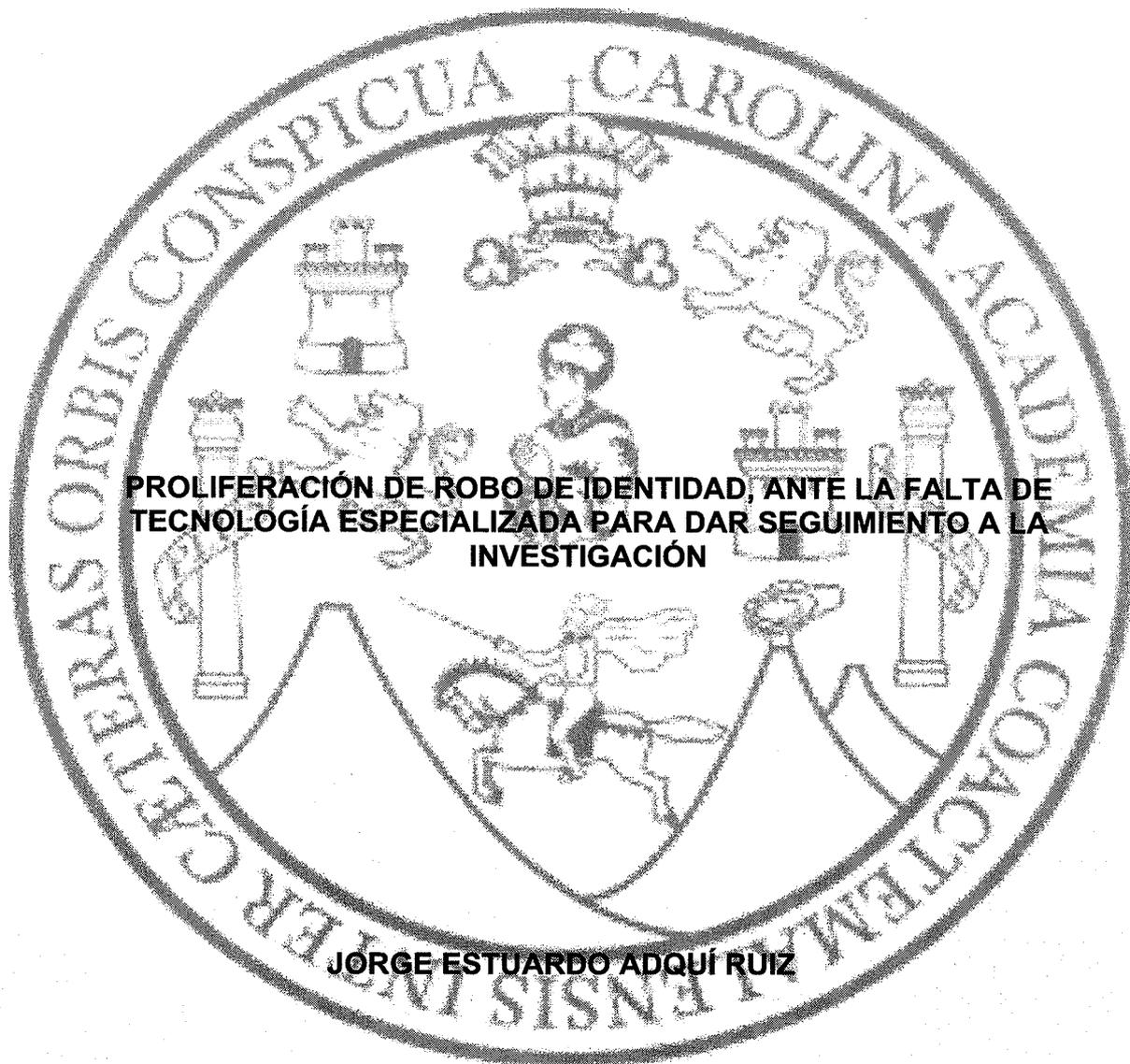


**UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES**



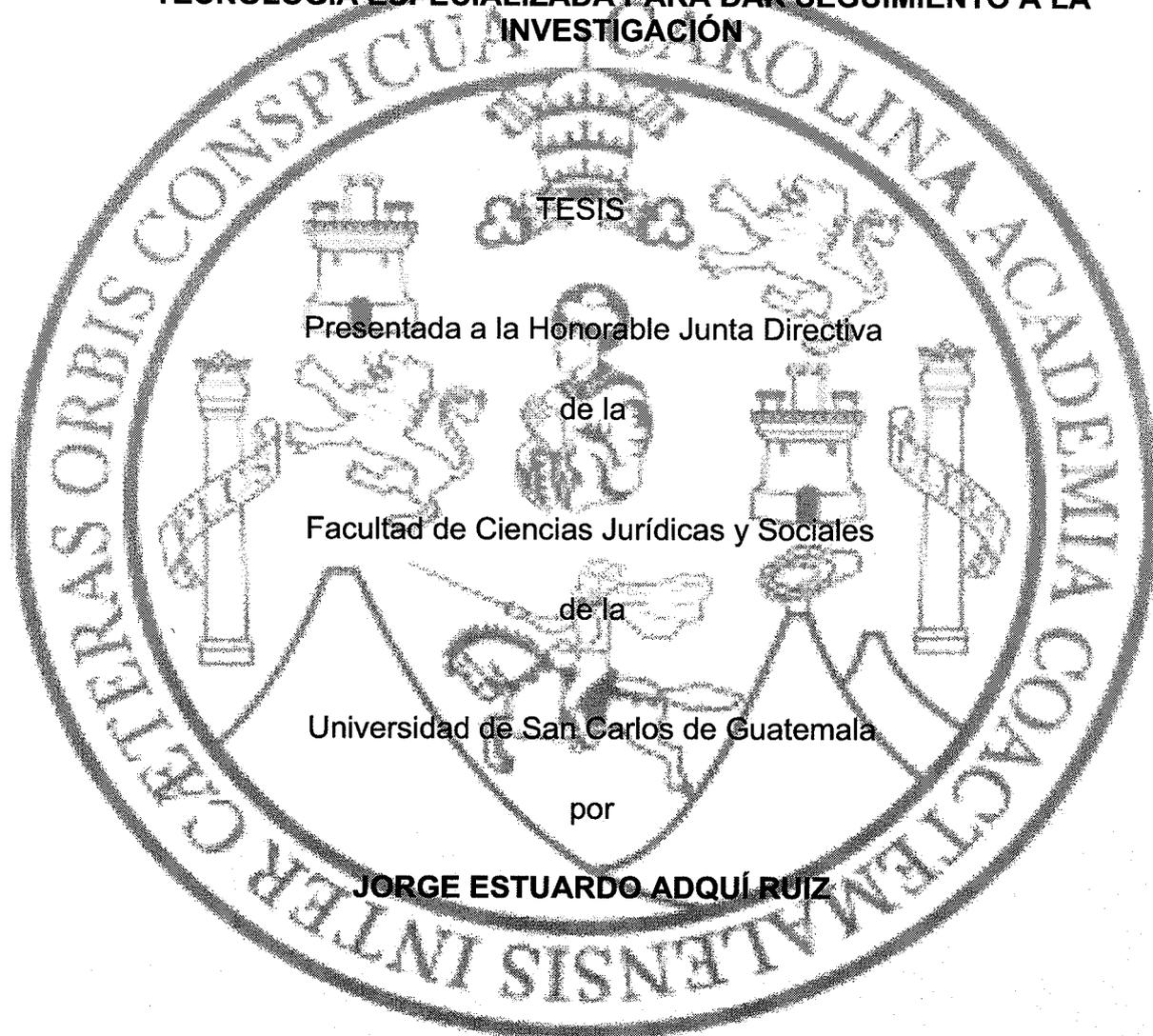
**PROLIFERACIÓN DE ROBO DE IDENTIDAD, ANTE LA FALTA DE
TECNOLOGÍA ESPECIALIZADA PARA DAR SEGUIMIENTO A LA
INVESTIGACIÓN**

JORGE ESTUARDO ADQUÍ RUIZ

GUATEMALA, MARZO DE 2023

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

**PROLIFERACIÓN DE ROBO DE IDENTIDAD, ANTE LA FALTA DE
TECNOLOGÍA ESPECIALIZADA PARA DAR SEGUIMIENTO A LA
INVESTIGACIÓN**



TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

por

JORGE ESTUARDO ADQUÍ RUIZ

Previo a conferírsele el grado académico de

LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

Guatemala, marzo de 2023

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

DECANO:	M.Sc.	Henry Manuel Arriaga Contreras
VOCAL I:	Licda.	Astrid Jeannette Lemus Rodríguez
VOCAL II:	Lic.	Rodolfo Barahona Jácome
VOCAL III:	Lic.	Helmer Rolando Reyes García
VOCAL IV:	Br.	Javier Eduardo Sarmiento Cabrera
VOCAL V:	Br.	Gustavo Adolfo Oroxom Aguilar
SECRETARIA:	Licda.	Evelyn Johanna Chevez Juárez

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 Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público).



