Constitución Nacional en su artículo 33.

Tercer objetivo; Averiguar los órganos encargados de sancionar a aquellas personas que hacen uso de información de carácter personal en la ciudad de Encarnación; como se mencionó más arriba se mencionaron cuáles son los órganos encargados en este caso la policía nacional, la unidad especializada de delitos informáticos.

Por otra parte en la encuesta realizada a la población seleccionada, se les pregunto en la encuesta si conocen si existe legislaciones que sancionen la utilización indebida de datos almacenados en la web, la cual arrojo el siguiente porcentaje, en un 73% desconocen de la existencia de legislaciones que sancionan la utilización de los datos de carácter privado, como se mencionó con anterioridad que sería de suma importancia dar estos tipos de informaciones, que ayude a mermar los actos delictivos cometidos en la web con datos personales.

Concluyendo con la investigación, con todo lo expuesto se da un margen de porcentaje en el análisis de las tabulaciones, encuadrando como acto delictivo el mal uso del internet, que las personas utilizan la web con datos privados, pero sin saber que pueden ser víctimas de algún tipo de delito, y si ellos son las víctimas de estos inescrupulosas, no saben dónde acudir para reclamar justicia. Con esta investigación se quiere contribuir a las aportaciones que consideramos de máxima actualidad, sobre las implicaciones de las nuevas tecnologías de la información y la comunicación y el respeto de los derechos fundamentales como son el honor y la intimidad personal.

Recomendaciones

En este apartado se realiza las recomendaciones referentes al tema de investigación, para futuras investigaciones:

- Se recomienda a las Universidades, indagar las formas de promover charlas acerca del uso de datos de carácter privado en la web, y su forma de utilización para una mejor convivencia social.

- Se recomienda al Ministerio de Educación y Ciencias el estudio de la prevención y sanciones sobre el uso indebido de datos de carácter privado como valor fundamental para la convivencia humana, así para evitar los actos delictivos por el medio informático.

- Se recomienda al Poder Judicial del Paraguay, indagar respecto a la forma de promover informaciones sobre la protección y sanciones del uso indebido de datos de carácter personal.

- Se recomienda al Gobierno Local (Municipalidad y Gobernación), la realización de trabajos de propagandas y afiches alusivos a la investigación con la finalidad de informar a la ciudadanía sobre la protección y las posibles sanciones al utilizar los datos de carácter privado en la web, en la ciudad de Encarnación.

Bibliografía

Acuña Llamas, F. J. (2015). *La protección integra de los datos de carácter personal en México: La inaplazable elección legislativa, enre el modelo norteamericano y el modelo de la Europa unificada.* Mñexico: Alianza Editorial.

Acuña, J., Fulchi, L. A., & Sequera, M. (2017). *La protección de datos personales en bses de datos públicos en Paraguay.* Asunción-Paraguay: La Ley.

Baron, A. (2021). *Guía de elaboración de trabajos de culminación de carreras de grado y programas de posgrado.* Fernando de la Mora - Paraguay: Universidad Tecnológica Intercontinental.

Bravo Resendiz, R. (2021). *¿Por qué es importante proteger los Datos Personales?* Veracruz: Universidad Veracruzana.

Castillo Jimenez, C. (2012). *Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información .* Sevilla: Facultad de Derecho. Universidad de Huelva.

Código Penal. (2004). Código Penal de la República del Paraguay y Leyes complementarias actualizadas. En I. Editora, *Ley 160/97* (pág. 164). Asunción. Paraguay: Intercontinental Editora.

Constitución Nacional. (2005). Derecho a la Vida. En *Constitución Nacional de la República del Paraguay.* Asunción. Paraguay: Intercontinental Editora.

Freund, J. (1995). *Lessence du politique.* París, Francia: Sirey.

Galan Muñoz, A. (2015). *El fraude y la estafa mediante sistemas informáticos .* Valencia : Universidad Pablo de Olavide.

González Gaitano, N. (2010). *El deber de respeto a la intimidad.* Pamplona: Eunsa.

