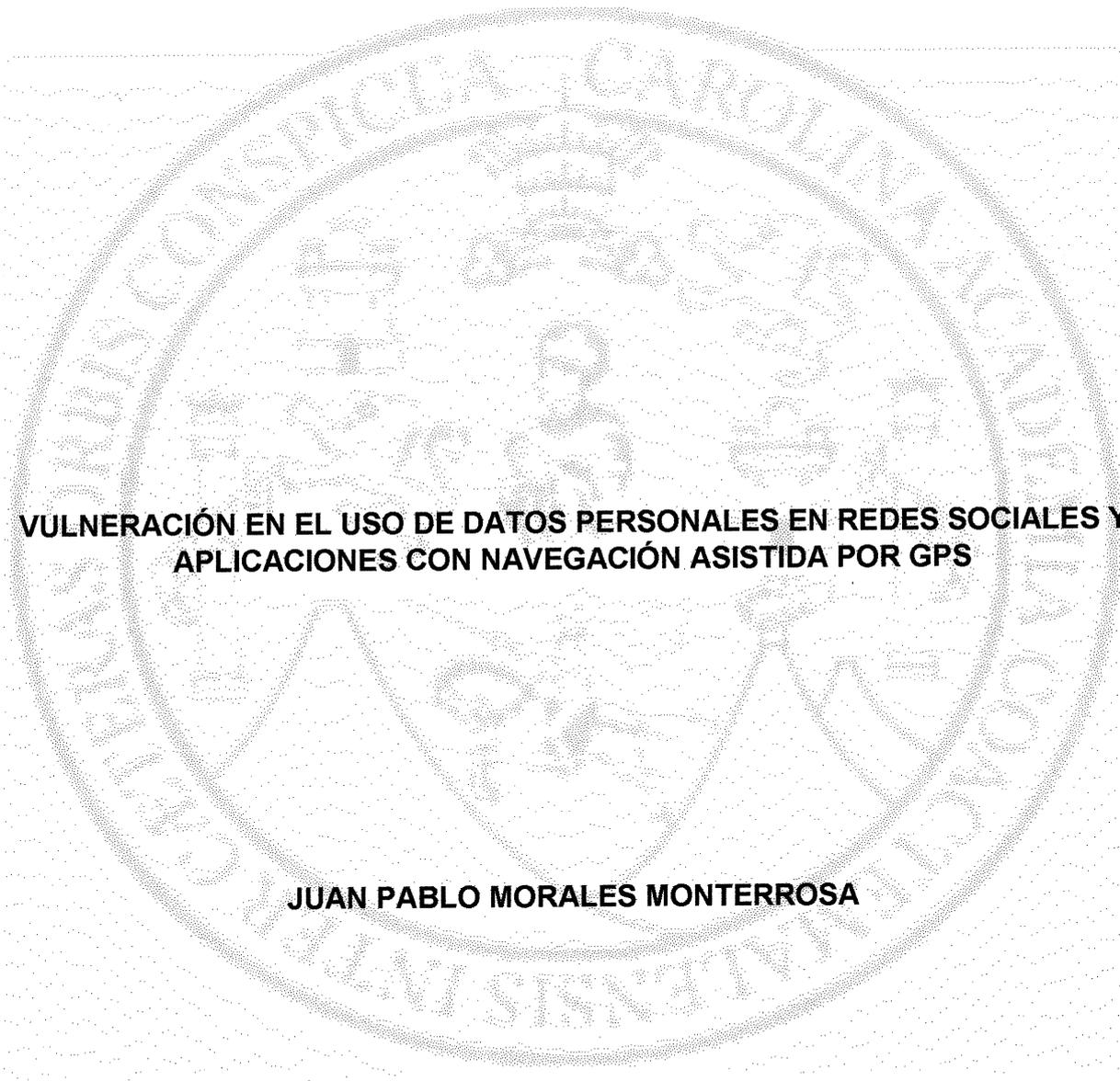


**UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES**



**VULNERACIÓN EN EL USO DE DATOS PERSONALES EN REDES SOCIALES Y
APLICACIONES CON NAVEGACIÓN ASISTIDA POR GPS**

JUAN PABLO MORALES MONTERROSA

GUATEMALA JULIO DE 2018

**UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES**

**VULNERACIÓN EN EL USO DE DATOS PERSONALES EN REDES SOCIALES Y
APLICACIONES CON NAVEGACIÓN ASISTIDA POR GPS**

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

JUAN PABLO MORALES MONTERROSA

Previo a conferírsele el grado académico de

LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

y los títulos profesionales de

ABOGADO Y NOTARIO

Guatemala, julio de 2018

**HONORABLE JUNTA DIRECTIVA
DE LA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
DE LA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA**

DECANO:	Lic.	Gustavo Bonilla
VOCAL I:	Lic.	Luis Rodolfo Polanco Gil
VOCAL II:	Lic.	Henry Manuel Arriaga Contreras
VOCAL III:	Lic.	Juan José Bolaños Mejía
VOCAL IV:	Br.	Jhonathan Josué Mayorga Urrutia
VOCAL V:	Br.	Freddy Noé Orellana Orellana
SECRETARIO:	Lic.	Fernando Antonio Chacón Urizar

**TRIBUNAL QUE PRACTICÓ
EL EXAMEN TÉCNICO PROFESIONAL**

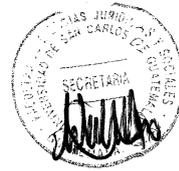
Primera Fase:

Presidenta:	Licda.	Ileana Noemí Villatoro Fernández
Vocal:	Lic.	José Miguel Cermeño Castillo
Secretario:	Lic.	William Armando Vanegas Urbina

Segunda Fase:

Presidente:	Lic.	Aníbal De León Velasco
Vocal:	Licda.	Gladis Maribel Reyes Cabrera
Secretario:	Lic.	Saúl Sigfredo Castañeda Guerra

RAZÓN: “Únicamente el autor es responsable de las doctrinas sustentadas y contenido de la tesis.” (Artículo 43 del Normativo para la Elaboración de Tesis de la Licenciatura de Ciencias Jurídicas y Sociales y del Examen General Público.)



Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala,
 07 de febrero de 2017.

Atentamente pase al (a) Profesional, EDGAR ARMINDO CASTILLO AYALA
 _____, para que proceda a asesorar el trabajo de tesis del (a) estudiante
 _____, con carné 201014101,
 intitulado PRIVACIDAD DE DATOS PERSONALES EN EL USO DE REDES SOCIALES Y APLICACIONES CON
NAVEGACIÓN ASISTIDA POR GPS.

Hago de su conocimiento que está facultado (a) para recomendar al (a) estudiante, la modificación del bosquejo preliminar de temas, las fuentes de consulta originalmente contempladas; así como, el título de tesis propuesto.

El dictamen correspondiente se debe emitir en un plazo no mayor de 90 días continuos a partir de concluida la investigación, en este debe hacer constar su opinión respecto del contenido científico y técnico de la tesis, la metodología y técnicas de investigación utilizadas, la redacción, los cuadros estadísticos si fueren necesarios, la contribución científica de la misma, la conclusión discursiva, y la bibliografía utilizada, si aprueba o desaprueba el trabajo de investigación. Expresamente declarará que no es pariente del (a) estudiante dentro de los grados de ley y otras consideraciones que estime pertinentes.

Adjunto encontrará el plan de tesis respectivo.

LIC ROBERTO FREDY ORELLANA MARTÍNEZ
 Jefe(a) de la Unidad de Asesoría de Tesis



Fecha de recepción 05 / 03 / 2017. f) _____

Asesor(a)
 (Firma y Sello)
Edgar Armindo Castillo Ayala
 Abogado y Notario



LIC. EDGAR ARMINDO CASTILLO AYALA
3ª. Avenida 13-62 Zona 1, Ciudad de Guatemala
COLEGIADO NO. 6220



Guatemala, 14 de mayo de 2018

Licenciado

Roberto Fredy Orellana Martínez

Jefe de la Unidad de Asesoría de Tesis

Facultad de Ciencias Jurídicas y Sociales

Universidad de San Carlos de Guatemala



Respetable Licenciado Roberto Orellana:

Como asesor de tesis del Bachiller **JUAN PABLO MORALES MONTERROSA**, en la elaboración del trabajo intitulado: **“PRIVACIDAD DE DATOS PERSONALES EN EL USO DE REDES SOCIALES Y APLICACIONES CON NAVEGACIÓN ASISTIDA POR GPS”**, se convino la modificación del título quedando así: **“VULNERACIÓN EN EL USO DE DATOS PERSONALES EN REDES SOCIALES Y APLICACIONES CON NAVEGACIÓN ASISTIDA POR GPS”**, me permito manifestarle que dicho trabajo contiene:

- a) En relación al contenido científico y técnico de la presente tesis, opino que cumple objetivamente con cada uno de los capítulos elaborados permitiendo un análisis concreto, que pueda establecer la necesidad de regular las nuevas conductas.
- b) En el presente trabajo de tesis se utilizó el método inductivo, deductivo y comparativo, ya que juntamente hacen evidente la carencia legislativa existente en Guatemala así como el desarrollo de un análisis sobre la vulneración de los datos personales en el uso de redes sociales así como en las aplicaciones con navegación asistida por GPS. En el presente trabajo fue utilizada la técnica bibliográfica.
- c) El presente trabajo reúne los requisitos de la actualidad no sólo en el aspecto académico doctrinario, sino en el aspecto normativo de la legislación guatemalteca vigente. En el análisis pude comprobar una redacción coherente y técnica lo que le permite un orden lógico a un trabajo de *Tesis Ad Gradum*.



LIC. EDGAR ARMINDO CASTILLO AYALA
3ª. Avenida 13-62 Zona 1, Ciudad de Guatemala
COLEGIDO 6220

d) La contribución científica permite sentar las bases de una doctrina para futuras investigaciones. Asimismo, demostrar en alguna medida la carencia legislativa que regule la protección de datos personales y privacidad de los usuarios de internet.

e) La conclusión discursiva como síntesis del contenido del trabajo de investigación es válida y firme, permite entender con sencillez la vulnerabilidad de la privacidad de datos, los riesgos que existen en el uso de redes sociales y la falta de regulación de conductas que puedan generarse.

f) La bibliografía ha sido correcta y suficiente para el presente trabajo, además es novedosa en relación al contenido y autores. Fue aplicada de forma adecuada, como fuente de doctrina, posibilitándose de esta manera la estructura de un estudio completo y adecuado de la carencia de normas jurídicas que regulen conductas derivadas del uso de redes sociales. Asimismo, manifiesto expresamente que no soy pariente del estudiante dentro de los grados de ley.

La tesis en cuestión, cumple con los requisitos legales prescritos y exigidos en el Artículo 31 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, razón por la cual emito **DICTAMEN FAVORABLE**, a efecto de que le permita continuar con el trámite correspondiente para su posterior evaluación por el Tribunal Examinador en el Exámen Público de Tesis, previo a optar el grado académico de licenciado en Ciencias Jurídicas y Sociales.

Deferentemente,

LIC. EDGAR ARMINDO CASTILLO AYALA
COLEGIADO 6220

Edgar Armindo Castillo Ayala
Abogado y Notario



DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, 16 de julio de 2018.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis del estudiante JUAN PABLO MORALES MONTERROSA, titulado VULNERACIÓN EN EL USO DE DATOS PERSONALES EN REDES SOCIALES Y APLICACIONES CON NAVEGACIÓN ASISTIDA POR GPS. Artículos 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

RFOM/cpchp.

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]



DEDICATORIA



- A DIOS:** Por la vida y permitir cumplir mis metas.
- A:** La Universidad de San Carlos de Guatemala y a la Facultad de Ciencias Jurídicas y Sociales, por darme la oportunidad de formarme como profesional del derecho, así como a cada uno de los catedráticos que han brindado sus conocimientos jurídicos.
- A MIS PADRES:** Luis Alberto y Mercedes Isolina, que durante el camino me han brindado su amor y apoyo sin condiciones y por ser personas ejemplares e intachables.
- A:** Ingrid, porque con tu ejemplo has inculcado en mí principios y valores.
- A MIS HERMANOS:** Marcelita (+), Luis Carlos, Cristhian, Marisol, Luis Alberto y Renato por ser ejemplo de lealtad, unidad, amor y proactividad en este proceso.
- A:** Claudia, por brindarme tu apoyo y ser un motor para lograr esta meta.
- A:** Ronni, por la amistad, el apoyo y el esfuerzo que hemos realizado.
- A:** Mayrita y Silvita, por brindarme su cariño y amistad.



PRESENTACIÓN

La presente investigación socio jurídica y de índole cualitativa se origina en virtud de la necesidad de la adaptación del ordenamiento jurídico vigente a la realidad social guatemalteca, su contexto se llevó a cabo en la Ciudad de Guatemala entre el transcurso del 2016 y 2017, en la que el uso masivo de las redes sociales ha incrementado vertiginosamente. Por ser un tema relativamente nuevo, la legislación vigente si bien regula algunos aspectos, denota carencia por temas de vigencia.