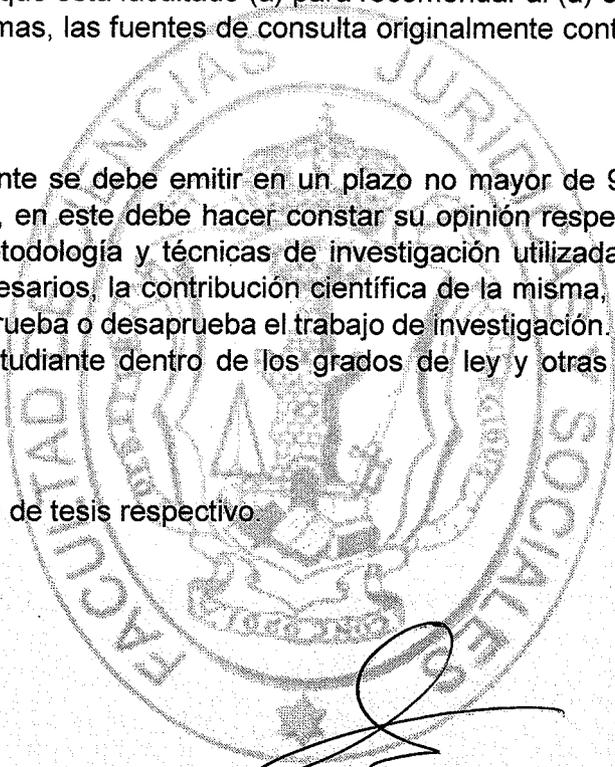
**Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala,
 10 de agosto de 2022**

Atentamente pase al (a) Profesional, **ROLANDO NECH PATZAN**, para que proceda a asesorar el trabajo de tesis del (a) estudiante **JORGE ESTUARDO ADQUÍ RUIZ**, con carné 201211936, intitulado: **PROLIFERACIÓN DE ROBO DE IDENTIDAD, ANTE LA FALTA DE TECNOLOGÍA ESPECIALIZADA PARA DAR SEGUIMIENTO A LA INVESTIGACIÓN.**

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.



CARLOS EBERTITO HERRERA REGINOS
 Jefe (a) de la Unidad de Asesoría de Tesis

SAQO

(Handwritten signature of Rolando Nech Patzan)

Licenciado
Rolando Nech Patzan
 Abogado y Notario

Fecha de recepción 16 / 08 / 2022

(f)

Asesor(a)
(Firma y sello)





Licenciado Rolando Nech Patzan
Abogado y Notario
Colegiado: No. 19527
12 calle 2-25, zona 1.
Teléfono No: 5132-7557.
Correo Electrónico: rolandonech@yahoo.com

Guatemala, 27 de septiembre de 2022

Dr. Carlos Ebertito Herrera Recinos
Jefe de Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala



Distinguido Dr. Herrera Recinos:

Atentamente me dirijo a usted para darle cumplimiento a la providencia de fecha diez de agosto de dos mil veintidós, por medio de la cual fui nombrado ASESOR de tesis del bachiller JORGE ESTUARDO ADQUÍ RUIZ, titulada: "PROLIFERACIÓN DE ROBO DE IDENTIDAD, ANTE LA FALTA DE TECNOLOGÍA ESPECIALIZADA PARA DAR SEGUIMIENTO A LA INVESTIGACIÓN".

En cumplimiento de esta designación, he brindado la orientación requerida y se ha asesorado el tema con la debida acuciosidad, dando como resultado que: el desarrollo del trabajo de tesis, denota una investigación y estudios completos, su contenido científico y técnico de tesis, cumple con los requisitos del método científico de las ciencias sociales; a través de éste, se hacen observaciones; en cuanto a las técnicas empleadas, éstas tienen como objetivo exponer propuestas que se realizaron para llegar a resolver el problema a través de los pasos establecidos previamente, utilizando la recolección de datos, tales como: libros, diccionarios, la exposición de doctrina en páginas Web y ejerciendo el cronograma de actividades planteado en el plan de investigación.

La metodología y las técnicas de investigación que se han utilizado, se desarrollaron a través de un análisis crítico y descriptivo del contenido de la presente tesis y la realización de síntesis y deducciones para generar la conclusión discursiva; de manera que se utilizó el análisis de diversas leyes, doctrinas y la información de páginas de internet, que se relacionan con el tema investigado; todo ello, con el fin de llegar a la conclusión discursiva de que se deben buscar soluciones al problema señalado.

La redacción utilizada por el estudiante, es la correcta; apeguándose a los requisitos de las normas mínimas establecidas en el Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales, y del Examen General Público.

La contribución científica de las ciencias sociales, son las normas, principios, fuentes y doctrinas; en donde el bachiller hace sus propias aportaciones, para comprobar y llegar a



Licenciado Rolando Nech Patzan
Abogado y Notario
Colegiado: No. 19527
12 calle 2-25, zona 1.
Teléfono No: 5132-7557.

Correo Electrónico: rolandonech@yahoo.com

cumplir con los objetivos planteados. La conclusión discursiva, resume los resultados obtenidos y sugerencias; en la cual se da la importancia del estudio sobre algo tan valioso como lo es la solución al problema; dándole la consideración que amerita al ser estudiada, haciendo notar la necesidad de que se controle el problema señalado. La bibliografía consultada se extrajo de fuentes de autores nacionales e internacionales, así como páginas del internet.

En síntesis, el contenido del trabajo de tesis, se ajusta a las exigencias científicas y técnicas que se deben cumplir, de conformidad con la normativa respectiva; la metodología y técnicas de investigación utilizadas, la redacción, la conclusión discursiva, bibliografía utilizada son congruentes con los temas desarrollados dentro de la investigación.

Indico que, no me une parentesco alguno con el bachiller. En tal virtud emito DICTAMEN FAVORABLE al referido trabajo de tesis, a efecto de que continúe con el trámite respectivo, ya que el estudio desarrollado cumple con los requisitos establecidos en el Artículo 31 del Normativo para la Elaboración de Tesis y de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

Atentamente,

Lic. Rolando Nech Patzan
Colegiado No. 19527

Licenciado
Rolando Nech Patzan
Abogado y Notario

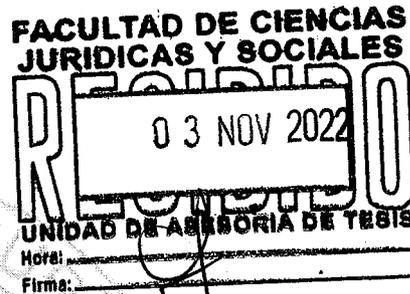


USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala



Guatemala, 03 de noviembre de 2022.

Doctor
Carlos Ebertito Herrera Recinos
Jefe de la Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala.



Estimado Doctor.

De manera atenta, le informo que fui asignado como consejero de redacción y estilo de la tesis titulada: "PROLIFERACIÓN DE ROBO DE IDENTIDAD, ANTE LA FALTA DE TECNOLOGÍA ESPECIALIZADA PARA DAR SEGUIMIENTO A LA INVESTIGACIÓN", realizada por el bachiller JORGE ESTUARDO ADQUÍ RUIZ, para obtener el grado académico de licenciada en Ciencias Jurídicas y Sociales.

El alumno cumplió con todas las observaciones que le hiciera, por lo cual dictamino de manera FAVORABLE, para que el trámite de orden de impresión continúe.

ID Y ENSEÑAD A TODOS

Lic. Roberto Fredy Orellana Martínez
Consejero de Comisión de Estilo





USAC

TRICENTENARIA

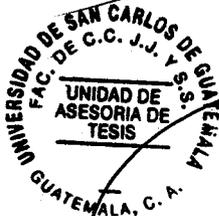
Universidad de San Carlos de Guatemala



Decanatura de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala. Ciudad de Guatemala, diez de marzo de dos mil veintitrés.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis del estudiante JORGE ESTUARDO ADQUÍ RUIZ, titulado PROLIFERACIÓN DE ROBO DE IDENTIDAD, ANTE LA FALTA DE TECNOLOGÍA ESPECIALIZADA PARA DAR SEGUIMIENTO A LA INVESTIGACIÓN. Artículos: 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

CEHR/SAQO





DEDICATORIA

A DIOS:

Por todas las bendiciones que derrama sobre mí y mi familia, por la vida, la salud y la sabiduría brindada para mi superación.