Itapúa en Noticias. (2020). *La información Online.* Encarnación. Recuperado el 01 de Septiembre de 2022, de https://itapuanoticias.tv/denuncian-sistema-delictivo-que-roba-cuentas-de-whatsapp/

LEY N° 1.682. (2012). *QUE REGLAMENTA LA INFORMACIÓN DE CARÁCTER PRIVADO. Se reglamenta la información de carácter privado (INFORMCONF).* Asunción-Paraguay. Obtenido de https://www.bacn.gov.py/leyes-paraguayas/1760/ley-n-1682-reglamenta-la-informacion-de-caracter-privado

LEY N° 5.830. (2012). *QUE PROHÍBE LA PUBLICIDAD NO AUTORIZADA POR LOS USUARIOS TITULARES DE TELEFONÍA MÓVIL.* Asunción-Paraguay: Biblioteca y Archivo del Congreso de la Nación.

LEY Nº 1969 . (2010). *QUE MODIFICA, AMPLÍA Y DEROGA VARIOS ARTICULOS DE LA LEY N° 1682/2001 "QUE REGLAMENTA LA INFORMACIÓN DE CARÁCTER PRIVADO" .* Asunción: Proyecto de Ley.

Ley Nº 642/95. (2015). *Ley de Telecomunicaciones: Régimen de protección a abonados y usuarios.* Asunción-Paraguay: Intercontinental. Obtenido de https://www.bacn.gov.py/leyes-paraguayas/2452/ley-n-642-telecomunicaciones

MarberthKubicki, A. (2010). *Computer und Internetstrafrecht.* München, Beck, segunda edición.

Martínez de Pisón, J. (2016). *El derecho a la intimidad: de la configuración inicial a los últimos desarrollosen la jurisprudencia constitucional.* Buenos Aires: Universidad de la Rioja.

Mata, M. R. (2017). *Delitos cometidos mediante sistemas informáticos (estafas, difusión de materiales pornográficos, ciberterrorismo).* Bilbao, Universidad de Deusto.

Mayer Lux, L. (2017). *El bien jurídico protegido en los delitos Informáticos.* Santiago-Chile: Revista chilena de derecho.

Mendoza Enríquez, O. A. (2018). *Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento.* México: Revista IUS.

Muñoz Conde, F. (2015). *Teoría general del delito.* Valencia: TEMIS S.A.

Pappalardo Zaldívar, C. (1992). *Reforma constitucional: proyectos y aportes, Volumen 1.* Asunción- Paraguay: Intercontinental.

Pérez, J. C. (2015). *Protección de datos y seguridad de la información. Guía práctica para ciudadanos y empresas.* Madrid, España: RA-MA, S. A.

RAE. (2021). *Real Academia Española: Conceptos de palabras utilizadas en la investigación.* Fundación la Caixa. Obtenido de https://dle.rae.es/protecci%C3%B3n%20?m=form

Resolución Nº 1350. (2002). *RESOLUCIÓN Nº 1350/2002.- POR LA CUAL SE ESTABLECE LA OBLIGATORIEDAD DE REGISTRO DE DETALLES DE LLAMADAS POR EL PLAZO DE SEIS (6) MESES.* Asunción-Paraguay: Gaceta Oficial. Obtenido de https://www.conatel.gov.py/conatel/wp-content/uploads/2019/10/go-021122-226bis-rd1350.pdf

Sampieri, R. H. (2010). *Metodología de la Investigación.* México D.F.: Mc Graw Hill.

Sánchez Bernal, J. (2009). *el bien jurídico protegido en el delito de estafa informática.* Universidad de Salamanca: Universidad de Salamanca y Becario de Colaboración en el departamento de Derecho Público General, por el Ministerio de Educación, Política Social y Deporte.

Apéndice

En el siguiente apartado, se detalla la lista de los apéndices del trabajo de investigación.

- Apéndice A: Encuesta: A Familias del Barrio Zona Alta de la Ciudad de Encarnación
- Apéndice B: Denuncian Sistemas Delictivos que roba cuentas de WhatsApp
- Apéndice C: LEY N° 6534. DE PROTECCIÓN DE DATOS PERSONALES CREDITICIOS

Apéndice A

Encuesta: A Familias del Barrio Zona Alta de la Ciudad de Encarnación.