Es importante establecer la importancia de la actual investigación repercute en las áreas de derecho constitucional, de derecho informático y derecho penal. Teniendo por objeto el estudio la privacidad de datos personales y el sujeto los usuarios de las redes sociales, la regulación de nuevos tipos penales dentro de las redes sociales, fomentar el adecuado uso de las mismas, establecer campañas para evitar ser víctimas de ciberacoso, estafas a través de redes sociales; así como el área constitucional, debido a la vulnerabilidad de datos personales y sensibles.

La finalidad de la tesis es ser un guía para el lector, para tener conciencia sobre el alcance que puede tener el hecho de utilizar una red social, las implicaciones que surgen al momento de aceptar las políticas de privacidad, términos y condiciones a modo de un contrato de adhesión.



HIPÓTESIS

Derivado del creciente número de usuarios de redes sociales y usuarios de aplicaciones con navegación asistida por el sistema de posicionamiento global, más conocido como GPS, es prioritaria la necesidad de actualizar, establecer y definir normas que protejan los datos sensibles de los usuarios y las políticas de privacidad. Ante un nuevo concepto de realidad y espacio, las normas que componen el ordenamiento jurídico no tienen el alcance suficiente para regular las nuevas conductas que surgen en el uso de redes sociales y aplicaciones por GPS, y necesariamente deben ser reguladas por el Estado en virtud de garantizar la privacidad, intimidad, seguridad, libertad de expresión e igualdad de las personas.



COMPROBACIÓN DE HIPÓTESIS

Culminado el proceso de investigación, cumpliendo con un análisis de las políticas de privacidad, términos y condiciones se puede concluir en que las mismas deben ser modificadas y la legislación vigente debe incluir normas que se adecúen a este fenómeno, así como la regulación de nuevas conductas que surgen en el uso de internet y redes sociales. Para llevar a cabo este trabajo de investigación se utilizaron: el método inductivo ya que se han identificado carencias legislativas en fenómenos particulares dentro de las redes sociales; el método deductivo en virtud que se analizan las políticas de privacidad, términos y condiciones de las diferentes redes sociales para evidenciar la falta de protección a los datos personales; y, comparativo porque se han observado las diferencias legislativas que preceptúan otros ordenamientos jurídicos. En consecuencia, existen deficiencias en cuanto a la privacidad y protección de los datos. Tal es caso de *Cambridge Analytica* con fines de campaña electoral en los Estados Unidos de América, que vulneró la privacidad de datos de millones de usuarios de la red social *Facebook*, una de las redes sociales más utilizadas en Guatemala. La vulnerabilidad de la privacidad de datos personales planteada en la hipótesis es validada.



ÍNDICE

	Pág.
Introducción.....	i

CAPÍTULO I

1. Marco jurídico.....	1
1.1. Derecho constitucional.....	1
1.1.1. Constitución Política de la República de Guatemala.....	2
1.1.2. Hábeas Data.....	5
1.1.3. Libertad de expresión.....	7
1.1.4. Ley de Acceso a la Información Pública.....	11
1.2. Derecho informático.....	11
1.2.1. Sociedad de la información.....	12
1.3 Derecho penal.....	13

CAPÍTULO II

2. Internet.....	17
2.1. Origen.....	19
2.1.1. Organizaciones.....	21
2.2. Seguridad en internet.....	24
2.3. Web.....	26
2.3.1. Funcionamiento de la web.....	27



CAPÍTULO III

3. Redes sociales.....	31
3.1. Origen.....	31
3.2. Naturaleza jurídica de las redes sociales.....	35
3.3. <i>Facebook</i>	36
3.3.1. Privacidad de datos personales.....	39
3.4. <i>WhatsApp Inc</i>	43
3.5. Problemática jurídica de las redes sociales en Guatemala.....	44

CAPÍTULO IV

4. Aplicaciones con navegación asistida por GPS.....	47
4.1. Sistema de posicionamiento global.....	47
4.2. <i>Waze</i>	51
4.3. <i>Tinder</i>	53
4.4. <i>Google Maps</i>	57

CAPÍTULO V

5. Vulneración en el uso de datos personales en redes sociales y aplicaciones con navegación asistida por GPS	61
5.1. Datos personales sensibles.....	62
5.2. Legislación extranjera sobre la protección de datos personales.....	65



Pág.

5.3. Propuesta de reforma al Código Penal Decreto Número 17-73.....	67
CONCLUSIÓN DISCURSIVA.....	71
BIBLIOGRAFÍA.....	73



INTRODUCCIÓN

Debido al aumento en la creación de redes sociales y aplicaciones con navegación asistida por el sistema de posicionamiento global que ha sido evidente en los últimos años, la vulnerabilidad a la que están expuestos la privacidad y los datos personales de los usuarios de las distintas redes sociales y las aplicaciones en cuestión ha crecido de forma exponencial; por lo que actualmente este es un tema de relevancia trascendental para el fortalecimiento del sistema democrático que ostenta la República de Guatemala, ya que es deber del Estado garantizar a sus ciudadanos la protección de los derechos considerados como inherentes a las personas.

El objetivo general del presente trabajo de investigación es el uso inadecuado de datos que, sin consentimiento de usuarios, es utilizado de forma anómala por parte de algunas plataformas virtuales. Asimismo, se pretende concientizar del contenido que se hace público ya que muchos usuarios desconocen el alcance que pueden llegar a tener.

La hipótesis del presente trabajo de investigación hace referencia a la carencia legislativa en virtud que las normas que integran el ordenamiento jurídico no tienen el alcance suficiente para regular las nuevas conductas que surgen en el uso de redes sociales y aplicaciones por GPS. La hipótesis es validada ya que la falta de regulación genera vulnerabilidad a la privacidad, intimidad, seguridad, libertad de expresión e igualdad de las personas en el uso de redes sociales y aplicaciones con navegación asistida por GPS.

En consecuencia, la presente investigación se estructura de la forma siguiente: En el capítulo I se constituyen las ramas del derecho que atañen al tema en cuestión; El capítulo II hace referencia al Internet y la forma en que ha surgido, asimismo su funcionamiento; el capítulo III versa sobre las redes sociales, siendo el tema central de



esta investigación, se lleva a cabo un análisis sobre el origen de las mismas, así como de la naturaleza jurídica y la problemática jurídica que surge en su uso; el capítulo IV radica en las aplicaciones con navegación asistida por GPS o Sistema de Posicionamiento Global, tales como *Waze*, *Google Maps*, *Tinder*, analizando los aspectos principales de cada una, su funcionamiento y la vulnerabilidad que existe en virtud del manejo de ubicación de los usuarios; y, el capítulo V se centra en la privacidad de datos personales en el uso de redes sociales y aplicaciones con navegación asistida por GPS, así mismo se plantea una propuesta de reforma al Código Penal, Decreto Número 17-73.

Es importante establecer que existen agencias de seguridad, compañías privadas y entidades reconocidas a nivel mundial han desarrollado sistemas informáticos que tienen por objeto la obtención de datos que se generan en el uso de internet y redes sociales, generando una violación a la privacidad de datos personales de usuarios de redes sociales y aplicaciones de navegación asistida por GPS, por lo tanto es de imperante que se adecúen normas jurídicas para el efecto.

En el presente trabajo de investigación se han empleado los métodos siguientes: el método deductivo, que permite establecer la falta de adecuación de las normas jurídicas relativas a la protección de datos personales; el método inductivo, a través del cual se concluye que existen nuevas conductas en el uso de redes sociales con necesidad de ser reguladas; y, el método comparativo, porque en diferentes ordenamientos jurídicos la regulación sobre la protección de datos personales ha sido adecuada a la realidad social. La técnica utilizada fue eminentemente bibliográfica.

La presente tesis tiene por objeto de acercar al lector a una mayor comprensión, a generar conciencia en el uso de redes sociales, los riesgos que se derivan así como obtener un panorama actual sobre la realidad social en Guatemala y demostrar la insuficiencia legislativa existente en cuanto a la protección de datos personales.



CAPÍTULO I

1. Marco jurídico

El impacto de la tecnología genera cambios significativos dentro de la sociedad y los sistemas de derecho vigentes. El aspecto informático no puede quedar sin un control legal, así como el encuadramiento de nuevos tipos penales que surgen. Tal es el caso del uso de redes sociales y aplicaciones con navegación asistida por GPS.

El derecho informático se encarga de buscar soluciones a los retos planteados por la evolución de las aplicaciones digitales. En consecuencia, esta rama del derecho se encuentra en constante cambio y procura el estudio de los avances, los adelantos y las transformaciones tecnológicas con el fin de establecer las medidas adecuadas que permitan una armónica convivencia social.

1.1. Derecho constitucional

Es considerado como la rama del derecho público que comprende la estructura del Estado dentro de una constitución, la situación del individuo frente al poder del Estado, la organización y funcionamiento de ese poder en sus aspectos fundamentales y las instituciones políticas que constituyen el soporte de ese poder estatal.



1.1.1 Constitución Política de la República de Guatemala

La Constitución Política de la República de Guatemala se encuentra en la parte más alta del ordenamiento jurídico, la cual comprende un conjunto de principios y normas jurídicas que regulan el fin y los deberes del Estado, los derechos humanos individuales, sociales, colectivos, económicos y culturales, así como los derechos y deberes cívico-políticos de los ciudadanos; establece la estructura y organización del Estado de Guatemala en tres organismos y demás entidades centralizadas, desconcentradas, descentralizadas y autónomas; instituye las garantías constitucionales para la defensa de los derechos fundamentales, e instaura un órgano de jurisdicción privativa encargado de la defensa del orden constitucional, y la Comisión y Procuraduría de los Derechos Humanos.

La supremacía constitucional es reconocida en la misma Constitución Política de la República de Guatemala: serán nulas *ipso jure* las leyes y disposiciones gubernativas o de cualquier otro orden que disminuyan, restrinjan o tergiversen los derechos que la Constitución Política de la República de Guatemala garantiza. Ninguna ley podrá contrariar sus disposiciones. Los tribunales de justicia en toda resolución o sentencia observarán obligadamente que la Constitución Política de la República de Guatemala prevalece sobre cualquier ley o tratado. La Asamblea Nacional Constituyente emite el 31 de mayo de 1985 la Constitución Política de la República de Guatemala, y entra en vigencia el 14 de enero de 1986.



La Constitución Política de la República de Guatemala está dividida en cinco partes, que son: dogmática, orgánica, pragmática referente a las garantías constitucionales, de las reformas constitucionales y disposiciones finales y transitorias.

La parte dogmática se refiere a aquella en la que se establecen los principios, creencias y, fundamentalmente, los derechos humanos, tanto individuales como sociales, que se le otorgan al pueblo como sector gobernado frente al poder público como sector gobernante, para que éste último respete esos derechos.

En referencia a la parte orgánica, se refiere a aquella que establece cómo se organiza el Estado de Guatemala; la forma de organización del poder, es decir, la estructura jurídico-política del Estado; y las limitaciones del poder frente a la persona o población.

Dentro de la parte pragmática se instauran las garantías constitucionales para la defensa del orden constitucional y velar por el cumplimiento del ordenamiento jurídico guatemalteco.

La parte reformativa comprende los órganos estatales que ostentan la facultad de tener iniciativa de reforma constitucional.



En la parte de las disposiciones finales y transitorias, se norman temas referentes a la promulgación y vigencia y demás disposiciones acordes a la Constitución Política de la República de Guatemala.

Dentro de la Constitución Política de la República de Guatemala, se protege la intimidad y privacidad de las personas. Sin embargo, dichos preceptos fueron promulgados en un momento en que Internet, la telefonía móvil, y las tecnologías de información y comunicación eran inexistentes. En consecuencia, determinar el alcance de las normas jurídicas y si es suficiente para dar una respuesta efectiva a la vulneración de derechos en la red, o bien si es necesaria la implementación de nuevas normas jurídicas que protejan a los usuarios de Internet.

Atendiendo a lo que establece la Constitución Política de la República de Guatemala en cuanto a la privacidad y el derecho de intimidad, el Artículo 24 norma: "Inviolabilidad de correspondencia, documentos y libros. La correspondencia de toda persona, sus documentos y libros son inviolables. Sólo podrán revisarse o incautarse, en virtud de resolución firme dictada por juez competente y con las formalidades legales. Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna.

Los libros, documentos y archivos que se relacionan con el pago de impuestos, tasa, arbitrios y contribuciones, podrán ser revisados por la autoridad competente de



conformidad con la ley. Es punible revelar el monto de los impuestos pagados, utilidades, pérdidas, costos y cualquier otro dato referente a las contabilidades revisadas a personas individuales o jurídicas, con excepción de los balances generales, cuya publicación ordene la ley.

Los documentos o informaciones obtenidas con violación de este artículo no producen fe ni hacen prueba en juicio.”