A MIS PADRES:

Víctor Adquí y Carmen Ruíz, quienes me dieron la vida y han sido ejemplo de lucha, quienes han dado todo su esfuerzo para formarme como hombre de bien y quienes me dan su apoyo incondicional, especialmente a ellos dedico todas mis metas cumplidas, especialmente este triunfo.

A MIS HIJOS:

Andrea, Santiago y María José, por ser mi mayor inspiración y el motivo por el que me esfuerzo para salir adelante, a quienes debo el mejor ejemplo y espero que esta meta cumplida les recuerde que pueden cumplir cualquier meta que se propongan en la vida.

A KIMBERLY:

Por ser mi complemento y el respaldo que todo hombre necesita para ser exitoso y vivir en armonía, por acompañarme en todas las circunstancias vividas, buenas y malas, porque esta es una meta más que ganamos juntos para el futuro de nuestro hogar.

A MIS HERMANOS:

Marisabel, Víctor y Yessica por siempre apoyarme, por todos los momentos vividos y compartidos a lo



largo de la vida, por su cariño y sus mejores deseos para mi vida.

A MIS SOBRINOS:

Por su amor y para quienes también es mi deseo ser ejemplo de superación, porque al igual que yo puedan salir adelante y llegar a ser profesionales de éxito.

A MIS AMIGOS:

Todos los que han estado apoyándome moralmente y quienes son parte de mi vida diaria, aconsejándome y motivándome para superarme, especialmente a Brenda Ramos (Q.E.P.D.) y a Marco Antonio Ramos por su cariño y apoyo incondicional.

A:

La Universidad de San Carlos de Guatemala, por abrirme las puertas y permitir que pudiera formarme como profesional.

AL:

Instituto de la Defensa Pública Penal, por ser la institución a quien debo mi formación como persona y también profesional a lo largo de tantos años allí laborados.



PRESENTACIÓN

El derecho a la intimidad o vida privada, es la facultad que la ley le reconoce a una persona para que su vida íntima sea respetada y que sus actos no sean objeto de observación; a efecto de que nadie pueda entrometerse en la existencia ajena, publicando retratos, divulgando secretos, difundiendo correspondencia, mortificando a otro en sus costumbres y perturbando de cualquier otro modo su intimidad; así como robar su identidad para cometer actos fuera de la ley. La intimidad está conformada por aquella parte de nuestra vida que no está consagrada a una actividad pública y que por lo mismo no está destinada a trascender e impactar a la sociedad de manera directa y en donde en principio los terceros no deben tener acceso alguno, toda vez que las actividades que en ella se desarrollan no son de su incumbencia, ni les afectan.

Este estudio corresponde a la rama del derecho cibernético. El período en que se desarrolla la investigación es de mayo de 2021 a marzo de 2022; en la ciudad de Guatemala. Es de tipo cualitativa. El sujeto de estudio es el robo de identidad; asimismo, el objeto la proliferación de robo de identidad ante la falta de herramientas especiales de parte del ente investigador.

Concluyendo con el aporte científico de que, se le debe prestar importancia al robo de identidad, por cuanto las víctimas son dobles, al que se le roba y al que se estafa; asimismo para evitar el daño irreversible que se le causa a estas personas.



HIPÓTESIS

El robo de identidad en Guatemala se refleja en un alto índice de robo de dispositivos móviles o dispositivos electrónicos y con ello la muy probable comercialización, dado que se brinda la oportunidad, de bases de datos, información, fotografías, claves, pines, contactos y una gran cantidad de datos importantes en materia de seguridad, para el usuario del medio electrónico; por lo que es muy fácil robarle la identidad, ante la falta de herramientas de parte del enter investigador, para poder hacerles frente.

Derivado del creciente número de denuncias de incidentes relacionados con el robo de identidad, se requieren métodos adicionales de protección: asimismo que, el ente investigador se provea de tecnología especial para poder combatir a estos delincuentes.



COMPROBACIÓN DE HIPÓTESIS

La hipótesis planteada para esta tesis, fue debidamente comprobada, en el sentido de que, hay falta de herramientas especiales de parte del ente investigador, para poderle hacer frente a los delincuentes, en su mayoría, cibernéticos, que se muestran con robo de identidad; con lo cual engañan a las víctimas, que muchas veces son violadas y asesinadas; en los últimos años se refleja en un alto índice el robo de dispositivos móviles o dispositivos electrónicos y con ello, muy probable comercialización, dado que se brinda la oportunidad, de bases de datos, información, fotografías, claves, pines, contactos y una gran cantidad de datos importantes en materia de seguridad, para el usuario del medio electrónico; por lo que es muy fácil robarle la identidad.

Derivado del creciente número de denuncias de incidentes relacionados con el robo de identidad, se requieren métodos adicionales de protección: asimismo que, el ente investigador se provea de tecnología especial para poder combatir a estos delincuentes. Entre los métodos que se emplearon para la validación de la hipótesis formulada, están: el analítico, el sintético, el deductivo e inductivo y el dialéctico, para la elaboración de razonamientos que sustentaron aspectos científicos y jurídicos; con lo que se pudo ampliar el conocimiento y perspectiva del tema en estudio. Asimismo, fueron de utilidad las técnicas de investigación bibliográfica y documental.

ÍNDICE



Pág.

Introducción.....	i
-------------------	---

CAPÍTULO I

1. Datos personales y derechos humanos	1
1.1. Derecho a la intimidad.....	2
1.2. Derecho a la dignidad	4
1.3. Derecho a la privacidad.....	5
1.4. Datos personales	6
1.5. Datos sensibles.....	10
1.6. Datos crediticios	12
1.7. <i>El habeas data</i>	14

CAPÍTULO II

2. Robo de identidad	19
2.1. Las instituciones del Estado frente al robo de identidad	21
2.2. Instancias del Estado que tienen banco de datos.....	22
2.3. La corrupción.....	23
2.4. Derecho comparado en relación al robo de identidad.....	24
2.4.1. Estados Unidos de América	24
2.4.2. Chile.....	25



2.4.3. Países bajos	26
2.4.4. Delitos informáticos en América Latina	26

CAPÍTULO III

3. Proliferación del robo de identidad, ante la falta de tecnología especializada para la realización de la investigación	29
3.1. Características de la usurpación de estado civil o suplantación de identidad	29
3.2. Alcance de la usurpación de estado civil	30
3.3. Bienes jurídicos protegidos	30
3.4. Protección de datos y derecho a la intimidad.....	32
3.5. Datos de carácter personal	34
3.5.1. Datos personales íntimos	35
3.5.2. Datos personales públicos.....	36
3.6. Los registros o bases de datos computarizados	36
3.7. La justicia ante nuevos retos al darse los avances tecnológicos	38
3.8. Derechos básicos y fundamentales en internet	40
3.8.1. Derecho a la información.....	41
3.8.2. Derecho a la privacidad	42
3.9. Modificación y adaptación de las relaciones jurídicas tradicionales al internet.....	43
3.10. Deslocalización de los derechos y obligaciones en internet	46
3.11. Los derechos fundamentales, la intimidad, el honor y la propia imagen, en las nuevas tecnologías	48
3.12. Riesgos de las nuevas tecnologías y vulneración de derechos fundamentales.....	50
3.13. Protección jurídica de la persona y sus derechos fundamentales, a través de normas legales nacionales e internacionales.....	52



3.14. Desarrollo y masificación de las nuevas tecnologías de la información.....	54
3.15. ¿Qué es robo de identidad? Tips para no caer en esta estafa	56
3.15.1 Diez tips para evitar ser víctima de esta estafa	56
3.16. Robo de identidad: Sacó un préstamo por Q400 mil con documentos falsos pero fue sorprendido y capturado en la zona 10	58
3.16.1. Confirman detención por robo de identidad y estafa	59
CONCLUSIÓN DISCURSIVA	63
BIBLIOGRAFÍA.....	65



INTRODUCCIÓN

Datos personales son toda información sobre una persona física identificada o identificable. Entendiéndose por identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, o fisiológica, psíquica, económica, cultural o social.

El desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos, información personal, mediante los cuales es posible obtener grandes beneficios económicos y causar perjuicios materiales o morales. La diferencia se basa en que es más difícil de descubrir, porque éste tipo singular de delincuentes es capaz de borrar sus huellas del hecho.