Soy José Manuel Morínigo Pérez: estudiante de la Carrera de Derecho de la UTIC Sede Encarnación estoy trabajando en una investigación que se exige como requisito para la obtención de título de Abogado en la Universidad Tecnológica Intercontinental UTIC sobre: “Protección y sanciones concernientes a la utilización de datos de carácter privado en la Ciudad de Encarnación”. Le pido su valiosa colaboración para llevar adelante este trabajo, rellenando algunas preguntas, tú opinión es la que cuenta, (la encuesta es anónima). **Marca con una X**

Preguntas

1. Usted ¿Conoces que son los datos de carácter privado?

☐ Conozco

☐ Desconozco

2. Usted ¿Utiliza para almacenar dados personales, la web?

☐ Utilizo

☐ Utilizo Poco

☐ No utilizo

3. Usted ¿Qué tipo de herramienta o aplicación utiliza para almacenar sus datos personales?

☐ Correo electrónico

☐ Facebook

☐ Whatsapp

☐ Twitter

☐ Telegran

☐ Instagram

4. Usted ¿Conoce las normas que regulan la protección del uso de los datos personales en nuestro país?

☐ Conozco

☐ Desconozco

5. Usted ¿Conoce las consecuencias jurídicas que conllevan la utilización de datos privados que se encuentran en la web?

☐ Conozco
☐ Desconozco

6. Usted ¿Conoce a que institución debe recurrir en caso de uso indebido de sus datos privados en la ciudad de Encarnación?

☐ Conozco
☐ Desconozco

7. Usted ¿Conoces si existen legislaciones que sancionen la utilización indebida de datos almacenados en la web?

☐ Conozco
☐ Desconozco

Apéndice B

Denuncian Sistemas Delictivos que roba cuentas de WhatsApp.

Desde la Dirección de Delitos Económicos y Financieros de la Policía Nacional en Encarnación, denunciaron que últimamente vienen registrando varios casos de usuarios que han sido víctimas del robo de sus cuentas de WhatsApp, esto luego de abrir enlaces maliciosos que llegan al teléfono que finalmente resultan ser una trampa de los ciberdelincuentes

Para elegir a sus potenciales víctimas, los delincuentes utilizan la llamada ingeniería social (la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos) y posteriormente envían links haciéndose pasar por representantes de operadoras, solicitando datos personales, instando a un posible cambio de contraseña entre otras excusas. Acto seguido, contactan a través de WhatsApp para pedir códigos para completar el proceso.

Según el Oficial Inspector David Fariña, la manera más efectiva de evitar ser engañados es evitando dar cualquier tipo de información personal por teléfono y vinculando las cuentas a un correo de seguridad que al final dará mayor seguridad. El nuevo modus operandi, el robo de perfiles de WhatsApp para realizar estafas registra casos en varios países y en Paraguay se reportó una ola de denuncias a finales del año pasado.

Según investigaciones del Departamento de Delitos Informáticos, los delincuentes instalan el WhatsApp en un dispositivo e introducen el número de teléfono de su víctima. Para validar la aplicación, el delincuente sólo requiere que el dueño de la línea le reenvíe un código de verificación o que ingrese al link que le llega mediante un SMS y es en ese momento cuando la potencial víctima debe estar atento y no caer en el engaño.

Actualmente ya se realizaron denuncias sobre este caso en la ciudad de Encarnación [19].

[19] Fuente extraída de ITAPUÁ EN NOTICIAS- disponible en: https://itapuanoticias.tv/denuncian-sistema-delictivo-que-roba-cuentas-de-whatsapp/

Apéndice C.

LEY N° 6534[20].

DE PROTECCIÓN DE DATOS PERSONALES CREDITICIOS

CAPÍTULO I

DISPOSICIONES GENERALES.

Artículo 1°- OBJETO. La presente Ley tiene por objeto garantizar la protección de datos crediticios de toda persona, cualquiera sea su nacionalidad, residencia o domicilio.
También se busca regular la actividad de recolección y el acceso a datos de información crediticia, así como la constitución, organización, funcionamiento, derechos, obligaciones y extinción de las personas jurídicas que se dediquen a la obtención y provisión de información crediticia, con el fin de preservar los derechos fundamentales, la intimidad, la autodeterminación informativa, la libertad, la seguridad y el trato justo de las personas, de conformidad con lo establecido en la Constitución Nacional, la presente Ley y los Tratados suscritos y ratificados por la República del Paraguay.

Artículo 2°- ÁMBITO DE APLICACIÓN. Esta Ley es de aplicación obligatoria al tratamiento de datos personales en registros públicos o privados recopilados o almacenados en el territorio nacional en sistemas de información, archivos, registros o bases de datos físicos, electrónicos o digitales a través de mecanismos manuales, automatizados o parcialmente automatizados de recolección de datos.