Es implícita la protección del derecho a la privacidad e intimidad que la Constitución Política de la República de Guatemala comprende en el Artículo referido. El texto constitucional además de establecer una clasificación de comunicaciones que gozan de protección, no restringe nuevas comunicaciones que puedan surgir. Acertadamente, se toma en cuenta el progreso tecnológico y el cambio incesante que existe en la sociedad y de esta forma adaptarse a nuevas realidades sociales al garantizar el secreto de correspondencia a otros productos de la tecnología moderna. Sin embargo, es necesaria la adaptación a la realidad social del ordenamiento jurídico para evitar la vulneración de los bienes jurídicos tutelados.

1.1.2. Hábeas data

Para definir esta figura, se cita a Tiberio Torres que en su obra establece: “Es una garantía de carácter constitucional que le permite a la persona, individual o colectiva,



conocer de la información que sobre sí misma reposa en un registro o banco de datos de carácter público o privado, y cuando es del caso, exigir su corrección o modificación si dichos datos son erróneos, inexactos o falsos y le causan algún tipo de perjuicio.”¹

Atendiendo a lo anterior, existe la problemática jurídica al momento de crear una cuenta de una determinada red social. En virtud que se desconoce el alcance que pueden tener los datos personales, datos sensibles de cada usuario y cuáles personas tienen acceso a los mismos, sin consentimiento; vulnerando totalmente la privacidad de los usuarios de las redes sociales.

El Hábeas Data es una garantía que permite acceder a un banco de información o registro de datos que incluye referencias informativas sobre información personal. El sujeto tiene derecho a exigir que se corrijan, modifiquen o extingan parte o la totalidad de los datos en caso que estos le generen algún tipo de perjuicio o que sean erróneos.

En ese orden de ideas, este derecho constitucional faculta a las personas el manejo sobre la adecuada manipulación de la información personal que se encuentra bajo conocimiento de terceros. Esto permite impedir los abusos y corregir los errores involuntarios en la administración y publicación de dichos datos.

¹ **La protección de la intimidad en el derecho tributario.** Pág. 21.



Dentro de la legislación guatemalteca se reconoce el Hábeas data como una acción que permite a los ciudadanos requerir cualquier información propia que conste en archivos, en virtud de lo cual el Artículo 30 de la Constitución Política de la República de Guatemala norma: “Publicidad de los actos administrativos. Todos los actos de la administración son públicos. Los interesados tienen derecho a obtener, en cualquier tiempo, informes, copias, reproducciones y certificaciones que soliciten y la exhibición de los expedientes que deseen consultar, salvo que se trate de asuntos militares o diplomáticos de seguridad nacional, o de datos suministrados por particulares bajo garantía de confidencia.”

En ese orden de ideas, el Artículo 31 de la Constitución Política de la República de Guatemala establece: “Acceso a archivos y registros estatales. Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos.”

1.1.3. Libertad de expresión

Dentro del ordenamiento jurídico guatemalteco, en la Constitución Política de la República de Guatemala es reconocido el derecho a la libertad de emisión del pensamiento. Disposición que también es denominada en otros cuerpos normativos



como libertad de expresión. Debido al crecimiento exponencial de las redes sociales, existen muchas cuentas falsas que pueden ser utilizadas para fines ilícitos.

Para el efecto, el Artículo 35 de la Constitución Política de la República de Guatemala norma: "Libertad de emisión del pensamiento. Es libre la emisión del pensamiento por cualesquiera medios de difusión, sin censura ni licencia previa. Este derecho constitucional no podrá ser restringido por ley o disposición gubernamental alguna. Quien en uso de esta libertad faltare al respeto a la vida privada o a la moral, será responsable conforme a la ley. Quienes se creyeren ofendidos tienen derechos a la publicación de sus defensas, aclaraciones y rectificaciones.

Los funcionarios y empleados públicos podrán exigir que un tribunal de honor, integrado en la forma que determine la ley, declare que la publicación que los afecta se basa en hechos inexactos o que los cargos que se les hacen son infundados. El fallo que reivindique al ofendido, deberá publicarse en el mismo medio de comunicación social donde apareció la imputación.

La actividad de los medios de comunicación social es de interés público y éstos en ningún caso podrán ser expropiados. Por faltas o delitos en la emisión del pensamiento no podrán ser clausurados, embargados, intervenidos, confiscados o decomisados, ni interrumpidos en su funcionamiento las empresas, los talleres, equipo, maquinaria y enseres de los medios de comunicación social.



Es libre el acceso a las fuentes de información y ninguna autoridad podrá limitar ese derecho.

La autorización, limitación o cancelación de las concesiones otorgadas por el Estado a las personas, no pueden utilizarse como elementos de presión o coacción, para limitar el ejercicio de la libre emisión del pensamiento.

Un jurado conocerá privativamente de los delitos o faltas a que se refiere este artículo. Todo lo relativo a este derecho constitucional se regula en la Ley Constitucional de Emisión del Pensamiento.

Los propietarios de los medios de comunicación social, deberán proporcionar cobertura socioeconómica a sus reporteros, a través de la contratación de seguros de vida.”

Las empresas de redes sociales no tienen la capacidad de ejecutar enérgicamente sus propias políticas de privacidad, términos y condiciones, en función de evitar la suplantación, con lo cual hace posible la divulgación de noticias falsas y de propaganda, y permiten que prospere un mercado negro de identidades falsas en sus plataformas sociales.



Asimismo, la Ley de Libre Emisión del Pensamiento, es la norma jurídica de rango constitucional y emitida por los diputados a la Asamblea Nacional Constituyente, que regula el ejercicio de este derecho fundamental. La necesidad de crear una ley específica se establecía en el Artículo 65 de la Constitución Política de la República de Guatemala de 1965, el anterior texto constitucional a la era democrática. En consecuencia, es importante comprender que la regulación de este derecho requiere la adecuación a la realidad nacional e internacional.

La Ley de Libre Emisión del Pensamiento establece en su articulado que la emisión del pensamiento es libre en cualesquiera formas, es decir, se garantiza el derecho de las y los ciudadanos de expresarse por cualquier medio. Para los efectos de la Ley, los medios que sirven de soporte para la emisión del pensamiento son los siguientes: impresos, de radiodifusión y televisión, y por cualquier otro procedimiento que pueda emplearse en el futuro para la reproducción de las ideas.

Por otro lado, la Ley de Libre Emisión del Pensamiento regula que ninguna persona puede ser molestada ni perseguida por las opiniones que exprese por cualquier medio. La excepción a esta protección se aplicaría a aquellas personas que falten el respeto, la vida privada, moral o incurran en delitos y faltas contenidos en este cuerpo normativo, y, en consecuencia, serán responsables por sus conductas ante la ley.



1.1.4. Ley de Acceso a la Información Pública

El Decreto Número 57-2008 del Congreso de la República de Guatemala, Ley de Acceso a la Información Pública, se constituye como uno de los pilares fundamentales para la consolidación de un Estado democrático de Derecho, ya que facilita el desarrollo de un mecanismo de control social a través de la información, especialmente la de carácter público.

Básicamente, una de las finalidades del cuerpo normativo en cuestión, es llevar a cabo la reconstrucción del concepto transparencia y crear confianza en la autoridad por parte de los ciudadanos en cuanto al funcionamiento, estructura y organización de las entidades públicas. La justificación de la existencia de un cuerpo normativo que regule este derecho es brindar herramientas y procedimientos efectivos a la ciudadanía para el ejercicio de sus derechos fundamentales, permitiendo así la eficiencia y eficacia en el sector público. A través de la construcción participativa de todos los sectores de la sociedad guatemalteca, fortaleciendo la institucionalidad, la transparencia y el combate a la corrupción e impunidad.

1.2. Derecho informático

El derecho informático es una disciplina jurídica moderna que tiene como objeto inmediato de estudio la informática y como objeto mediato la información. Su método



científico se caracteriza por desarrollar las instituciones jurídicas informáticas e interrelacionarlas sistemáticamente con la realidad; así, se tiene que los problemas derivados del *software*, de la información computarizada, del *hardware*, *firmware*, *shareware* y otros bienes, son tratados desde sus distintos alcances en el ordenamiento legal, buscando coherencia y tratamiento integral.

Como principio general, el derecho debe evolucionar con las nuevas necesidades y costumbres de los seres humanos para regular adecuadamente las nuevas relaciones que surgen. En consecuencia, esta rama jurídica es considerada como un punto de inflexión del derecho, puesto que todas sus áreas de estudio se han visto afectadas por la aparición de la sociedad de la información, cambiando de este modo los procesos sociales y, por tanto, los procesos políticos y jurídicos.

1.2.1. Sociedad de la información

El imparable desarrollo tecnológico está afectando de forma profunda a todas las actividades que realizan los seres humanos, tanto en su trabajo y en su ocio como en su forma de relacionarse o de comunicarse. Esta denominación, hace referencia a que la información de cualquier naturaleza, su generación, su distribución y su uso se han convertido en el eje fundamental de todo lo que hacen los seres humanos.



Más allá de la tecnología, el correcto desarrollo de la Sociedad de la Información depende también del establecimiento de un marco legal y regulatorio adecuado, que permita la inversión de recursos y el desarrollo de todas las aplicaciones y servicios que hacen posible la nueva etapa de la sociedad.

En ese orden de ideas, Raúl Trejo Delarbre indica que “las sociedades de la información se caracterizan por basarse en el conocimiento y en los esfuerzos por convertir la información en conocimiento. Cuanto mayor es la cantidad de información generada por una sociedad, mayor es la necesidad de convertirla en conocimiento. Otra dimensión de tales sociedades es la velocidad con que la información se genera, transmite y procesa. En la actualidad, la información puede obtenerse de manera prácticamente instantánea y, muchas veces, a partir de la misma fuente que la produce, sin distinción de lugar.”²

1.3. Derecho penal

Es una rama del derecho público que contiene el conjunto de normas jurídicas que regulan la potestad punitiva del Estado, asociando a los hechos estrictamente determinados por la ley, como presupuesto, una pena, medida de seguridad o corrección como consecuencia; con el objetivo de asegurar los valores elementales sobre los cuales descansa la convivencia humana pacífica.

² **La nueva alfombra mágica. Usos y mitos de internet, redes sociales. Pág. 25.**



La facultad de castigar corresponde con exclusividad al Estado, se manifiesta para su aplicación a través de un conjunto de normas jurídico-penales, que tienen a regular la conducta humana en una sociedad jurídicamente organizada y ese conjunto de normas penales que tienen un doble contenido: la descripción de una conducta antijurídica y la descripción de las consecuencias penales.

La ley penal es el conjunto de normas jurídicas que definen los delitos y las falta, determinan las responsabilidades o las exenciones y establecen las penas o medidas de seguridad que corresponden a las figuras delictivas.

Algunas características de la ley penal son:

- a. Igualdad. Todas las personas son iguales ante la ley sin distinción alguna, con excepción del antejudio y la inmunidad.
- b. Exclusividad. Corresponde a la ley penal la creación de delitos, establecer penas y medidas de seguridad para los mismos.
- c. Sancionadora: Se refiere a la consecuencia jurídica establecida en la norma jurídica, que puede ser una pena o una medida de seguridad.
- d. Constitucional. En virtud que su fundamento está en la Constitución Política de la República de Guatemala.



El jurista Moisés Barrio Andrés en su obra indica sobre el delito informático que “la realización de una acción, que reuniendo las características que delimitan el concepto de delito, sea llevada cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea *hardware* o *software*.”³

Uno de los principales elementos de la teoría general del delito es la tipicidad, que hace referencia a encuadrar, subsumir o adecuarse a un tipo penal. El tipo penal es considerado como la descripción de la conducta que el legislador ha plasmado en la norma penal como un supuesto de hecho. Ahora bien, en el uso de redes sociales e internet surgen nuevas conductas que deben ser reguladas.

El almacenamiento y registro de datos personales suponen la sensible exposición de la intimidad personal a intromisiones y transgresiones extrínsecas. El avance tecnológico en el área informática y en el ámbito de las comunicaciones ha determinado la proliferación y versatilidad de las eventuales vulneraciones a esta facultad. En consecuencia, las legislaciones extranjeras han propiciado la regulación jurídica penal sobre la protección de datos y la intimidad, contemplándose no sólo mecanismos de prevención sino también de sanción.

³ **Ciberdelitos, amenazas criminales del ciberespacio.** Pág. 25.





CAPÍTULO II

2. Internet

Se trata de un sistema de redes informáticas interconectadas mediante distintos medios de conexión, que ofrece una gran diversidad de servicios y recursos, como, por ejemplo, el acceso a plataformas digitales.

Internet ha sido considerada como una asociación de miles de redes y millones de computadores alrededor del mundo que trabajan juntas compartiendo información. Existen rutas principales, llamadas columnas vertebrales, *backbones*, y transportan la mayor parte del tráfico de información en la red. Estos *backbones* forman el sistema más grande de redes y son propiedad de los mayores proveedores del servicio de internet, *internet's services providers*: ISP, quienes se encargan de distribuir el acceso a la red a través de la obtención de licencias.