En Guatemala, un delincuente de delitos cibernéticos tiene la gran ventaja de que la mayoría de la población no tiene educación sobre cómo mantener seguros sus datos. La ignorancia es la principal aliada del delincuente. Por ejemplo, si a una persona le roban su teléfono celular o dispositivo móvil, pueden tener en un lapso de tiempo, acceso a datos importantes sobre las personas; pines de seguridad, correos electrónicos, estados bancarios o manejo de cuentas bancarias, contraseñas, teléfonos celulares y con este contacto, redes sociales, etc. vulnerando los datos del usuario y éstos pueden ser



vendidos a personas inescrupulosas.

Para que la apropiación del estado civil o identidad configure un delito, debe reunir todas las características o datos que integran la identidad de una persona. Es decir, que para que se configure la usurpación, el usurpador debe poder hacer algo que solo la persona original podría hacer.

Para este informe se plantearon los siguientes objetivos: Como general, evidenciar la falta de herramientas específicas de parte del ente investigador, para hacer frente a delincuentes cibernéticos. Y, como específico: analizar el robo de identidad, así como sus consecuencias para la víctima.

Esta tesis está integrada por tres capítulos, los cuales se detallan a continuación: en el primero, se trató lo referente a los datos personales y los derechos humanos; en el segundo, el robo de identidad; en el tercero, el tema proliferación del robo de identidad, ante la falta de tecnología especializada para la realización de la investigación.

Cabe mencionar que, los métodos utilizados en la elaboración de esta tesis fueron: el analítico, el sintético, el deductivo e inductivo. Las técnicas utilizadas fueron: la documental y las fichas bibliográficas, con las cuales se recolectó información suficiente y de actualidad y la observación.

Se espera que esta tesis sea de utilidad para que se prevean soluciones a problemas, como los manifestados en este informe; logrando que el ente investigar se enfrente con nuevas estrategias para delinquir, de parte de delincuentes cibernéticos.

CAPÍTULO I



1. Datos personales y derechos humanos

Ante la observancia del irrespeto a los derechos humanos derivado de las guerras y dictaduras de Estado, surge una conciencia social común donde se unen las diferentes naciones del mundo, apoyadas en el derecho internacional, para acordar la protección de los derechos fundamentales del hombre y la mujer con el afán de mantener una armonía en las naciones.

La protección de los datos personales sensibles y crediticios incluye el respetar los derechos fundamentales e inherentes al ser humano a nivel universal, la Organización de las Naciones Unidas habla que son derechos inherentes a todos los seres humanos, sin distinción alguna de nacionalidad, lugar de residencia, sexo, origen nacional o étnico, color, religión, lengua, o cualquier otra condición.

Estos derechos se también se encuentran incluidos en las normativas internas de algunos países y fundamentados en tratados internacionales, el derecho internacional consuetudinario, los principios generales del derecho y los demás mecanismos del derecho internacional.

Es por ello, por lo que, todas las personas están afectas de ser protegidas de sus derechos más esenciales los cuales deben de ser respetados sin importar las condiciones en que se encuentren, y es también obligación de cada individuo el respetar y cumplir

con lo estipulado con respecto a este tema y no violentar el derecho de los demás



Los Estados también cumplen la obligación de respetarlos, absteniéndose de interferir en el disfrute de los derechos humanos, protegiéndolos impidiendo el abuso de los mismos contra individuos y grupos, realizándolos mediante la adopción de medidas positivas que faciliten el disfrute de los derechos humanos.

Esto, siendo parte esencial y elemental para el correcto funcionamiento de la sociedad sabiendo que es importante el debido cumplimiento de los derechos humanos, así como el de los mecanismos de cumplimiento de los mismos, siendo una parte integral para el desarrollo de cada persona.

Es así como también, nacen mecanismos internacionales que se encargan de velar por el cumplimiento de los derechos humanos por parte de los estados, evitando el abuso y el irrespeto a los mismos, pues es bien sabido que diversidad de estados se han atrevido a violentarlos, y es entonces cuando las personas interesadas acuden hacia organismos internacionales que se encargan del debido cumplimiento de la normativa en relación a este aspecto fundamental de las personas.

1.1. Derecho a la intimidad

El derecho a la intimidad o vida privada es la facultad que la ley le reconoce a una persona para que su vida íntima sea respetada y que sus actos no sean objeto de observación a efectos de que nadie pueda entrometerse en la existencia ajena publicando retratos,



divulgando secretos, difundiendo correspondencia, mortificando a otro en sus costumbres y perturbando de cualquier otro modo su intimidad.

La intimidad está conformada por aquella parte de nuestra vida que no está consagrada a una actividad pública y que por lo mismo no está destinada a trascender e impactar a la sociedad de manera directa y en donde en principio los terceros no deben tener acceso alguno, toda vez que las actividades que en ella se desarrollan no son de su incumbencia, ni les afectan.

Esto teniendo en cuenta que la privacidad consiste en el comportamiento del individuo con respecto a su ámbito de intimidad, esto hace una clara diferenciación entre intimidad y vida privada, pero al mismo tiempo afirma que estas dos se complementan entre sí y depende una de otra, para lograr su total comprensión.

Esto da una dimensión de lo que la intimidad implica, pues traspasa la barrera de la persona pública, quien por su condición de ser pública no implica que carezca de intimidad ni que no debe ser respetada la misma, su actuación como persona pública es la que debe interesar y no traspasar los límites de su intimidad.

Sin duda es necesario un espacio privado intocable, un espacio íntimo que constituiría lo que podríamos denominar como el “ámbito de la intimidad”, un ámbito sobre el cual no es posible injerencia externa alguna, tanto porque se trata de una información que no afecta ni impacta a la sociedad ni a los derechos de los demás, por referirse a aspectos estrictamente personales o familiares, como porque el uso o conocimiento de esa



información, sin aportar ningún beneficio o utilidad a la sociedad, puede ser origen de acciones discriminatorias frente a las cuales el individuo queda o causa de acciones discriminatorias frente a las cuales el individuo quedaría en absoluto estado de indefensión.

1.2. Derecho a la dignidad

La dignidad es un derecho que lleva implícito muchos otros derechos como por ejemplo el derecho a la vida, a la integridad física, a la libertad, la honorabilidad, la ética, puesto a que dignidad no puede definirse como un singular sino un compuesto de derechos que son relativos e indispensables para la persona y que sin duda alguna conforman una armonía de igualdad frente a los demás.

Es entonces la dignidad humana es un derecho que se forma de un conjunto de derechos intrínsecos y no se puede tomar como una definición singular “se encuentra relacionado con el respeto a la persona humana, la honra la reputación, además la dignidad es un valor espiritual y moral inherente a la persona, que se manifiesta singularmente, por la autodeterminación consciente y responsable de la propia vida y que lleva consigo la pretensión al respeto por parte de los de más y de la otredad (el respeto que yo debo a las otras u otros)”.¹

¹ Barco Pérez, Edi Lili, **Análisis del derecho a la intimidad en el ordenamiento jurídico guatemalteco referido a entidades mercantiles que comercializan datos personales**, Guatemala, Universidad Rafael Landívar, 2009. Pág 8.



Se trata de un respeto que debe cumplirse en cada persona, esto funciona cuando todos son conscientes de sus deberes, obligaciones, responsabilidades y derechos, esto quiere decir que, así como ellos o ellas son respetados, así también deben de respetar al prójimo, manteniendo una armonía y el que irrespete a el derecho de los demás debe de ser sancionado.

1.3. Derecho a la privacidad

Se hace necesario dar a conocer el origen de la palabra privacidad: puesto que, puede darse a diferentes interpretaciones que lleve hacia un sentido equivocado de lo que en verdad esta palabra transmite, proviene del latín *privare*, que significa privar que deriva en “*privatus*” que significa “aquello que no es público”.

En términos específicos, se puede afirmar que, es lo que una persona lleva a cabo en un ámbito reservado. Esto quiere decir que, la persona decide que sea de conocimiento público, para proteger su integridad. “Un sujeto, por lo tanto, tiene derecho a mantener su privacidad fuera del alcance de otras personas, asegurándose la confidencialidad de sus cosas privadas”.²

El derecho a la privacidad va más allá de las legislaciones nacionales e inclusive está considerado a la Declaración Universal de los Derechos Humanos; esto quiere decir que, tiene una importancia relevante y se convierte en intransferible, inalienable, irrenunciable

² *Ibíd.* Pág. 10.



e independiente; por lo que, busca un fin supremo, garantizando la dignidad del ser humano.

1.4. Datos personales

Cabe resaltar la procedencia de establecer la diferencia entre información y datos, pues, aunque son similares, no se refieren a lo mismo, como el autor William Ramírez expone: “dato es el antecedente o noticia cierta que sirve de punto de partida para la investigación de la verdad y aceptamos que ese dato se encuentra en un documento o soporte –físico o biológico- con la calidad de testimonio”.³

Lo anterior evidencia que, el dato es aquella información de la cual se tiene una certeza, así como un documento de respaldo, mientras que la información se limita a no tener una certeza exacta ni se necesita un respaldo que compruebe el extremo expuesto.