Artículo 3°- DEFINICIONES. A los efectos de la presente Ley, se entiende por:

Datos Personales: Información de cualquier tipo, referida a personas jurídicas o personas físicas determinadas o determinables. Se entenderá por determinable la persona que pueda ser identificada mediante algún identificador o por uno o varios elementos característicos de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

[20] La presente ley estable las definiciones de los conceptos necesarios para la realización de la investigación y tener un panorama más amplio sobre la utilización de los datos de carácter privado en la ciudad de encarnación.

Los derechos y garantías de protección de datos personales serán extendidos a personas jurídicas en cuanto le sean aplicables.

Datos personales sensibles: Aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. Se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.

Titular de Datos: Persona física o jurídica, cuyos datos son objeto de tratamiento.

Base de datos: Cualquier plataforma, archivo, registro o banco de información que contenga de manera manual o electrónica, o de cualquier otra índole que pudiera surgir, información referida a las personas.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados realizadas sobre datos personales, relacionadas de manera enunciativa más no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, cesión, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales.

Responsable del Tratamiento: La persona física o jurídica, autoridad pública u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento de los datos.

Encargado del Tratamiento: La persona física o jurídica, autoridad pública, u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Información crediticia: Es aquella información, positiva y negativa, relacionada con el historial crediticio de personas físicas y jurídicas, acerca de actividades crediticias, comerciales y otras de naturaleza análoga, que sirva para identificar correcta e inequívocamente a la persona, su domicilio, actividad

comercial, determinar su nivel de endeudamiento, de cumplimiento de sus obligaciones y, en general, de riesgos crediticios en un determinado momento.

Fuentes de información: Cualquier persona o entidad pública o privada que en el ejercicio de sus funciones o actividades, gestionen una base de datos personales o crediticios.

Fuentes de información crediticia: Son las personas públicas y privadas que, debido a sus actividades, poseen información crediticia. A los efectos de esta Ley, serán consideradas fuentes de información los Organismos y Entidades del Estado, y Entidades Administradoras de Fondos Previsionales que, por su naturaleza y funciones, posean información relevante para el análisis del riesgo crediticio.

Sociedad de información crediticia: Conocida también como Buró de Información Crediticia. Es la sociedad cuyo objeto social es la prestación de servicios de referencias crediticias sobre el titular de la información crediticia, que se adecuen a los requisitos establecidos en esta Ley.

Usuario de información crediticia: Toda persona, física o jurídica, con interés legítimo que contrata la prestación de servicios de referencias crediticias. El interés legítimo está configurado por el empleo del crédito bajo sus diversas modalidades o la intermediación para el perfeccionamiento de este tipo de operaciones, como herramienta habitual de gestión en la actividad económica desarrollada, incluidos los contratos con prestaciones diferidas que impliquen pagos periódicos de sumas de dinero por plazos determinados, así como relaciones comerciales que pudieran existir entre los usuarios y titular del derecho.

Consentimiento: Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el titular de datos acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de sus datos personales.

Artículo 4°- PROHIBICIÓN. Se prohíbe dar a publicidad o difundir datos sensibles de personas que sean explícitamente individualizadas o individualizables.

Artículo 5°- DERECHO A LA AUTODETERMINACIÓN INFORMATIVA. Se garantiza a toda persona el acceso a la información y a los datos sobre sí misma, sobre quienes se hallen bajo su patria potestad y sobre personas que acredite se hallen bajo su tutela o curatela, así como sobre sus bienes, que obren en registros oficiales o privados de carácter público o en entidades que suministren información sobre solvencia económica y situación patrimonial, así como conocer el uso que se haga de los mismos o su finalidad y a requerir su acceso, rectificación, cancelación y oposición.

Artículo 6°- DEL CONSENTIMIENTO INFORMADO. Toda persona tiene derecho a ser informada en forma expresa y clara sobre la finalidad que se dará a los datos personales requeridos sobre ella, a fin de manifestar expresamente su consentimiento para la obtención y utilización de sus datos personales, el cual deberá ser expreso e inequívoco, en condiciones que no admitan dudas de su otorgamiento y deberá constar de manera escrita, electrónica, digital u otro mecanismo fehaciente. El consentimiento podrá ser revocado de forma expresa en las mismas condiciones y a título gratuito. Este acto no generará efecto retroactivo.
El tratamiento y la cesión de datos personales son ilícitos cuando el titular de los datos no hubiere prestado su consentimiento libre, expreso y consciente. En todos los casos, el responsable del tratamiento tiene la carga de demostrar que el titular de los datos consintió el uso de sus datos personales.