Para Omar Barrios, internet "es una contracción de *internetwork system* (sistema de intercomunicación de redes). Algunos técnicos lo identificaban como una contracción de Red Internacional de Computadoras. Es el conjunto de todas las redes IP interconectadas en tiempo real, vía protocolos de interconexión TCP/IP. Es un sistema



maestro de diversas redes de computación que cumple con dos funciones básicas: medio de comunicación y medio de información.”⁴

Dichas redes son adquiridas por pequeños proveedores de servicios de Internet (ISP) locales y regionales, quienes permiten a compañías e individuos acceder en turno a las áreas de cobertura. Sin embargo el literario Etienne Sanz de Acedo Hecquet, muestra su postura con respecto al control del Internet, “ninguna persona, compañía, institución u organización gubernamental es dueña de Internet, ni tampoco lo gobierna, o incluso tiene un interés controlante. El Internet es de verdad una empresa colaboradora, colectiva.”⁵

En relación a lo anterior, si cualquiera de las empresas, los organismos o las instituciones que intervienen tuviera, de alguna manera, la posibilidad de modificar, condicionar, dominar u obtener una posición de predominio, se estará frente al verdadero controlador o, al menos, al mayor influyente de Internet.

Sin embargo, el control al cual se hace referencia, no debe ser el control formal; aunque de hecho existan una serie de reglamentaciones que emanan de las organizaciones que tienen gran injerencia en el desarrollo de la red.

⁴ **Derecho e Informática: aspectos fundamentales.** Pág. 36.

⁵ **Marcas renombradas y nombres de dominio en Internet: En torno a la ciberpiratería.** Pág. 57.



Hecquet indica que “el Internet, puede describirse simplemente la red de redes, es un sistema mundial de redes de computadoras, un conjunto integrado por las diferentes redes de cada país del mundo, por medio del cual un usuario en cualquier computadora puede, en caso de contar con los permisos apropiados, ingresar información de otra computadora y poder tener inclusive comunicación directa con otros usuarios en otras computadoras.”⁶ Es plurijurisdiccional, en virtud que los usuarios pueden tener acceso desde cualquier parte del planeta. Debido a su tecnología de conmutación de paquetes, la información puede viajar a través de diversos países o jurisdicciones para llegar a su destino.

El Internet no tiene una reglamentación específica, se ve afectado por la legislación y los reglamentos que se aplican generalmente en las distintas jurisdicciones del mundo. Sin embargo han sido pocas las disposiciones legislativas nacionales dirigidas específicamente a Internet y no se ha diseñado ningún instrumento jurídico internacional para regular el Internet.

2.1. Origen

Al principio, el internet era como red galáctica, dicho término fue acuñado en 1962 por el informático estadounidense Joseph Licklider. La red era comprendida como “un conjunto de ordenadores interconectados globalmente, a través de los que todo el mundo podía

⁶ **Ibid.** Pág. 58.

acceder rápidamente a datos y programas desde cualquier sitio.”⁷ Básicamente es una noción de lo que ahora se conoce como internet.

La aplicación del proyecto al plan ARPANET, que se refería a una red de computadoras situadas en distintos puntos estratégicos de los Estados Unidos con el objeto de instalar y conectar el primer *host* en la historia mundial llevado a cabo por la Universidad de California. Consecuentemente, hubo un progreso marcado y una expansión que permite a las universidades el desarrollo de la red.

La versión mencionada surge a finales de los años cincuenta con la implementación práctica de estos conceptos tecnológicos. Se le atribuye a la década de los ochentas, como las bases de internet, lo cual comienza a expandirse por todo el mundo y se crea por ende la *World Wide Web* (WWW).

En consecuencia, internet se esparce de manera global con objetivo de dar inicio a la moderna red mundial de ordenadores. Se crea un acceso mundial a la información y comunicación sin precedentes. Internet también alteró la economía del mundo entero. Es un fenómeno que no ha terminado de regularse en su totalidad, así como las conductas que devienen en el uso del mismo.

⁷ Leiner, Barry: <https://www.internetsociety.org/es/breve-historia-de-internet/> (Consultado: 10 de enero de 2018.)



2.1.1. Organizaciones

En internet existe un completo conjunto de organizaciones que son verdaderamente influyentes y han conformado juntas una clase de sistema de intrincados controles recíprocos. Es oportuno repasar el cúmulo de organizaciones de tipo no gubernamental, sin fines de lucro, que están a cargo de los distintos aspectos de la red. Esta es la característica más sobresaliente de Internet, un servicio que está manejado por organizaciones sin fines de lucro, de las cuales emanan normas que se hacen obligatorias para todos aquellos que utilizan este servicio. Estas normas tienen origen contractual y no por ello son de menor importancia.

- A. ISOC (*Internet Society*): Es un grupo conformado por profesionales expertos en Internet, que a través de sus opiniones y evaluaciones, examinan constantemente las políticas y las prácticas a ser adoptadas. Así mismo, supervisan a otras organizaciones, grupos de tareas y consejos, que trabajan en las decisiones de políticas de la red.
- B. IETF (*Internet Engineering Task Force*): Sus inicios fueron en 1986, básicamente su función consiste en desarrollar protocolos y conectividad de la red.
- C. IAB (*Internet Architecture Board*): El IAB es un grupo de consultores técnicos informáticos de la ISOC, que tienen por función la creación de mecanismos que



permitan fluidez constante en la conmutación de paquetes para un correcto desempeño de la red.

- D. IRTF (*Internet Research Task Force*): La función principal de la IRTF comprende la investigación y comprensión de la trascendencia que genera el progreso que el Internet logra en el tiempo, para lo cual cuenta con grupos de largo y corto plazo, abocados al estudio de los protocolos, las aplicaciones, la arquitectura y la tecnología de la red. La organización está conducida por su jefe, quien es designado por el IAB.
- E. ISTF (*Internet Societal Task Force*): Es una organización abierta de personas, que tienen por objeto ejecutar la misión de la *Internet Society* (ISOC), es decir, asegurar un abierto desarrollo, evolución y uso de Internet, para el bienestar de todos los usuarios alrededor del mundo. Debido al impacto económico y social de Internet, las cuestiones políticas adquieren tanta importancia como las técnicas. Su principal propósito es describir los pasos a seguir para asegurar que Internet sea para todos. Para ello, caracteriza las dificultades sociales y económicas relacionándolas con el desarrollo y utilización de la red, como asimismo la identificación y la descripción de condiciones locales, regionales y globales, para ayudar al uso y disponibilidad de Internet de manera global.
- F. IANA (*Internet Assigned Numbers Authority*): La IANA está a cargo de los parámetros originales de Internet, incluidas las direcciones de IP. Tiene su sede en el Instituto de Ciencias de la Información de la Universidad del Sur de California. Cada nombre de

dominio está asociado con una única dirección IP, un número que consiste de cuatro bloques hasta tres dígitos cada uno, cuyo sistema se utiliza para direccionar la información a través de la red. La IANA es la autoridad responsable de:

- La vigilancia del alojamiento de las direcciones IP;
- La coordinación de la asignación de los parámetros de protocolo provistos por los estándares técnicos de Internet;
- El manejo de los DNS;
- La delegación de los dominios de primer nivel;
- La vigilancia del sistema de servidor de nombres de raíz.

Los autores que tienen por ocupación el funcionamiento y desarrollo de Internet, se encargan de remarcar que no se puede asimilar este control al control en términos políticos o jurídicos, sino más bien a cierto tipo de influencia económica debido al impacto que tiene en la sociedad. Es importante destacar la distinción al momento de hablar de control, autoridad de control y autoridad de aplicación; elementos que no existen en Internet.

Es una problemática que atenta a los usuarios en virtud que no hay un estatuto ni normas jurídicas consensuadas o impuestas que tengan por finalidad proteger los datos personales y la privacidad de los usuarios de internet; a pesar que, existe alguna normativa aislada, no abarca los alcances de la red en todo el mundo.



No obstante, este panorama deja la pauta sobre la falta de una autoridad, al menos en los términos tradicionales. Esto tiene razón de ser en virtud del sistema en el cual fueron elaboradas las reglamentaciones que regulan estas organizaciones, y que provienen generalmente de delegaciones estatales o fueron elaboradas mediante el método de consultas.

2.2. Seguridad en internet

La seguridad en internet es un tema que atañe el análisis de varios componentes, como los son la fuente del ataque, el objeto del ataque, las calidades de los atacantes y los atacados, y la diferenciación entre ataque a la seguridad y a la privacidad. Siendo el objetivo principal la prevención de ataques dirigidos a los bienes jurídicos tutelados.

En consecuencia, se originan acciones que atentan en contra de la privacidad de los usuarios de internet, tales como *phishing*, que hace referencia a una suplantación de identidad. Básicamente es un término informático que denomina un modelo de abuso y que se caracteriza por intentar adquirir información confidencial de forma fraudulenta.

Para Francisco Palomares, “El cibercriminal, conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso



utilizando también llamadas telefónicas.”⁸ En el 2017, Google sufrió ataques relacionados a la figura anterior y reconoció públicamente que sus medidas de control y protección fueron superadas.

Es importante destacar que la legislación guatemalteca, si bien regula algunos delitos informáticos, necesita regular figuras nuevas, establecer nuevos tipos penales acordes a la realidad social y, específicamente, que puedan originarse debido al uso de internet. Existen ordenamientos jurídicos extranjeros que establecen la protección de bienes jurídicos tutelados, incluyendo nuevos tipos penales, referentes al uso indebido de las redes sociales, el uso de internet, tales como:

- a. Difusión y exhibición de datos personales sensibles;
- b. Interceptación de comunicaciones escritas;
- c. Estafas electrónicas;
- d. Publicidad engañosa;
- e. Daños informáticos;
- f. Distribución de contenido publicado por usuario sin consentimiento;
- g. Comercialización de datos personales.
- h. Elaboración de bases de datos clandestinas.

⁸ Resolución de averías lógicas en equipos microinformáticos. Pág. 159.

2.3. Web

La *web* emplea páginas individuales, normalmente combinadas para constituir sitios. Las páginas *web* se escriben en HTML, que hace referencia al idioma de señalización de hipertextos que instruye al *browser* de la *web*, como hacer el despliegue de la página y los elementos. En consecuencia, la principal función de la *web* es conectar páginas entre sí a vídeo, audio y archivos de imágenes por medio de hipervínculos.

A pesar de su habilidad de *hyperlinking*, la primera *web* fue elaborada por un tiempo en forma marginal, mediante una alternativa poco conocida y técnicamente menos avanzada que el *gopher protocol*. Pero en 1993, Marc Andreessen, introdujo el primer *browser web* gráfico, llamado mosaico.

Un sitio *web* hace referencia al conjunto de páginas *web* que se desarrollan en código html, y que están relacionadas a un dominio de internet que puede visualizarse en la *World Wide Web* (www) a través los navegadores *web*. Así mismo, se establece una clasificación de sitios *web*, siendo los anteriores, estáticos y dinámicos. Los primeros se refieren a aquellos que no acceden a una base de datos para obtener el contenido. Por lo general un sitio *web* estático es utilizado cuando el propietario del sitio no requiere realizar un continuo cambio en la información que contiene cada página. Y los segundos, son aquellos que acceden a una base de datos para elaborar los contenidos y reflejar los resultados obtenidos de la base de datos, en las páginas del sitio *web*.



El propietario del sitio *web* podrá agregar, modificar y eliminar contenidos de éste a través de un sistema *web*, generalmente con acceso restringido al público mediante usuario y contraseña, tal es el caso en una magnitud mayor de las plataformas de redes sociales.

2.3.1. Funcionamiento de la *web*

Para la comprensión del funcionamiento de la *web* es fundamental entender que está basada en un juego de reglas de intercambio de textos, imágenes, video y otros archivos de multimedia, conocidos colectivamente como HTTP (protocolos de transferencia de hipertextos). La página *web* puede intercambiarse en internet porque ambos, el *browser* y los servidores de *web*, funcionan valiéndose del HTTP.

La *web* posee un esquema de direcciones que cada computadora de la red compatibiliza. En consecuencia, es imprescindible definir a la dirección IP, que se refiere a un número de cuatro dígitos, que identifica e individualiza a una computadora específica conectada a Internet. Estos dígitos se organizan en cuatro grupos de números separados por períodos.

Los nombres de dominio constituyen el nivel siguiente de direcciones de internet, creando una sola identidad, para una serie de computadoras utilizadas por una compañía o institución. Es decir, que dentro de una compañía existen 50 servidores y cada uno con

su propia dirección IP, sin embargo todos comparten un nombre de dominio común. En ese orden de ideas, el nombre de dominio identifica a las computadoras en un grupo.