Establecida la diferencia, se puede definir ¿qué es lo que se entiende por datos personales?, indicando que “son todos aquellos que se refieren a una persona física identificada, desde su nombre hasta cualquier otro que revele información sobre sus hábitos, preferencias, forma de vida, etc”.⁴ Desde este punto de vista se aprecia que los Datos personales abarcan toda información que se refiera a un individuo, hace referencia a una persona física que sea capaz de ser identificada y por ende que sea comprobable

³ Ramírez, William, **Libre acceso a la información, protección de datos y hábeas data**, Guatemala, Fundación Myrna Mack, 2003. Pág.66.

⁴ Barco Pérez, Edi Lili. **Op. Cit.** Pág. 68

su existencia.

Datos personales son toda información sobre una persona física identificada o identificable. Entendiéndose por identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, o fisiológica, psíquica, económica, cultural o social.

Lo anterior “reafirma el concepto de identificable, lo cual se refiere a la existencia física, entonces el dato es aquello que existe y lo cual puede ser comprobado de alguna u otra forma”.⁵

Para adaptarlo a la realidad de la normativa de Guatemala se menciona desde su Carta Magna que establece en su Artículo 31 lo referente a este el cual establece que “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.”

La Ley de Acceso a la Información Pública de Guatemala en su Artículo 9 numeral 1 determina como datos personales a “Los relativos a cualquier información concerniente

⁵ Ibid.



a personas naturales identificadas o identificables.”

Pero para poder llegar a una determinación más exacta es importante mencionar que existe una diferencia dentro de los datos personales, entre los confidenciales que pueden ser aquellos “que sólo podrán ser proporcionados por la persona cuando exista una obligación de carácter legal, sea de naturaleza periódica o excepcional y la cual deba ser otorgada bajo garantía de confidencialidad.”

A diferencia de los secretos estableciendo que son los que la persona no está obligada a dar a nadie en ningún momento y por ninguna circunstancia. “Esto afirma que los confidenciales si pueden ser transmitidos bajo ciertas circunstancias, mientras que los secretos no pueden ser otorgados a ninguna persona por ningún motivo, pues al ser revelados se estaría atentando con los derechos de la persona”.⁶

Es por ello que, su protección es una necesidad que debe de cumplirse, en el caso de Europa fue el primero en implementar una forma de protección de los datos personales, siendo pionero en este ámbito, se fundamentaron en principios básicos para poder normar el tema de los datos personales, respetando cada uno de los derechos que son fundamentales para el ser humano.

Basados en el principio de que la recolección de datos debe tener un propósito en específico que debe cumplir y debe de utilizarse en forma razonable, pero esta

⁶ **Ibid.**



recolección debe de ser bajo el conocimiento de las personas y obtenerse por medios lícitos, utilizando la menor cantidad de información con respecto al individuo para no dañar su integridad.

Hay que tener en cuenta que, los datos deben de ser exactos, y deben de estar completos además de ser actuales, tres fundamentos que deben de ser fundamentales para que la información que sea errónea no afecte a las personas, algo que ocurre en nuestro país en la actualidad.

Los datos deben de tener un fin específico que sea lícito, esto quiere decir que no deben ser utilizados para fines delictivos o que dañen de alguna u otra forma la integridad o dignidad de la persona.

Esta información debe de tener las medidas de seguridad necesarias para que este aislada de terceros y no sea accesible a terceros sin previa autorización legal de las personas. Esto no debe ser solamente normado sino también garantizado, esto significa que se deben de adoptar las medidas necesarias para que la información sea salvaguardada, no limitándose nada más a generar normativas sino también garantías que propongan un manejo integral de la información.

Toda información debe de ser transparente; esto quiere decir que, las personas deben de saber cuál es la información que se tiene, y para qué fines o con que usos será utilizada, siendo un periodo y cometido específico, esto quiere decir que esta información debe de cumplir el cometido para la que fue recaudada, después de ello debe de ser



seguramente desechada sin dejar rastros ni malos usos, puesto que el tener una base de datos sin un fin en específico genera un descontrol que puede causar graves daños a la persona.

Un aspecto importantísimo sería la creación de un ente institucional que se encargue de regular los datos personales sensibles y crediticios, así como de la protección de los mismos, vigilando las entidades que los recaudan, así como las que los utilizan, rigiéndose por la legislación y respetando la normativa relativa al tema.

El aspecto más importante es el de consagrar el derecho que cada persona individual tiene de acceder a sus datos personales, y a los demás derechos relacionados con el tema, esto quiere decir que toda persona tiene el derecho de acceder a su información y esta no debe ser limitada ni mucho menos ocultada a los individuos.

1.5. Datos sensibles

Aquellos datos personales que revelen origen racial o étnico, opiniones políticas, convicciones religiosas o morales, afiliación sindical, información referente a la salud o a la vida sexual o cualquier otro dato que pueda producir, por su naturaleza o su contexto, algún trato discriminatorio al titular de los datos. Esto refleja que son datos que están ligados fuertemente con la persona y que puede llegar a generar cierta discriminación injustificada, guiada por prejuicios que generarían una imagen distorsionada de la persona, sin darle el valor como ser humano.



El autor William Ramírez va más allá e incluye los aspectos físicos que a fin de cuentas marcan una diferencia en el ámbito de apreciación de las personas, pues menciona que los datos personales sensibles “(...) se refieren a las características físicas o morales de las personas o hechos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.”⁷

La moralidad puede llegar a ser factor de apreciación por parte de las personas, inclusive llegando a generar cierta tendencia, es verdad que muchos actos morales no se encuentran normados, pero que ante los ojos de la sociedad pueden ser juzgados y objeto de fuertes críticas que afectan de gran manera al ser humano.

En Guatemala la Ley de Acceso a la Información Pública en su Artículo noveno, numeral segundo define los datos 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 u otras cuestiones íntimas de similar naturaleza.”

Esto aborda el tema desde un punto de vista integral, como se puede observar abarca todos los ámbitos antes mencionados y la importancia que cada uno, es fundamental

⁷ Ibid.

resaltar que una buena definición del tema logra crear una buena plataforma para el caso que se le pueda dar, y las directrices a tomar en torno a el tratamiento de este aspecto.

Los datos personales sensibles y crediticios en poder de terceros, pueden llegar a condicionar y afectar a las personas, pues los prejuicios de la sociedad generan discriminación, la cual no se limita solamente a la parte racial, sino que también sucede en todos los ámbitos de la vida cotidiana, desde la obtención de trabajos hasta expresiones en contra de individuos, pues el ser humano es un ser social y por ende necesita pertenecer a la misma sociedad que es la que contribuye al crecimiento y desenvolvimiento del individuo.

La importancia de la protección y la buena utilización de los datos personales sensibles es vital, puesto a que sin duda alguna pueden llegar a ser un condicionante en el correcto desenvolvimiento del ser humano, en el aspecto físico afectivo, laboral, sentimental y mental, dentro de otros, por lo que las instituciones encargadas de velar por el correcta utilización y distribución de la misma deben de funcionar de forma correcta y con apego a la ley.

1.6. Datos crediticios

Los datos crediticios también forman parte de los datos personales, y es importante la correcta apreciación de los mismos para entender de una forma integral el tema, la Superintendencia de Bancos de Guatemala a través de su sitio electrónico explica de una mejor forma lo que puede tomarse como datos personales como el reporte morosidad del



individuo, el endeudamiento, esto incluye a la institución, número de crédito, tipo de crédito, la garantía con la cual se respaldó dicho crédito, el saldo de la deuda de capital, los intereses pactados y cuando fue realizado el último pago para el abono de la deuda, siendo deudor o codeudor.

En términos concretos es el historial financiero de la persona de crédito bancario, en el cual esta anotado con detalles la información recopilada de todas las entidades financieras existentes, las cuales aportan dicha información.

Esto quiere decir que, solamente estas entidades tienen autorizado el acceso a esta información de las personas e inclusive son las únicas que pueden poseer estos datos, lo cual excluye a las entidades privadas que en su poder tengan este tipo de información sin autorización y que actúan al margen de la ley.

Pero esto también presenta otra interrogante de cómo las entidades privadas que se dedican a la comercialización de datos personales sensibles y crediticios obtienen la información crediticia de las personas, pues está claro que solamente las entidades antes mencionadas tienen el acceso a la misma.

La forma en que estos datos de carácter crediticio lleguen a entidades privadas es por medio de entidades bancarias y financieras que comercialicen con los datos personales y crediticios, teniendo en cuenta que no se puede obtener este tipo de información de otras fuentes que no sean las mencionadas anteriormente.