Artículo 7°- CALIDAD DE LA INFORMACIÓN. Los datos personales recolectados o almacenados deberán ser lícitos, exactos, completos, veraces y actualizados para el fin específico para los que fueron recolectados.

Artículo 8°- EJERCICIOS DE LOS DERECHO DEL TITULAR DE DATOS. El titular de datos o su representante tiene derecho a acceder a los datos personales que de ella consten en registros mantenidos por personas físicas o jurídicas, públicas o privadas, así como a conocer cualquier información relacionada con las condiciones generales y específicas de su tratamiento.

Éste podrá solicitar, en cualquier momento al responsable, el acceso, actualización, rectificación, la supresión, oposición y portabilidad de los datos personales que le conciernen.

El responsable deberá establecer medios y procedimientos sencillos, expeditos, accesibles y gratuitos que permitan al titular de datos ejercer sus derechos.

En caso de personas fallecidas, el ejercicio de los derechos establecidos en la presente Ley corresponderá a sus herederos o legatarios.

Artículo 9°- DERECHO AL OLVIDO DE DATOS CREDITICIOS. La conservación de los datos personales, que puedan afectar a su titular, no deberá exceder el plazo de 5 (cinco) años, desde la fecha de ocurrencia de los hechos registrados, salvo disposición normativa especial que establezca otro plazo o porque el acuerdo de las partes haya establecido un plazo menor. En caso que sea necesaria su conservación, más allá del plazo estipulado, deberán ser desasociados los datos personales de su titular.

Artículo 10.- SEGURIDAD DE LOS DATOS. El responsable del tratamiento de los datos personales crediticios deberá garantizar la adopción e implementación de medidas técnicas, organizativas y de seguridad necesarias para salvaguardar el acceso y la integridad de los datos personales, a fin de evitar su alteración, pérdida, consulta, comercialización o acceso no autorizado.

Artículo 11.- DEBER DE SECRETO. Las personas responsables, encargadas del tratamiento de datos crediticios y quienes intervengan en cualquier fase de la recolección, procesamiento, almacenamiento, utilización o circulación de datos con fines crediticios están obligados a guardar el secreto respecto de los mismos, salvo que requiera ser revelado por autoridad competente mediando orden judicial.

El deber de secreto se mantiene aun cuando la persona responsable cese en sus funciones.

Esta obligación es extensible a las personas debidamente reconocidas como usuarios o suscriptores de una Empresa de Información Crediticia, que tengan acceso, de conformidad con lo establecido en la Ley, al historial de datos de un

titular; pues deberán guardar absoluta reserva y cuidado sobre la información obtenida.

El deber de secreto no regirá cuando la información sea requerida por:

El Banco Central del Paraguay y sus órganos de supervisión, en ejercicio de sus facultades legales.

La autoridad judicial competente, en virtud de resolución dictada en juicio en el que el afectado sea parte. En tal caso, deberán adoptarse las medidas pertinentes que garanticen la reserva.

El Contralor General de la República, en el marco de sus atribuciones, sobre la base de las siguientes condiciones:

Debe referirse a una persona física o jurídica determinada.

Debe encontrarse en curso una auditoría o verificación patrimonial con respecto a esa persona.

La misma deberá ser solicitada formalmente.

La máxima autoridad de la Subsecretaría de Estado de Tributación y de la Dirección Nacional de Aduanas, en el marco de sus atribuciones, sobre la base de las siguientes condiciones:

Debe referirse a un responsable o contribuyente determinado.

La información deberá ser solicitada formalmente.

Debe encontrarse en curso una verificación con respecto a ese responsable o contribuyente.

La fiscalía general del Estado y los agentes fiscales que conforman el Ministerio Público, en el marco de las atribuciones que le son legalmente conferidas por la legislación.

La Secretaría de Prevención de Lavado de Dinero o Bienes, en el marco de las atribuciones que le son legalmente conferidas por la legislación.