En caso de querer obtener una página específica almacenada en cualquiera de esas computadoras es necesaria una dirección más precisa. Cada página *web* tiene su propia y única dirección, también conocida como recurso de localización uniforme, que instruye al browser los pasos a seguir para encontrar una página.

Con objeto de complementar la explicación del funcionamiento *web*, se definen los siguientes términos:

- a. TCP/IP: Protocolo de Control de Transmisión y Protocolo de Internet, son los protocolos de comunicación que definen cómo deben transportarse los datos a través de la *web*.
- b. DNS: Los servidores del Sistema de Nombres de Dominio, hacen referencia a las direcciones de sitios *web*. Al momento de ingresar una dirección *web* en el navegador, el navegador identifica los DNS antes de recuperar el sitio *web*, por lo tanto necesita averiguar en qué servidor se encuentra el sitio *web* y así enviar los mensajes HTTP al lugar correcto.



- c. HTTP: Se refiere al Protocolo de Transferencia de Hipertexto que tiene por función ser un protocolo de aplicación que define un idioma para que los clientes y servidores se puedan comunicar.





CAPÍTULO III

3. Redes sociales

Las redes sociales permiten establecer comunicación con usuarios por medio de un sitio *web* y comprenden un conjunto de programas, equipos, transmisores y usuarios que mantienen intereses y actividades en común o bien, se encuentran interesados en conocer nuevos usuarios entablado una conversación desde los servicios propios que cada plataforma virtual de la red social ofrezca.

3.1. Origen

La interacción de los seres humanos es inevitable, las redes sociales se han originado como una herramienta para facilitar dicha interacción. “El estudio de las redes sociales tiene su origen en los años cuarenta y luego alcanza un interesante desarrollo en los sesenta, principalmente en la sociología y en la antropología, y después se extiende a todo el espectro de las ciencias sociales. Ha llegado incluso a ocupar un lugar en el vocabulario de la vida cotidiana, al punto de designar todo tipo de servicios y productos.”⁹

⁹ Varios Autores. **Redes sociales: infancia, familia y comunidad.** Pág. 2.

En consecuencia, el derecho debe tomar en consideración estos avances tecnológicos; y en virtud del uso masivo de las redes sociales en la población, la regulación jurídica de las mismas debe acatarse de una forma más precisa y actualizada.

El desarrollo del pensamiento sobre las redes sociales, atendiendo a lo que establecen Auslande y Litwin, tuvo dos orígenes. El concepto sociológico y la conducta de las personas en función de la situación social, es decir, el grado de influencia y popularidad sobre los demás usuarios.

“Como concepto sociológico, al final de la década de los cuarenta, que sirvió para definir las interrelaciones entre un sistema social, constituyendo un modelo alternativo frente a la entonces dominante perspectiva de acción estructural funcionalista. Desde este enfoque se hizo énfasis en las características de los lazos de unión entre la gente, a partir de las estructuras de la red.

Como consecuencia de los desarrollos de la teoría de campo adaptada por Lewin, en la cual la conducta es considerada como la función de una persona en una situación social. Esto significa que el entendimiento de una acción individual depende tanto del sistema social general en que se desarrollan las acciones como de las relaciones sociales de ese individuo con ese sistema social.”¹⁰

¹⁰ **Ibid.** Pág. 7

En la actualidad, es evidente que las corrientes planteadas por ambos autores están comprobadas. En las redes se construye una visión compartida de la interconexión para el intercambio horizontal de conocimientos, experiencias y posibilidades.

En cuanto a la definición de una red social, Mabel Cajal acierta indicando que “es un sitio en internet que tiene como finalidad servir de herramienta de comunicación entre diversos usuarios que se unen en un mismo espacio virtual para compartir información en diversos formatos como texto, videos, imágenes, música entablando comentarios sobre algún interés o tema común.”¹¹

Existen dos clasificaciones de las redes sociales, pueden ser horizontales y verticales. Según Elia Sánchez, las redes sociales horizontales “Son aquellas dirigidas a todo tipo de usuario y sin una temática definida. Se basan en una estructura de celdillas permitiendo la entrada y participación libre y genérica sin un fin definido, distinto del de generar masa. Ejemplos del sector son *Facebook* o *Twitter*.”¹²

La autora citada hace referencia a las redes sociales verticales, estableciendo que las mismas “están concebidas sobre la base de un eje temático. Su objetivo es el de congregar en torno a una temática definida a un colectivo concreto. En función de su

¹¹<https://www.mabelcajal.com/2017/06/que-es-una-red-social-tipos-redes-sociales-para-que-sirven.html/> (Consultado: 30 de enero de 2018.)

¹²<https://lavanadeelia.wordpress.com/2011/09/27/redes-sociales-verticales-y-horizontales> (Consultado: 30 de enero de 2018.)

especialización, la autonomía que se le ofrece al usuario en el mundo virtual, ha permitido que éste pueda decidir entre múltiples opciones para representarse en el ciberespacio, ya sea extendiendo su propia identidad, creando una falsa, o bien, ocupando una ajena.”¹³

Entre los riesgos más relevantes en el uso de las redes sociales, además de la adicción, destacan: el acceso a contenidos inapropiados, el ciberacoso o la vulneración de la intimidad y privacidad de los usuarios. En virtud de lo anterior, en las redes sociales se puede acceder a contenidos pornográficos o violentos, denigrar a personas, y la realización de publicaciones de mensajes racistas. Ya que no existen filtros de seguridad, si bien es cierto el contenido publicado que tienda a denigrar a las personas puede ser denunciado y por ende borrado de la plataforma virtual. Sin embargo, las capturas de pantalla darán la facilidad para la comercialización y distribución sin consentimiento de dicha publicaciones.

En usuarios vulnerables existe el riesgo de crearse una cuenta de red social falsa, potenciada por un factor de engaño, autoengaño o con finalidad publicitaria, de propaganda o generar tendencias.

¹³ **Ibid.**



3.2. Naturaleza jurídica de las redes sociales

Resulta incuestionable que la naturaleza jurídica de las redes sociales, en cuanto al acuerdo que nace entre el usuario y la plataforma virtual, es un contrato de adhesión. La peculiaridad del mismo reside en el hecho que no son ambas partes las que redactan el clausulado, sino que este es predispuesto e impuesto por una de ellas a la otra, que no puede más que aceptarlo o rechazarlo. Es decir, su especialidad no depende de que el contrato haya sido redactado por una de las partes, sino en que la autonomía de la voluntad de la contraparte queda reducida a su mínima expresión, ya sea simple aceptación.

El contrato de adhesión es aquél cuyo clausulado se redacta por una de las partes sin intervención de la otra, cuya libertad contractual queda limitada a manifestar o no la aceptación de sus estipulaciones, de adherirse o no al contrato.

Villegas Lara establece que “son producto de la negociación en masa; son elaborados en serie, según la ley de los grandes números, sometidos a las leyes de una estandarización rigurosa, que por un proceso de tipificación contractual reduce al mínimo el esfuerzo de las partes y la pérdida de tiempo.”¹⁴

¹⁴ **Derecho mercantil guatemalteco III.** Pág. 34.



El contrato de adhesión circunscribe el consentimiento sin deliberaciones previas al aceptarse una fórmula establecida. En virtud de lo anterior, el usuario en el proceso de creación de cuenta en cualquier red social, debe obligatoriamente aceptar y prestar conformidad a los términos y condiciones del sitio y políticas de privacidad impuestas unilateralmente y el ingreso de correo electrónico, nombre, número telefónico. En esa virtud, la naturaleza jurídica de los términos y condiciones, las políticas de privacidad o los términos de uso es considerada como la de un contrato de adhesión.

3.3. Facebook

En 2004, *Facebook* se origina, en aquel entonces, por el estudiante de *Harvard*, Mark Zuckerberg, como un servicio propio para los estudiantes de dicha universidad. En el primer año de funcionamiento logró la suscripción de más de la mitad del total de los estudiantes de *Harvard*, expandiéndose, por el éxito que tuvo, a varias universidades prestigiosas de Estados Unidos, así como instituciones importantes.

Fue en 2006 cuando *Facebook* lanza la plataforma virtual y naturaleza de red social pública para que usuarios en cualquier parte del mundo crearan su propia cuenta y formaran parte de la misma con un correo electrónico. Un año después del lanzamiento, logró la mayor cantidad de usuarios registrados en comparación con otros sitios *web*, superando los 19 millones de miembros a nivel mundial. Es importante destacar que en sus inicios, *Facebook* fue publicado únicamente en inglés.



Para el ingeniero informático, Ricardo Suárez, *Facebook* “es una plataforma de red social mediante la cual los usuarios pueden mantenerse en contacto continuo con un grupo de amistades e intercambiar con ellos cualquier tipo de contenido, como por ejemplo fotografías, comentarios y memes; a través de internet; pero el poder de Facebook es tal hoy día que la empresa también es dueña de *Instagram* y *WhatsApp*.”¹⁵

Tal es el éxito de dicha compañía, que ha tenido la capacidad económica de adueñarse de otras redes sociales interconectando entre sí las mismas, con objetivos lucrativos que permiten a empresas llegar a mercados de una forma más penetrante, en virtud de conocer los gustos y preferencias de los usuarios a los cuales quieran convertir en un mercado. Los expertos recomiendan para preservar la intimidad y protección de datos personales sensibles, completar los parámetros de privacidad de la cuenta estableciendo las opciones acordes al contenido que se desea hacer público o privado. En consecuencia, se puede limitar el acceso a cada aplicación utilizada, fotografías, información y contenido que se publica dentro de la cuenta de dicha red social.

Así mismo, los parámetros de búsqueda pueden ser modificados con el objeto de limitar los resultados que se deriven de la misma, al momento que cualquier persona con una cuenta o sin ella busque en *Facebook* a cualquier usuario, para lo cual se permite la

¹⁵ <https://iiemd.com/articulo/facebook/que-es-como-funciona-facebook-entrar-2>. (Consultado: 5 de febrero de 2018.)

visualización total, parcial o nula de los datos personales o el perfil sin ninguna información personal.

La tendencia en el uso de redes sociales incrementa constantemente, los servicios de las mismas se han popularizado, así como el incremento de usuarios de internet. *WhatsApp Inc* en conjunto con *Facebook* han pasado a considerarse las redes sociales de mayor preferencia de los usuarios de la red en Guatemala.

Atendiendo al último estudio realizado por la firma de consultoría digital *iLifebet* de redes sociales en Centroamérica de enero de 2018, se estima que “Guatemala se encuentra en el primer lugar, con la mayor cantidad de perfiles en Centroamérica y el Caribe, alcanzando más de 5.3 millones de usuarios, en segundo lugar está República Dominicana, con 4.5 millones, mientras que El Salvador y Costa Rica, con 3.1 y 2.9 millones, respectivamente. Guatemala es además, el país en donde más crece la afición por las redes sociales, ya que desde junio del 2015 hasta la actualidad ha crecido en 1.1 millón de usuarios, mientras que en los últimos tres meses se ha incrementado a un ritmo de 100 mil nuevos usuarios por mes.”¹⁶

En 2011, el CEO de *Facebook*, Mark Zuckerberg, lleva a cabo la adquisición de la red social *Instagram*, es importante mencionar que tal interés no radicaría en la

¹⁶ <http://gtmtecno.com/2016/07/28/estudio-guatemalteco-redes-sociales/>. (Consultado: 11 de abril de 2018.)



aplicación en sí, sino en la adquisición de tres aspectos importantes: un rival potencial con una base de usuarios en rápido crecimiento, un arma para combatir otras amenazas aún más grandes en el campo de las redes sociales, y un mejor anzuelo en el mundo de las plataformas móviles.

En consecuencia, “*Instagram* actualizó sus términos de privacidad y condiciones de uso, otorgándose así el derecho a vender las fotos de los usuarios a terceros sin notificación o compensación a partir de enero de 2013. La crítica de los defensores de la privacidad, los consumidores, *National Geographic* y usuarios reconocidos llevó a *Instagram* a deshacer los cambios impuestos en la declaración de los términos de privacidad. Aun así, *Instagram* perdió gran parte de usuarios, que optaron por cambiarse a otros servicios similares a *Instagram*.¹⁷”

3.3.1. Privacidad de datos personales

Facebook ha enfrentado el mayor obstáculo de su historia en marzo de 2018, cuando el caso de *Cambridge Analytica*, la firma británica que se hizo con datos de los usuarios de la red social para utilizarlos luego en campañas de *marketing* político, se supo que afectó a 87 millones de usuarios de dicha red social.

La función principal de dicha compañía es el análisis de datos con la comunicación

¹⁷ Fundación Wikimedia, Inc. <https://es.wikipedia.org/wiki/Instagram>. (Consultado: 15 de marzo de 2018.)

estratégica para la creación de campañas publicitarias y propagandas políticas. En marzo de 2018, reconocidos medios de comunicación evidencian anomalías en cuanto a las políticas de privacidad e información personal de usuarios de *Facebook*, creando anuncios políticos durante las elecciones presidenciales de 2016 en Estados Unidos. A pesar de tener el conocimiento de la violación a la privacidad, *Facebook* omitió tomar acciones en contra de la citada compañía británica.