El Artículo 58, de la Ley de Bancos y Grupos Financieros de Guatemala regula la exclusividad del acceso a la información de este tipo, estableciendo lo siguiente: La Superintendencia de Bancos implementará un sistema de información de riesgos, para lo cual los entes a que se refiere la presente Ley están obligados a proporcionar la información que para el efecto determine dicha Superintendencia.

Al sistema de información de riesgos tendrán acceso, exclusivamente para fines de análisis de crédito, los bancos y grupos financieros y otras entidades de intermediación financiera que a pedido de la Superintendencia de Bancos apruebe la Junta Monetaria.”

En el último párrafo del Artículo 32 de la Ley de Libre Acceso a la Información Pública también regula lo siguiente: “En ningún caso se podrán crear bancos de datos o archivos con datos sensibles o datos personales sensibles, salvo que sean utilizados para el servicio y atención propia de la institución.”

La mala utilización de esta facultad representa un riesgo inminente para las personas y un abuso por parte de los banco y entidades financieras, puesto que algunas personas aprovechan su posición para sacar ventaja y comerciar con los datos de sus propios clientes, quienes ignoran o desconocen el gran abuso que se está cometiendo contra su persona.

1.7. El habeas data

“(…) derecho que tiene por objeto garantizar la facultad de las personas para conocer y



acceder a las informaciones que les conciernen archivadas en bancos de datos; controlar su calidad, lo que implica la posibilidad de corregir o cancelar los datos inexactos indebidamente procesados y disponer sobre su transmisión”.⁸

Esto contempla el conocer y acceder a la información que pertenece al mismo individuo que estén contenidos en cualquier banco de datos, teniendo el control de los mismos con la facultad de realizar correcciones o solicitar la cancelación de los mismos, protegiendo la veracidad de los datos y la integridad de la persona.

El autor William Ramírez lo define como “(...) una garantía procesal constitucional que protege el derecho a la intimidad, privacidad e identidad de la persona, frente al mal tratamiento que se le pueda realizar de los datos en poder del Estado o de entidades particulares (...)”⁹

En esta definición se incluyen derechos como la intimidad, privacidad e identidad, para algunos autores la privacidad es el derecho elemental a ser protegido, pues es allí donde convergen varios de los derechos fundamentales de la persona, pero es importante la mención de la intervención de los registros tanto del Estado, como de particulares, pues es bien sabido que la violación a estos derechos no solamente puede ser cometida por el estado, sino que es muy común en estos tiempos que entidades particulares se dediquen a la recopilación de los datos personales sensibles y crediticios funcionando al

⁸ Abad Yupanqui, Samuel B. **La Constitución de 1993. Análisis y comentarios**. Comisión Andina de Juristas. Serie: Lecturas sobre temas Constitucionales. Primera edición. 1994. Lima Perú. Pág. 266

⁹ **Ibid.**

margen de la ley.



Por su parte, la Ley de Acceso a la Información Pública de Guatemala delimita al habeas data en su Artículo 90, numeral cuarto como "(...) la garantía que tiene toda persona de ejercer el derecho para conocer lo que de ella conste en archivos, fichas, registros o cualquier otra forma de registros públicos, y la finalidad a que se dedica esta información, así como a su protección, corrección, rectificación o actualización.

Los datos impersonales no identificables, como aquellos de carácter demográfico recolectados para mantener estadísticas, no se sujetan al régimen de hábeas data o protección de datos personales de la presente ley."

Lo anterior quiere decir que, no solamente se realiza la importancia del habeas data sino también se instituye como una garantía para las personas, que debe ser cumplida para la protección de los derechos fundamentales, pero es también importante mencionar que se limita a registros públicos, por lo cual termina siendo vaga y poco funcional ante las amenazas que surgen en el presente, por parte de entidades particulares.

Es importante mencionar que, el habeas data más que un recurso, representa una garantía que persigue salvaguardar lo establecido en ley, puesto a que el recurso representa una acción procesal en la cual se reconocen las garantías que establece en el ordenamiento jurídico, mientras que para conocer la información que los sujetos obligados y demás entidades poseen en relación a las personas no hace falta el accionar un proceso específico, sino basta con el requerimiento a las autoridades y entidades

correspondientes, así como la rectificación de dicha información en base a la documentación que así lo respalde.







CAPÍTULO II

2. Robo de identidad

“En Guatemala no está tipificado el robo de identidad; asimismo, el Estado no cuenta con la tecnología suficiente, ni la capacitación de recurso humano, para la investigación de delitos informáticos”¹⁰.

De acuerdo con la tesis citada, el increíble avance en el desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos, información personal, mediante los cuales es posible obtener grandes beneficios económicos y causar perjuicios materiales o morales. La diferencia se basa en que es más difícil de descubrir, porque éste tipo singular de delincuentes es capaz de borrar sus huellas del hecho.

Según la actual cita, el robo, hurto o apropiación de la identidad de una persona se utiliza, siempre en perjuicio de la víctima, pues el acceso es ilegal y sin permiso. La falta de protección al consumidor de servicios de comunicación mediante dispositivos electrónicos vulnera indiscriminadamente a los usuarios de cualquier dispositivo

¹⁰ Zea Welmann, Arely Marisol. **Fenómeno del robo de identidad a través de dispositivos electrónicos en la ciudad de Guatemala**. Tesis de grado de la Facultad de Ciencias Jurídicas y Sociales, de la Universidad Rafael Landívar. 2016.



electrónico.

En Guatemala se atraen potenciales víctimas, mediante la utilización de la tecnología y los medios electrónicos robándoles sus claves, identidad o extorsionándole para perjudicarles y pedir dinero a cambio de terminar éstas acciones.

En el caso específico del fenómeno del robo de identidad en Guatemala es importante analizar el alto índice de robo de dispositivos móviles o dispositivos electrónicos y con ello la muy probable comercialización, dado que se brinda la oportunidad, de bases de datos, información, fotografías, claves, pines, contactos y un sin número de datos importantes en materia de seguridad para el usuario del medio electrónico.

Según la tesis citada, derivado el creciente número de denuncias de incidentes relacionados con el robo de identidad, se requieren métodos adicionales de protección. Se han realizado intentos con leyes que castigan la práctica y campañas para prevenir a los usuarios con la aplicación de medidas técnicas a los programas. Sin embargo, hasta el momento en Guatemala, el Estado no cuenta con una institución, dirección o unidad que vele por el bienestar del consumidor, cliente/usuario de la red.

En Guatemala, un delincuente de delitos cibernéticos tiene la gran ventaja de que la mayoría de la población no tiene educación sobre cómo mantener seguros sus datos. La ignorancia es la principal aliada del delincuente. Por ejemplo, si a una persona le roban su teléfono celular o dispositivo móvil, pueden tener en un lapso de tiempo, acceso a datos importantes sobre las personas; pines de seguridad, correos electrónicos, estados



bancarios o manejo de cuentas bancarias, contraseñas, teléfonos celulares y con este contacto, redes sociales, etc. vulnerando los datos del usuario y éstos pueden ser vendidos a personas inescrupulosas.

En la actualidad, en Guatemala se realizan investigaciones para ubicar a los responsables de 30 casos de robo de identidad en los que se utilizan los datos para adquirir préstamos bancarios, inscribir empresas, emitir facturas y cometer hechos delictivos. Dicha denuncia, publicada por todos los medios de comunicación, motiva la apertura de la Sección de Delitos Económicos del Ministerio Público y consecuentemente una Dirección de Delitos Económicos en la Policía Nacional Civil.

2.1. Las instituciones del Estado frente al robo de identidad

En Guatemala, cuando se trata de un delito penal, las instituciones de justicia que participan son:

- Policía Nacional Civil, encargado de la seguridad, de realizar las investigaciones y realizar las capturas emanadas desde el Organismo Judicial.
- Ministerio Público, dirige la investigación y realiza la persecución penal.
- Organismo Judicial, encargado de impartir justicia dentro del sistema de administración de justicia guatemalteco.
- El Instituto de Ciencias Forenses (INACIF), encargado de los peritajes
- El perito y el consultor.



- El Instituto de la Defensa Pública Penal, otorga defensa al sujeto procesado, regularmente el sindicado.

Sin embargo, no se ha articulado la cadena de justicia de tal forma que permita desplegar políticas de prevención del delito de robo de Identidad. Ninguna de las instituciones de justicia cuenta con una unidad especializada en la delincuencia cibernética para combatirla. El extremo radica en que las propias instituciones de justicia no cuentan con la seguridad necesaria para mantener sus propios datos seguros. Dicho extremo se manifiesta a nivel noticioso, cuando han sido públicos cientos de “ataques cibernéticos” a instituciones como el Ministerio Público, Ministerio de Gobernación, entre otras instituciones del Estado.

2.2. Instancias del Estado que tienen banco de datos

Las instancias del Estado que tienen banco de datos son, las siguientes:

- Registro Nacional de las Personas: a través del DPI
- Empresa Maycom: Extiende las licencias de conducir.
- Instituto Guatemalteco de Seguridad Social: a través del número de seguro social.
- Dirección General de Migración: extiende los pasaportes de los ciudadanos guatemaltecos. Instancias del Estado que registran datos:
- Registro Mercantil.
- Registro de la Propiedad.



- Departamento de Tránsito, a través la emisión de licencias de conducir.
- Registro de Marcas.
- Algunas instancias particulares que registran datos:
 - Entidades Bancarias
 - Redes Sociales
 - Páginas web
 - Personas individuales
 - Empresas de telefonía
 - Colegios profesionales
 - Universidades, colegios y escuelas

2.3. La corrupción

La desconfianza entre las instituciones se hace manifiesta, hasta en los medios de comunicación, que reflejan operaciones realizadas por el Ministerio Público, sin el conocimiento de la Policía Nacional Civil. Y es que, aunque en el Ministerio de Gobernación, Ministerio Público y Organismo Judicial (como principales instituciones del Estado, en los casos de robo de identidad mediante dispositivos electrónicos) cuentan con Oficinas de Inspectoría para la investigación de asuntos internos, éstas existen en papel, pero no cuentan con presupuesto asignado ni personal capaz de realizar todas las investigaciones.

En el caso de la Policía de Guatemala, la Oficina de Responsabilidad Profesional procede



luego de una denuncia contra un miembro de la institución, que luego será sometido al proceso disciplinario según llene las características tipificadas en el reglamento de la Ley Orgánica de la Policía Nacional Civil.

Las múltiples noticias, expuestas en medios de prensa, sobre corrupción en las instituciones dan cuenta de que al menos el 25% de cada presupuesto, se utiliza en distintas formas de corrupción.

2.4. Derecho comparado en relación al robo de identidad

Hay varios países que han demostrado un esfuerzo por regular el robo de identidad y en el caso de Guatemala, que no existe una tipificación sobre este delito, puede tomarse como ejemplo lo que se ha regulado al respecto en otros países como combate a este delito.

2.4.1. Estados Unidos de América

En los Estados Unidos de América, derivado de la enemistad con sectores de diferentes países, por sus políticas pasadas e intervencionistas, se aprobó la Ley de transacciones de crédito justas y precisas, (Fair and Accurate Credit Transactions Act o FACTA,) en la que la Comisión Federal del Comercio ha propuesto recientemente una definición de robo de identidad que se suma a la ley de Robo de Identidad; la que señala que el robo de identidad es todo fraude consumado o no consumado mediante el uso de información identificativa de otra persona sin permiso legal.



En donde la información identificativa es cualquier nombre o número que pueda servir, de manera individual o junto con otra información, para la identificación de un individuo concreto, incluyendo: nombre, número de seguridad social, fecha de nacimiento, licencia de conducir, número de carne de identidad, ya sea expedido por el Estado o por Gobierno Federal, número de pasaporte, número de identificación fiscal. Datos biométricos (huella dactilar, imagen de la retina o el iris, registro de voz o cualquier otra representación de un rasgo físico intrínseco. Número de identificación, dirección o código de enrutamiento electrónico exclusivos. Información de identificación de telecomunicaciones o dispositivos de acceso.

2.4.2. Chile

En mayo de 1993 se promulgó la Ley relativa a delitos informáticos, No.:19223, que establece:

“Artículo 1º.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2º.- El que, con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.



Artículo 3º.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4º.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado."

2.4.3. Países bajos

El primero de marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza los siguientes delitos:

- El hacking.
- El preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio).
- La ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría).
- La distribución de virus.

2.4.4. Delitos informáticos en América Latina

La tipificación difiere en el nombre que les acuña a los delitos, pero el espíritu de cada



uno es singular y característico. Otros países, sin embargo, tienen institucionalidad para el combate a éstos delito. La diferencia se basa en que el Estado no se ha fortalecido con herramientas para el combate de estos delitos.

La diferencia entre la consecución de los delitos tipificados en el Artículo 274 del Código Penal y el robo de identidad es la vulnerabilidad específica a la dignidad y seguridad de las personas.

Por otro lado, la clonación de tarjetas en Guatemala necesita del Robo de la Identidad de otra persona a quien le serán vulnerados 7 incisos (A – G) del Artículo 274 bajo el título de “destrucción de registros informáticos”, del código penal, con la consecuencia del apoderamiento de recurso financiero de la víctima.

Es ese dinero que le roban al usuario, de una tarjeta, lo que motiva la denuncia, lo que determina el robo de la identidad mediante un dispositivo electrónico y que deriva en la vulneración a raíz de obtener una copia exacta de claves, datos y accesos que permiten la sustracción de dinero.

En una tipificación de delito de clonación de tarjeta, habría que colocar la acción de sustracción de dinero del usuario del dispositivo, y si queremos ir más adelante, se coacciona la cooperación de entidades bancarias y se suprime el secreto bancario.

En muchos países de América Latina, no se toma en cuenta la ingeniería social como objeto de estudio permanente, ni se penaliza. Esta situación evidencia que la tipificación



específica de ciertos delitos describiría con mejor detalle la violación a la privacidad que un individuo sufre por parte de un sujeto que mediante actos de persuasión, encanto o engaño obtiene información de un usuario de dispositivo.

CAPÍTULO III



3. Proliferación del robo de identidad, ante la falta de tecnología especializada para la realización de la investigación

De acuerdo con la publicación del 17 de septiembre de 2021, de Saray Contreras Fresneda, abogada especialista en derecho penal, graduada en derecho por la Universidad Complutense de Madrid, España, el delito de usurpación de estado civil o suplantación de identidad consiste en la apropiación de todas las cualidades de una persona real, simulando ser ésta en distintos actos jurídicos. Debe tenerse ánimo de lucro, aunque no se exige que cause daños. También se da la suplantación de identidad digital.

3.1. Características de la usurpación de estado civil o suplantación de identidad

- Es considerada una falsedad personal.
- Es un delito de mera actividad, es decir que no se precisa la obtención del resultado.
- La situación debe tener una cierta duración o permanencia que induzca a confusión, y no solamente para algunos actos concretos y determinados.
- Además, debe tener cierta trascendencia.
- Recae sobre el estatus civil, como nombre, estado civil, profesión, nacionalidad, derechos conyugales y cuantos elementos conforman el estado civil.
- Debe tener la clara intención de obtener un beneficio o causar un daño, aunque éste



no llegue a materializarse.

- Deben haberse ejercido ciertos derechos y acciones de la persona suplantada.
- La persona sustituida debe ser real, aunque haya fallecido.

3.2. Alcance de la usurpación de estado civil

Para que la apropiación del estado civil o identidad configure un delito, debe reunir todas las características o datos que integran la identidad de una persona. Es decir, que para que se configure la usurpación, el usurpador debe poder hacer algo que solo la persona original podría hacer. De lo contrario, no se trata de un delito sino de supuestos de error, es decir, cuando el autor cree de buena fe ser una persona distinta de la que es.

3.3. Bienes jurídicos protegidos

Los bienes jurídicos protegidos, son:

- El estado civil. Este es individual, intransferible, y debe estar bien delimitado.
- Falseamiento de la realidad, que prevalece sobre el estado civil.
- Relaciones familiares, en tanto generan el estado civil de las personas y los deberes y derechos que nacen de éste.
- Seguridad del tráfico jurídico, en base a la idea de identidad personal y lo que ésta significa para la estabilidad de las relaciones jurídicas.

En cuanto a las personas perjudicadas, se considera que el delito de usurpación de

estado civil tiene dos víctimas: la persona usurpada y la persona engañada. El elemento subjetivo de este delito es el dolo directo, la suplantación llevada a cabo para usar los derechos y obligaciones de la persona sustituida. La conducta típica de la usurpación de identidad o estado civil es fingir ser otra persona real y verdadera con la clara intención de beneficiarse o producir un daño.

Los medios para usurpar el estado civil pueden ser:

- El engaño.
- Falseamiento de documentos privados, públicos u oficiales.
- Falsificación de certificaciones.
- Falsificación de tarjetas de crédito y débito y cheques de viajero.

La suplantación de identidad, tanto física como digital, además de daños materiales, puede causar problemas de credibilidad y afectar la reputación de las personas.