El problema en cuestión se suscitó en principio como una encuesta, en la cual participaron más de 250000 usuarios, lo cual derivó la recopilación de información de más de 70 millones de perfiles, en virtud que dicha encuesta solicitaba el acceso a los datos de los amigos. La información obtenida fue enviada a *Cambridge Analytica* sin el permiso de los usuarios, violentando así el derecho a la privacidad de datos de usuarios y quebrantando las políticas de privacidad.

La consultora que desempeñó un papel central en el escándalo de la masiva filtración y uso no autorizado de datos personales de *Facebook*, anunció que cierran sus operaciones en virtud de lo anterior. La compañía británica ha estado envuelta en un escándalo desde que, a mediados del pasado mes de marzo de 2018, una investigación periodística de entidades reconocidas a nivel mundial, reveló que datos personales de más 50 millones de estadounidense habían sido obtenidos irregularmente de *Facebook* y utilizados indebidamente para fines electorales.



En la realidad guatemalteca, los *net centers*, son empresas de carácter ilícito considerados como grupos anónimos en redes sociales, que tienen por objeto desprestigiar a personas a cambio de una remuneración. Básicamente, se busca información personal de quien se tenga por objeto difamar o calumniar y fácilmente, con una gran cantidad de cuentas falsas, se crea una tendencia con publicaciones falsas. El contenido es divulgado de forma masiva en el gran número de cuentas que manejan estas empresas.

En ese orden de ideas, el objetivo del *net center*, es crear criterios equivocados, generar desconfianza y desinformar a través del contenido que se publica en las redes sociales. Este tipo de acciones no pueden ser perseguidos penalmente, en virtud, que no pueden encuadrarse en un tipo penal. Es decir, no están reconocidos dentro del ordenamiento jurídico como delitos.

En consecuencia, es importante establecer cuál es el propósito del *net center*. La finalidad de los mismos es manipular la opinión pública mediante contenido que se publica. Básicamente, pueden simular ser un grupo de presión, promocionar una agenda en contra de cierta persona o figura pública, o colocar a un político o particular en las redes sociales con el objeto de dar a conocerlo a la población y así contar con aprobación política y ciudadana.



En Guatemala, las personas que hacen funcionar un net center, en promedio, radica en particulares que no encuentran empleo y que tienen conocimientos avanzados en la utilización de redes sociales. La cantidad que se les ofrece a cambio de la prestación de este servicio oscila entre Q5000.00 a Q6000.00, servicio que es prestado en una oficina o en cualquier lugar de forma organizada para generar contenido tendencioso.

Para comprender el modo de operar de estos grupos, se analiza que cuentan con grandes cantidades de cuentas en todas las redes sociales y tienen múltiples dispositivos móviles con internet para no tener la misma dirección IP, manipulando encuestas en línea, llenando comentarios a favor a personas específicas y en contra de su oposición.

Los *net centers* no solo sirven para fines políticos. Este recurso también ha sido utilizado por el sector privado para defender a sus corporativos o bien para lanzar campañas en contra de la competencia de sus marcas. Existe un vacío legal en cuanto el tema; se puede incurrir en el delito de difamación de acuerdo al Artículo 164 del Código Penal, si la publicación se hace por un medio de divulgación y provoca odio o descrédito, o que menoscabe el honor, la dignidad o el decoro de una persona ante la sociedad.

El Artículo 342 B del Código Penal preceptúa que comete el delito de pánico financiero todo aquel que elabore, divulgue o reproduzca por cualquier medio o sistema de comunicación, información falsa o inexacta que menoscabe la confianza de los clientes, usuarios, depositantes o inversionistas de una institución financiera. Sin embargo, la

identidad de estos sujetos está protegida a través de cuentas falsas, lugares de ubicación que no son reales, generando desconcierto en virtud de no estar regulado de forma adecuada.

3.4. *WhatsApp Inc*

WhatsApp Inc fue fundada en 2009 por Jan Koum y Brian Acton, quienes conjuntamente trabajaron por 20 años en *Yahoo*. *WhatsApp Inc* fue adquirido por la compañía *Facebook* en el 2014, pero continúa operando como una aplicación independiente y enfocada en construir un servicio de mensajería rápido y confiable en cualquier parte del mundo.

En febrero de 2014, Mark Zuckerberg, anunció la compra de la aplicación móvil por un importe total de 19 000 millones de dólares, argumentando que compró la aplicación para incrementar los usuarios en *Facebook*.

Fue en marzo de 2015 cuando se lanzó *WhatsApp Web*, la cual permite utilizar *WhatsApp Inc* en una computadora, sincronizando el teléfono con ella mediante un código QR. Se puede acceder siguiendo las instrucciones en web.whatsapp.com. En 2016, se habilitó el cifrado de extremo a extremo, lo que impide que nadie, ni siquiera la misma empresa, tenga acceso a los contenidos que se envían; solo el emisor y el receptor.

Sin embargo, existen posturas suspicaces, tal es el caso del jurista alemán Thilo Weichert que expresó a través de un comunicado: "*WhatsApp* es una forma insegura de comunicarse y tiene severos problemas de seguridad y privacidad; ambas compañías se han negado a acatar las normativas de seguridad y de privacidad de datos establecidas por la UE y sus usuarios deben saber que están totalmente desprotegidos."¹⁸

La política de privacidad de *WhatsApp Inc*, según sus responsables, consiste en compartir información con otros proveedores de servicio y en usar información personal, ya sean datos de uso, *cookies*, IP, entre otros; con el objetivo de mejorar la calidad del servicio y generar la creación de nuevas características para modernizar la experiencia del usuario.

3.5. Problemática jurídica de las redes sociales en Guatemala

Cualquier persona que decida crear una cuenta dentro de una red social se limita a adherirse a las políticas de privacidad del proveedor de la red social. Siendo requisito indispensable y obligatorio la aceptación de las políticas de privacidad y términos y condiciones.

En virtud de lo anterior, es importante destacar que la mayoría de usuarios desconocen

¹⁸ <http://www.elmundo.es/tecnologia/2014/02/24/530b1a8fca4741c3388b456d.html> (Consultado: 15 de abril de 2018.)



el contenido de dichas normas, que generalmente vulneran derechos fundamentales. Basta un *click* para aceptar y omitir el conocimiento sobre la regulación de la privacidad de datos de los usuarios.

Resulta necesario llevar a cabo una lectura, análisis y un estudio sobre el contenido de los términos y condiciones, políticas de privacidad, como una obligación previa a la apertura de una cuenta en cualquier red social, verificando el cumplimiento de las necesidades del nuevo usuario.

Las plataformas virtuales de las redes sociales permiten al usuario establecer el carácter privado de la cuenta. No obstante, mediante motores de búsqueda, personas ajenas a la red social pueden tener acceso a contenido que ha sido publicado, constituyendo una violación a la privacidad de datos de los usuarios. Tal es el caso de *Cambridge Analytica*, expuesto con anterioridad.





CAPÍTULO IV

4. Aplicaciones con navegación asistida por GPS

El sistema de posicionamiento global es un instrumento útil empleado por una gran cantidad de aplicaciones para diferentes usos. Comúnmente es utilizado en aplicaciones para determinar las rutas y trayectorias de vehículos, para rastreo de automotores, mapas, localización de usuarios, etc. En la telefonía celular se está incluyendo dentro de los equipos un receptor GPS que tiene las mismas funcionalidades y que pueden ser usadas de manera gratuita.

4.1. Sistema de posicionamiento global

Es más conocido por sus siglas en inglés, GPS, *Global Positioning System*. Dicho sistema tiene por objeto determinar la ubicación, posición y latitud, dentro de todo el planeta con precisión, a través de sistemas digitales incrustados a telefonía móvil, vehículos o cualquier dispositivo electrónico con un soporte adecuado.

Para entender el funcionamiento del GPS, se cita a José Manuel Moya que expresa: “El principio de funcionamiento del sistema GPS (*Global Positioning System*) o Sistema de Posicionamiento Global es una constelación de 24 satélites (constituida por 6 planos orbitales con 4 satélites cada uno, inclinados 55° respecto al horizonte) situados en una órbita ICO (20000 km con un período orbital de 12 horas) que transmiten continuamente

información relativo al tiempo, sus órbitas, identificación, etc. De tal manera que los usuarios pueden calcular su posición en tres dimensiones (latitud, longitud y altura), rumbo y velocidad de desplazamiento, mediante un sencillo terminal receptor, en base al tiempo empleado por las señales en viajar desde cada satélite (triangulación) y medida de la desviación de la frecuencia de la señal recibida (medición Doppler). Estos datos pueden ser transmitidos, además, a través de una red GSM a una posición de control.”¹⁹

Es tendencia global integrar tecnología GPS a los dispositivos de telefonía móvil. El uso y masificación del GPS está generalmente extendido en los teléfonos móviles *smartphone*, lo que ha hecho surgir todo un ecosistema de software para este tipo de dispositivos, así como nuevos modelos de negocios que van desde el uso del terminal móvil para la navegación tradicional punto a punto, hasta la prestación de los llamados servicios basados en la localización.

Los servicios de navegación por satélite optimizan las rutas para sus usuarios, teniendo en cuenta los atascos, los accidentes y las obras viales. Este tipo de aplicaciones recopilan los datos desde servicios municipales y desde los informes que los usuarios les hacen llegar. En consecuencia de lo anterior, surgen aplicaciones de uso diario que facilitan la organización y movimiento de las personas diariamente, así como conocer nuevas personas con intereses comunes. Sin embargo, son aplicaciones eminentemente

¹⁹ **Sistemas de telefonía.** Pág. 196.



peligrosas en un país en el que existe un índice alto de delitos contra la vida y el honor de las personas.

El sistema de posicionamiento global, adaptado a un teléfono móvil, funciona enviando señales a antenas de la estación base más cercana. Es decir, el terminal de un teléfono móvil se ubica de una celda a otra para obtener señal. Las estaciones base se encargan de monitorizar la fuerza de señal del móvil. Es por ese motivo, que en sitios más rurales o remotos, las torres de comunicación suelen estar muy separadas y por eso la señal es irregular.

Sin embargo, un teléfono móvil que carece de GPS también puede proporcionar su ubicación, a través de la forma en que se comunica con la red de telefonía en general. Un ordenador o una aplicación en el móvil pueden determinar la localización en función de tres aspectos: la aproximación a la torres de telefonía, por el tiempo que tarda la señal en ir de torre a torre y por la fuerza de la señal recibida.

Si bien existe la concreción del derecho a buscar y recibir información, las plataformas virtuales que ofrecen este tipo de servicios deben hacer rigurosos informes sobre la administración e información de datos de los ciudadanos, ya que a través del sistema de posicionamiento global es permitido conocer la ubicación, lugares que se visitan y rutas que pueden ser concurridas.



El derecho de acceso a la información se constituye como herramienta legal para alcanzar la transparencia de los actos del Estado, también como medio de fiscalización y participación efectiva de todos los sectores de la sociedad sin discriminación. Propiciar y promover el acceso a la información de los sectores más empobrecidos de las sociedades del hemisferio, habilitaría su participación activa e informada sobre el diseño de políticas y medidas públicas que afectan directamente a las personas.

Con una regulación severa del tema en cuestión, puede surgir un afianzamiento del sistema de relaciones democráticas de conformidad con la Constitución Política de la República de Guatemala, así como el ejercicio efectivo de otros derechos y libertades.

La comercialización y uso de los dispositivos con Sistema de Posicionamiento Global, están incluidos en los teléfonos móviles de alta gama con funciones de navegación. Con el objeto de prevenir incidentes se hacen estas recomendaciones:

- a. No programar el navegador mientras se conduce. Establecer las rutas sin estar en marcha;
- b. Para la obtención de información de ruta, activar el sistema por voz con el objeto de reducir el riesgo por distracción provocado por observar la pantalla.
- c. Utilizar un sistema que permita introducir los datos de la ruta mediante la voz, para



evitar modificar el GPS durante la marcha;

d. Seleccionar los caracteres más claros y sencillos de entender.

4.2. Waze

En principio el servicio fue llamado *Linqmap*, dicha compañía fue creada en 2008 en Israel por Uri Levine, Ehud Shabtai y Amir Shinar. Considerado como uno de los grandes éxitos que produjo la industria tecnológica en los últimos años, en 2013 fue comprada por *Google* por la cantidad de US\$1.300 millones.

Es una aplicación social de tránsito automotor en tiempo real y navegación asistida por GPS desarrollada por *Waze mobile*. Una de sus fuentes principales son los reportes que realizan los usuarios en tiempo real sobre el tránsito en las rutas. Así mismo, permite que usuarios etiqueten las ubicaciones de vehículos de policía aparcados, accidentes, congestión, cámaras de tráfico, cuevas y más; funciona como una red social de conductores que se apoyan mutuamente al emplear la herramienta, alertando cuando hay embotellamientos, accidentes y bloqueos, y compartiendo rutas alternas.

Actualmente, existen más de 200 millones de usuarios de *Waze* alrededor del mundo, y cuando se vendió la empresa había 60 millones. Un estudio publicado por Jaramillo, en *Estrategia y Negocios* indica que “en Guatemala, *Waze* empezó a finales de 2009; en la

actualidad aproximadamente tiene 800.000 usuarios.”²⁰

En consecuencia, la problemática jurídica que atañe, se centra en la vigilancia de movimientos de los usuarios. Así mismo, el riesgo inminente que existe de distracciones en virtud de los íconos y notificaciones que la aplicación genera. Una de las funciones de dicha aplicación consiste en dar aviso de dónde existen retenes policiales, esta función ha generado controversia y opiniones divididas porque elimina el factor sorpresa por parte del cuerpo policial.

Los ciberdelincuentes, a través de dicha aplicación, pueden tener acceso al historial de lugares frecuentados, rutas diarias y concurridas. La raíz de esta peligrosa vulnerabilidad está en las comunicaciones entre los servidores de *Waze* y la aplicación en el móvil. Dichos servidores utilizan una conexión cifrada SSL como medida de seguridad, sin embargo el equipo de investigación de la Universidad de California descubrió que podían hacer que el móvil aceptara un ordenador como puente de conexión entre la aplicación y el servidor de *Waze*.

En virtud de lo anterior, el protocolo de seguridad de *Waze* fue descifrado, por lo tanto la interacción del usuario y la aplicación fue visible. Es una aplicación de uso común que tiende a facilitar la comisión de hechos delictivos para los ciberdelincuentes, en caso se

²⁰ <http://www.estrategiaynegocios.net/lasclavesdeldia/913286-330/la-historia-de-waze-contada-por-uri-levine>. (Consultado: 15 de abril de 2018.)

establezcan puentes de conexión entre los dispositivos y la aplicación. Es importante mencionar que *Waze*, dentro de sus ajustes, permite a los usuarios colocar el modo invisible, con la salvedad que dicho ajuste deberá activarse cada vez que se inicie sesión.

Sin embargo, el uso de esta aplicación genera un gran riesgo en la integridad de los conductores, en virtud de las distracciones que genera. El Sistema de Posicionamiento Global es un elemento de distracción utilizando un vehículo al mismo tiempo; cuando el conductor manipula la pantalla durante la marcha del vehículo, se convierte en una acción peligrosa.

4.3. *Tinder*

Sus inicios se remontan al 2012, sus creadores son Sean Rad, Justin Mateen, Jonathan Badeen y Ramón Denia. *Tinder* es una red social con asistencia de sistema de posicionamiento global que permite a los usuarios conocer a otros usuarios en base a una relación de preferencias en común para conversar, concretar citas o encuentros.

En principio, se debe registrar e iniciar sesión. Luego, *Tinder* proporciona una lista de usuarios en forma aleatoria o bien con las preferencias en base a intereses personales que se han ajustado en la cuenta. Existe un ajuste relacionado a la distancia que hay entre usuarios de dicha red social. Este, consiste en activar un rango de distancia que directamente presenta a los usuarios que estén dentro de ese perímetro.

De conformidad con las políticas de privacidad, términos y condiciones de *Tinder*, se establece que “Podremos recopilar Información personal, incluyendo Datos sensibles, y otra información. “Información personal” se entiende como información identificable a nivel individual que nos permitiría determinar la identidad real de una persona en concreto y contactar con ella. El término Datos sensibles incluye información, comentarios o contenido (p. ej.: fotografías, vídeos, perfil, estilo de vida) que usted proporcione de forma opcional y que pueda revelar su origen étnico, nacionalidad, religión y/u orientación sexual. Al proporcionarnos Datos sensibles, consiente en la recopilación, uso y divulgación de dichos Datos sensibles en la medida en la que las leyes de privacidad pertinentes lo permitan. También podremos recopilar información de su geolocalización con su consentimiento. Podremos recopilar esta información a través de la página web, de la aplicación móvil o de otros servicios en línea. Al hacer uso del Servicio, nos autoriza a reunir, analizar y conservar datos relacionados con la proporción del Servicio. Cuando proporciona información personal a través del Servicio, la información puede enviarse a servidores situados en los Estados Unidos y en otros países del mundo.”²¹

Como en todas las redes sociales, existen perfiles falsos que generan de forma automática interacción con otras cuentas. *Tinder* no está libre de riesgos, razón por la cual, han existido campañas con la finalidad de advertir sobre el *spam* de *webcam* para

²¹ <https://www.gotinder.com/privacy?locale=es>. (Consultado: 20 de marzo de 2018.)

adultos, así como también sobre el aumento de *bots* de *spam* una vez que la versión de *Android* fue liberada.

Un *bot* hace referencia a un programa informático que imita el comportamiento humano, haciendo creer al interlocutor que está chateando con una persona real. En *Tinder*, los ciberdelincuentes logran esto a través de perfiles falsos que envían *spam*. Cuando un usuario indica que le gusta uno de estos perfiles falsos, puede comenzar a chatear con esa persona, y ahí es cuando el *bot* ofrece, por ejemplo, sesiones de *webcam* para adultos pidiendo al usuario que haga *click* en un enlace que lo llevará a un sitio *web*. Una vez allí, se le solicita al usuario que ingrese sus datos personales y una tarjeta de crédito para poder acceder a la sesión de *webcam* y verificar su mayoría de edad.

Anteriormente se estableció que *Tinder* es mayormente usada para acordar reuniones sin mayor compromiso, las cuales generalmente terminan en un encuentro sexual. Dicha aplicación únicamente señala que es un medio facilitador para el contacto entre dos personas y hace recaer la responsabilidad de las citas sobre sus usuarios.

Esto es lo que señalan los términos de servicio de la compañía al respecto, excluyendo cualquier tipo de responsabilidad "Usted es el único responsable de sus interacciones con otros usuarios. Usted entiende que *Tinder* no verifica los antecedentes penales de los usuarios ni investiga de otro modo los antecedentes de sus usuarios. *Tinder* no hace declaraciones ni ofrece garantías en cuanto al comportamiento de los usuarios. *Tinder*

se reserva el derecho de llevar a cabo cualquier verificación de antecedentes penales u otras indagaciones (tales como búsquedas en registros de delincuentes sexuales) en cualquier momento utilizando los registros públicos disponibles.”²²

Sin embargo, *Tinder* es una red social que utiliza el sistema de posicionamiento global como una de sus principales características. En virtud de ello, existe un caso concreto que vulneró la privacidad e intimidad de los usuarios de dicha red. El problema en cuestión versó en que la localización de los usuarios era visible sin el consentimiento de los mismos, situación que hace vulnerable a cualquier persona de sufrir ataques, daños a su persona y a los bienes jurídicos tutelados.

En virtud de lo anterior, los ingenieros informáticos Pratllusà y Martínez pusieron en evidencia la gravedad de la vulnerabilidad: “El ingeniero informático Marc Pratllusà no podía ocultar la sorpresa cuando descubrió que esta aplicación le estaba dando las coordenadas exactas de donde se encontraba Oriol Martínez, también ingeniero informático especializado en seguridad. Pratllusà, experto en programación, no es hacker y ni siquiera necesitó entrar a los servidores de *Tinder* para conseguir esa información: fue más sencillo que todo eso. Un error en el diseño de la aplicación permitía conocer la latitud y longitud en la que se encontraban cada una de las personas con las que habías conectado a través de la aplicación.”²³

²² Tinder. <https://www.gotinder.com/terms>. (Consultado: 20 de marzo de 2018.)

²³ https://elpais.com/tecnologia/2016/08/23/actualidad/1471953934_487766.html?rel=mas. (Consultado: 20 de marzo de 2018.)

Tinder ignoró el fallo durante tiempo desconocido y luego de la publicación hecha por ambos informáticos corrigió el error. La localización se actualizaba cada vez que el usuario abría la aplicación en un lugar distinto, es decir, había que estar en un lugar diferente por lo menos 2 kilómetros de distancia como mínimo para que apareciera una nueva.

4.4. *Google Maps*

Es de importancia establecer que *Google Maps* no es considerada una red social. Sin embargo, esta aplicación es asistida por GPS y la privacidad se ve afectada en virtud del espionaje que puede hacer cualquier persona que ingrese a esta plataforma virtual.

Es considerada como una plataforma con asistencia del sistema de posicionamiento global, a través del satélite que permite introducir una dirección y proporciona la ubicación exacta, así como las rutas disponibles para llegar a ellas. Lo que en un principio surge a modo de GPS de localización, ha terminado convirtiéndose en una red social más con la que se pueden elaborar mapas de información, combina geolocalización con diversas fuentes de información por medio de hiperenlaces, fotos y texto, sin el consentimiento de las personas.



En sus inicios, *Google maps* podía utilizarse únicamente en los servidores de *Internet Explorer* y *Mozilla Firefox*. El usuario puede mover el mapa, y la visualización del mismo es descargada desde el servidor. Es considerado como un servidor de aplicaciones de mapas en la web, así como fotografías por satélite del mundo e incluso la ruta entre diferentes ubicaciones o imágenes a pie de calle con *google street view*.

Atendiendo al estudio publicado por crhoy, “en 2014, los documentos filtrados por Edward Snowden revelaron que *Google Maps* es parte y víctima del entramado de vigilancia mundial operado por varias agencias de inteligencia occidentales y empresas tecnológicas.”²⁴

Google Maps ofrece la capacidad de realizar acercamientos y alejamientos para mostrar el mapa. Los usuarios pueden ingresar una dirección, una intersección o un área en general para buscar en el mapa. El usuario puede controlar el mapa con el mouse o las teclas de dirección para moverse a la ubicación que se desee.

En consecuencia, la privacidad e intimidad de las personas se ve afectada debido a la facilidad de espionaje que cualquier persona pueda hacer a través de esta aplicación. Incluso personas que no tienen acceso a internet, y que, sin consentimiento son publicadas imágenes de sus inmuebles. Sin embargo, dentro de los ajustes que ofrece

²⁴ <https://www.crhoy.com/noticias-sobre/google-maps>. (Consultado: 20 de abril de 2018.)



Google Maps, permite difuminar lugares. No basta un *click* para llevar a cabo el mismo, el primer paso es la opción informar de un problema; luego, se debe completar un formulario con el objeto de borrar el lugar que se desea; después, es necesario introducir un correo electrónico para terminar la solicitud. *Google* analiza la solicitud y después de un tiempo, confirma a través de un correo electrónico si ha eliminado o no el lugar solicitado.

En consecuencia, se convierte en forma de integración y reutilización de búsqueda en el momento en el que se utiliza con otros fines, como los de una red social. *Google Maps* incluso permite esta característica a través de la opción *about* donde indica los usos que puedes hacer a través de ello.





CAPÍTULO V

5. Vulneración en el uso de datos personales en redes sociales y aplicaciones con navegación asistida por GPS

Alan Westin, planteó que “la privacidad es el derecho autónomo de los individuos, grupos o instituciones a determinar por si mismos cuándo, cómo y en qué medida se comunica a otros información sobre ellos.”²⁵ En la cultura jurídica hay una perspectiva que ve en lo íntimo y lo privado una manifestación de la propiedad, pero en los tiempos del capitalismo informacional no solo se abarca la propiedad física o la propiedad privada sino la propiedad intelectual, esto quiere decir que al emerger nuevas formas normativas la privacidad como derecho se ha complejizado. La privacidad sobre datos e información representa también en estos tiempos: propiedad intelectual.

Los sitio de redes sociales han sido construidos como sistemas que obtienen la información que circula en su plataforma, incluso aquella que los usuarios creen ficticiamente que no es visible para otros usuarios cuando ajustan sus respectivas configuraciones de privacidad, sin tomar en cuenta que pese a ello la empresa puede verlo todo. Inclusive la opción de configuración de privacidad que adoptan más la

²⁵ *Privacy and freedom*. Pág. 7



información recopilada en las diferentes redes sociales, con la que complementa nuestros perfiles, logrando conocernos mejor que a nosotros mismos.

5.1. Datos personales sensibles

Es importante destacar que dentro de la Ley de Libre Acceso a la Información Pública regula, además de lo relativo a la información pública, en su Artículo 9 los datos personales delimitan a los relativos a cualquier información concerniente a personas naturales identificadas o identificables; en el mismo Artículo, numeral segundo, se define a los datos personales sensibles como “aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o actividad, tales como los hábitos personales, de origen racial, el origen étnico, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos, preferencia o vida sexual, situación moral y familiar y otras cuestiones íntimas de similar naturaleza.”

Los datos personales constituyen todas las referencias que tienen por objeto identificar e individualizar el nombre, edad, estado civil, domicilio, impresión dactilar, entre otros; incluso, aspectos del área laboral, privada, patrimonial, académica, ideológica, historial crediticio, características personales y físicas, intereses y actividades, hábitos sexuales y origen. La protección jurídica de los datos personales ha ido en ascenso en las últimas décadas y países potencias muestran aceptación en la regulación de nuevas medidas.



Los datos personales comprenden un activo fundamental que al igual que las instalaciones, capital humano y recursos financieros; debe protegerse mediante un conjunto coherente de procesos y sistemas diseñados, administrados y mantenidos por las propias organizaciones del sector privado.

Además, existe una preocupación adicional, ya que muchas personas utilizan una misma contraseña en varias plataformas virtuales que ofrecen servicios de redes sociales, así que quien tenga los datos podría usar la información para acceder a *Gmail*, *Amazon*, *PayPal* y otras cuentas, llevando a cabo actos ilícitos en perjuicio de los usuarios.

Existen principios fundamentales para la protección de los datos personales, los cuales sirven de fundamento al derecho de intimidad de los seres humanos; en torno al tratamiento que reciben por parte de la administración pública, y en determinados casos de las empresas que prestan servicios de comunicación digitales, entre los cuales destacan:

- a. Principio de limitación de objetivos: Que se refiere al trato que se le debe de brindar a la información privada o datos personales; es decir, si van a utilizarse el objetivo no debe variar.
- b. Principio de proporcionalidad y de calidad: La información personal debe ser exacta y mantenerse actualizada.

- c. Principio de transparencia: Consistente en que se le debe informar a los dueños de los datos sensibles el trato y el objetivo por el cual se va a transferir la información.

- d. Principio de seguridad: Al momento de realizar, transferir o utilizar los datos personales, se debe responsabilizar el posible riesgo que involucre esa medida.

La intimidad y la privacidad son temas de relevancia cuando se analiza lo relativo a los sitios de redes sociales, pues son tópicos sensibles en la era de la información. Cada servicio de red social cuenta con sus particularidades en cuanto a la privacidad de sus usuarios, especialmente de los datos personales que divulgan en sus perfiles.

Los riesgos potenciales que representan las nuevas tecnologías de la información hacia los derechos de las personas, específicamente con relación al uso y comercialización de la información obtenida sin consentimiento, dan origen a un nuevo derecho fundamental concerniente a la protección de datos personales.

El derecho a la protección de datos personales comprende la facultad que se otorga al titular de poder decidir y controlar qué datos proporciona a un tercero, así como tener pleno conocimiento sobre quien posee dichos datos y con qué finalidad, teniendo la facultad de oponerse a dicha posesión o uso. En consecuencia, puede determinarse que

es el derecho que tiene toda persona a conocer y decidir, quién, cómo y de qué manera recaba, utiliza y comparte sus datos personales.

Sin embargo, la esfera íntima de los usuarios de redes sociales puede ser vulnerada en sus datos personales. Es por esta razón que, la protección de la información personal se ha separado del derecho a la intimidad, hasta convertirse expresamente en un derecho fundamental con un contenido independiente.

5.2. Legislación extranjera sobre la protección de datos personales

- a. La Resolución 509 del Consejo de Europa, en el año 1967, tiene por objeto estudiar la agresividad que genera las tecnologías de información hacia los derechos y libertades de las personas.
- b. Las Directrices de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), que hace referencia a los principios básicos aplicables al tratamiento de datos personales y a la vez garantiza la libre circulación de los mismos.
- c. El Convenio 108 del Consejo de Europa, que tiene por objeto garantizar a los ciudadanos de los Estados contratantes el respeto de sus derechos y libertades, en



particular, el derecho a la vida privada frente a los tratamientos de datos personales, conciliando el libre flujo de información entre los Estados contratantes.

- d. La Resolución 45 – 95 de la Asamblea General de la Organización de las Naciones Unidas, la cual enumera un conjunto de principios en materia de protección de datos personales de aplicación global.
- e. La Directiva 95 – 46 – CE, que tiene por objeto acrecentar los principios establecidos en otros instrumentos internacionales e impide la creación de obstáculos para la libre circulación de datos personales en todos los estados miembros de la Unión Europea.
- f. El Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico (APEC), que tiende a conseguir un equilibrio entre la seguridad de la información personal y el libre flujo de ésta para fines comerciales.
- g. La Carta de Derechos Fundamentales de la Unión Europea, en su Artículo 8, reconoce el derecho a la protección de datos como un derecho fundamental y autónomo, diferente al derecho de intimidad y la privacidad de las personas, permitiendo desligar uno de otro, otorgándole la exclusividad y reconociendo la importancia del mismo.

- h. Las Directrices para la Armonización de la regulación de la Protección de Datos en la Comunidad Iberoamericana, que ofrece a los poderes públicos de los Estados Iberoamericanos criterios orientados para el desarrollo de iniciativas normativas en dicha materia, facilitando establecer un marco similar que favorezca el intercambio de los flujos de información entre los Estados y terceros Estados bajo estándares similares de protección.

- i. Los Estándares Internacionales sobre la protección de datos personales y privacidad. Resolución de Madrid, la cual, determina, establece y define el conjunto de principios y derechos que garantizan de forma efectiva y uniforme la protección de datos personales, facilitando los flujos internacionales de éstos en un mundo globalizado.

5.3 Propuesta de reforma al Código Penal Decreto Número 17-73

El Decreto 17-73 Código Penal regula en el Libro Segundo los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos establece una protección leve de la privacidad de datos personales de usuarios de redes sociales, así mismo en el acceso a la información no autorizada, situándolas como nuevas modalidades de delitos informáticos que operan a través de las redes sociales. En ese orden de ideas, se propone el siguiente proyecto de reforma al Decreto Número 17-73.



EL CONGRESO DE LA REPÚBLICA DE GUATEMALA

DECRETO NÚMERO 21-2018

CONSIDERANDO:

Que la Constitución Política de la República de Guatemala, en su artículo 24 establece dentro de la inviolabilidad de correspondencia, documentos y libros abarca productos de la tecnología moderna protegiendo así datos personales de usuarios de nuevas tecnologías.

CONSIDERANDO:

Que atendiendo a la realidad nacional y contemplando el constante avance de la ciencia, el desarrollo de la Internet en los últimos años, es imperante la tipificación de nuevas figuras dentro de la legislación penal guatemalteca.

CONSIDERANDO:

Que el Derecho Penal es un derecho realista y objetivo, debe estudiar al futuro delito en su realidad social y debe resolver los casos determinados en base a la equidad, es indispensable enfocar ante todo la posición económica, social y cultural de los tipos penales, previendo y resolviendo los diversos problemas que con motivo de su aplicación surjan, con criterio social y a base de hechos concretos y tangibles.



POR TANTO:

En ejercicio de las atribuciones que le confiere el artículo 171 literal a) de la Constitución Política de la República de Guatemala,

DECRETA:

Las siguientes:

**REFORMAS AL DECRETO NÚMERO 17-73 DEL CONGRESO DE LA REPÚBLICA,
CÓDIGO PENAL**

Artículo 1. Se adicionan al artículo 274 “D” el párrafo siguiente, que quedará redactado así:

Artículo 274 D. Registros prohibidos. Se impondrá prisión de seis meses a cuatro años y multa de doscientos a mil quetzales, al que creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas. “La sanción establecida en el párrafo anterior se aumentará en una tercera parte si el autor utiliza, para crear un banco de datos, como medio principal las redes sociales afectando la privacidad de los usuarios.”

Artículo 2. Se reforma el artículo 274 “F”, el cual queda así:

“Artículo 274 “F”. Uso de información. Se impondrá prisión de seis meses a dos años, y multa de veinte mil quetzales a setenta y cinco mil quetzales al que, sin autorización haga uso indebido de registros informáticos, recopilación de datos personales sensibles



a través de redes sociales o aplicaciones similares para la creación de un banco de datos o archivos electrónicos.”

Artículo 3. Se adiciona el artículo “274 J”, el cual queda así:

Artículo 274 “J”. Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de dos a cuatro años y multa de veinticinco mil quetzales.

Artículo 4. El presente decreto entrará en vigencia el día siguiente de su publicación íntegra en el Diario Oficial.

REMÍTASE AL ORGANISMO EJECUTIVO PARA SU SANCIÓN, PROMULGACIÓN Y PUBLICACIÓN.

DADO EN EL PALACIO DEL ORGANISMO LEGISLATIVO EN LA CIUDAD DE GUATEMALA EL QUINCE DE ABRIL DE DOS MIL DIECIOCHO.



CONCLUSIÓN DISCURSIVA

La sociedad se mantiene en cambio constante, así también el derecho de privacidad e intimidad de datos personales en virtud de las nuevas tecnologías y sistemas informáticos. En consecuencia, los parámetros necesarios para legislar esta área son mayores y la legislación vigente resulta insuficiente. Es decir, la sociedad guatemalteca está viviendo una realidad que necesita nuevas normas jurídicas.

Por lo tanto, es urgente que sean implementados mecanismos que eviten la vulneración de la privacidad de datos personales de los usuarios de redes sociales por parte del Congreso de la República de Guatemala tales como la creación de cuerpos normativos, reformas al Código Penal en lo referente a delitos informáticos, así mismo extender el alcance jurídico del Hábeas Data adaptándolo a la realidad social de modo que abarque los sistemas informáticos que crean bases de datos con información privada de usuarios de redes sociales con la finalidad de garantizar el resguardo de los datos personales.





BIBLIOGRAFÍA

BARRIO ANDRÉS, Moises. **Ciberdelitos: amenazas criminales del ciberespacio.** España: REUS, 2017.

BARRIOS OSORIO, Omar Ricardo. **Derecho e informática: aspectos fundamentales.** Guatemala: Mayté, 2007.

CAJAL, Mabel. <https://www.mabelcajal.com/2017/06/que-es-una-red-social-tipos-redes-sociales-para-que-sirven.html/> (Consultado: 30 de enero de 2018).

Fundación Wikimedia, Inc. <https://es.wikipedia.org/wiki/Instagram>. (Consultado: 15 de marzo de 2018.)

<https://www.crhoy.com/noticias-sobre/google-maps>. (Consultado: 20 de abril de 2018.)

<http://www.elmundo.es/tecnologia/2014/02/24/530b1a8fca4741c3388b456d.html/> (Consultado: 15 de abril de 2018.)

<http://www.estrategiaynegocios.net/lasclavesdeldia/913286-330/la-historia-de-waze-contada-por-uri-levine> (Consultado: 15 de abril de 2018.)

https://elpais.com/tecnologia/2016/08/23/actualidad/1471953934_487766.html?rel=mas. (Consultado: 20 de marzo de 2018.)

<http://gtmtecono.com/2016/07/28/estudio-guatemalteco-redes-sociales/>. (Consultado: 11 de abril de 2018.)

LEINER, Barry. <https://www.internetsociety.org/es/breve-historia-de-internet/> (Consultado: 10 de enero de 2018.)

MOYA, José Manuel. **Sistemas de telefonía.** España: Editorial Paraninfo, S.A., 2006.



PALOMARES, Francisco. **Resolución de averías lógicas en equipos microinformáticos**. España: Editorial CEP, S.I., 2016.

SÁNCHEZ, Elia. <https://laventanadeelia.wordpress.com/2011/09/27/redes-sociales-verticales-y-horizontales/> (Consultado: 30 de enero de 2018).

SANZ DE ACEDO, Etienne. **Marcas renombradas y nombres de dominio en internet: en torno a la ciberpiratería**. España: Editorial Civitas, 2001.

SUÁREZ CABALLERO, Ricardo. <https://iiemd.com/articulo/facebook/que-es-como-funciona-facebook-entrar-2>. (Consultado: 5 de febrero de 2018.)

TINDER, <https://www.gotinder.com/privacy?locale=es> (Consultado: 20 de marzo de 2018).

TINDER, <https://www.gotinder.com/terms> (Consultado: 20 de marzo de 2018).

TORRES, Tiberio. **La protección de la intimidad en el derecho tributario**. Ecuador: Editorial Abya Yala, 2007.

TREJO DELARBRE, Raúl. **La nueva alfombra mágica. Usos y mitos de internet, las redes sociales**. México: Editorial Diana, 1996.

Varios Autores. **Redes sociales: infancia, familia y comunidad**. Colombia: Ediciones Uninorte, 2012.

VILLEGAS LARA, René Arturo. **Derecho mercantil III**. Guatemala: Editorial USAC, 2004.

WESTIN, Alan. **Privacy and freedom**. Estados Unidos: Editorial IG PUB, 2015.



Legislación:

Constitución Política de la República de Guatemala. Asamblea Nacional Constituyente, 1986.

Ley de Emisión del Pensamiento. Decreto Número 9 de la Asamblea Nacional Constituyente de la República de Guatemala, 1966.

Código Penal, Decreto 17-73 del Congreso de la República de Guatemala, 1973.

Ley de Acceso a la Información Pública. Decreto Número 57-2008 del Congreso de la República de Guatemala, 2009.