- Se debe evaluar:
 - Vulneración de derechos, por ejemplo, derecho a la intimidad o al honor.
 - Ventaja o beneficio económico obtenido por el usurpador.
 - Extensión en el tiempo del comportamiento delictivo.
 - Perjuicio para las víctimas.
 - Reincidencia.

3.4. Protección de datos y derecho a la intimidad

En la actualidad han aparecido nuevas técnicas que limitan nuestro derecho a la intimidad, relacionadas con el abuso de poder, asimismo como la necesidad de contar con información acerca de las personas y la libertad de acceso a la información, es necesario que se realicen algunas reformas en la legislación, para que se pueda proteger la vida privada e intimidad de las personas, teniendo como objeto que esta privacidad no sea transgredida, para lo que se necesita del apoyo de la ciencia Informática, por medio de la cual se violan con frecuencia estos derechos, y para que surja esta protección se necesita que exista una sólida protección de datos que nos debe brindar el Estado, por medio de una regulación específica y que debe llevarse a cabo por sus órganos, actualmente se encuentra vigente la Ley de Acceso a la Información Pública, Decreto 57-2008 del Congreso de la Republica.

Es necesario que se tomen las medidas pertinentes que tengan como finalidad evitar que miembros del Estado, de cualquier empresa privada o una persona particular, pueda realizar acciones con total discrecionalidad y sin ningún tipo de control, ya que se deben de establecer una serie de mecanismos adecuados que permitan a la ciudadanía conocer los actos efectuados por cualquiera de estos funcionarios o empleados, ya sean públicos o privados.

Uno de los mecanismos que se plantean es el reconocimiento del derecho de acceso a la información regulado en la Ley de acceso a la información, que tiene como fin, evitar que se caiga nuevamente en el autoritarismo o en acciones violatorias de los derechos



fundamentales o en acciones que afecten económica y socialmente a la mayor población. Existen numerosos motivos, por los cuales se ha generado la discusión de regular un conjunto de mecanismos con sus respectivas garantías, que permitan generar la protección de los datos privados y el derecho a la intimidad, con el objetivo de evitar que se violen las garantías fundamentales de las personas, por lo que los miembros de la sociedad civil van a poder controlar que datos van a ser públicos y cuáles van a ser privados.

Es de vital importancia que exista una regulación y clasificación legal de los datos personales, ya que en el mundo virtual existe una infinidad de información, que puede contener datos que puede obtener cualquier persona, con los cuales puede realizar perfiles culturales, económicos y sociales.

En este contexto se puede observar la importancia que tiene la información ya sea a nivel nacional, como en el ámbito internacional, por lo que se debe dar un tratamiento adecuado a esta información, conteniendo datos personales de las personas, que, por medio de la tecnología, se escapa de nuestras manos y se convierte en una fuente de ingresos de empresas inescrupulosas, que comercian con nuestros datos privados, violentando nuestro derecho de intimidad.

Se debe establecer que por medio de la tecnología se pueden obtener una serie de datos personales que son de gran valor o que representan poder, entre los que podemos citar:

a) Datos biográficos como el nombre, lugar y fecha de nacimiento y raza.



- b) Datos sobre el domicilio, ejemplo, dirección exacta del domicilio y teléfono.
- c) Datos civiles; estado civil de la persona e información acerca de los parientes legales y civiles.
- d) Datos laborales como el lugar y teléfono de trabajo, puesto de trabajo y salario.
- e) Datos financieros como la información acerca de las cuentas bancarias y tarjetas de crédito.
- f) información policiaca que incluye antecedentes penales y policiacos.

3.5. Datos de carácter personal

De acuerdo con la legislación comparada de España, según la Ley orgánica de protección de datos de carácter personal, se definen los datos de carácter personal "Como cualquier información concerniente a personas físicas identificada o identificables; y por tratamiento las operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, elaboración, conservación, modificación, bloqueo, y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones o transferencias".

Estos datos personales son aquellos que tienen características identificadoras de las personas o que se les pueden imputar a ellas; adquiriendo una vital importancia temas como la regulación de su uso, su manipulación y su protección legal.

Los datos personales se encuentran clasificados como datos personales íntimos que se subdividen a su vez en datos personales sensibles y datos personales no sensibles; y los



datos personales públicos que desarrollaremos a continuación:

3.5.1. Datos personales íntimos

Estos se dividen en los siguientes:

a. Datos personales sensibles

Se definen como “aquellos que por sí solos impulsan naturalmente a un individuo a la más íntima y absoluta reserva de dicha información. Por su carácter, requieren una regulación sumamente fina, detallada y muy especial que proteja correctamente la difusión de este tipo de datos y que su divulgación lo coloque en una situación de extrema incomodidad social”¹¹

b. Datos personales no sensibles

Se definen como "Son aquellos que se refieren a relativos a su fuero interno o íntimo sin llegar a ser un sujeto información identifican su personalidad, sus creencias e ideologías, sus pensamientos, sentimientos y salud, entre otras cosas".¹² Este tipo de datos son los relacionados al orden privado de los individuos, que los hacen merecedores de una protección más profundizada y específica que los demás tipos de datos generales, debido a que se revelan exclusivamente de forma particular e individual, y rara vez son objeto

¹¹ **ibid.**

¹² **ibid.**



de tratamiento público.

3.5.2. Datos personales públicos

Este tipo de datos se pueden definir como: "Son aquellos datos que constan en numerosos registros de carácter público o privado."¹³ Entre estos datos podemos citar el nombre y apellido, domicilio, estado civil, filiación, número de teléfono, la cedula de identidad y el pasaporte, título profesional, entre otros.

3.6. Los registros o bases de datos computarizados

A través del tiempo los seres humanos han basado su aprendizaje en experiencias que han tratado de preservar, ya que, en los inicios de la sociedad, el aprendizaje era transmitido de forma oral, de generación en generación, como cuentos, leyendas o historias de las experiencias vividas por las personas de mayor edad en la comunidad.

Desde entonces se han creado numerosos instrumentos y sistemas de almacenamiento, en donde se archivan todo tipo de datos incluso los de carácter personal, sin que esto afectara la intimidad y vida privada de los sujetos tal como señala el autor Santos Cifuentes "esa expansión de los archivos de toda índole, personales y de bienes, debido en general a la lentitud en la confección, falta de comunicación entre sí, tardanza en la búsqueda y encuentro de lo anotado, posibilidad de reaccionar a tiempo para evitar que

¹³ **ibid.**



se comuniquen los errores o que se publiquen las intimidades, facilidad en los pedidos de corrección antes de que se llegue al daño por causa de la entrada de asientos incompletos, inactuales o falsos, impidió que se levantara la inquietud ni se pensó en los peligros que para el ser humano tales registros podían representar".¹⁴

Actualmente, la evolución de los sistemas computadoras, la proliferación de las computadoras utilizadas de forma masiva y la creación de las bases o bancos de datos computarizados, la protección de los datos personales ha cambiado, ya que se ha convertido en una preocupación para las personas que tienden verse afectados en sus derechos, debido a que no existe un control estatal que nos de la seguridad que toda nuestra información esté protegida, por lo que se restringen nuestros derechos de privacidad y libertad de acción.

Con la Informática surge una serie de posibilidades en beneficio de la sociedad como son la posibilidad de una mayor capacidad de almacenamiento, la rapidez de la visualización de los archivos y la posibilidad de transmitirlos de una forma rápida y eficaz de un lugar a otro.

Al no ser utilizados estos beneficios de manera adecuada se pueden ocasionar daños a los derechos de las personas, pues dentro de las bases de datos, se encuentran diferentes tipos de características específicas de las personas como las sociales, psicológicas, somáticas, sanitarias, históricas, familiares, entre otras.

¹⁴ Santos Cifuentes, **Derecho personalísimo a los datos personales**, Pág. 35.



Esta información puede ser utilizada por terceros, sin el consentimiento del titular que acarrea una violación a sus derechos, al mismo tiempo, es un peligro para su privacidad, intimidad, su honor y su reputación.

Existe un temor en la proliferación de la violación de estos derechos fundamentales, que se lleven a cabo a través de los sistemas de archivos, ya que existen una serie de mecanismos tecnológicos que funcionan como medios de control o vigilancia de las actividades de las personas entre los que podemos mencionar: los teléfonos celulares, los software de red, el video, medios para ver a través de la vestimenta o a través de edificios, software para reconocer el contenido de un mensaje electrónico.

3.7. La justicia ante nuevos retos al darse los avances tecnológicos

El ser humano como sustento de los derechos fundamentales, se ve afectado por las influencias externas, políticas, económicas, sociales y culturales a nivel mundial. Dentro de esas circunstancias externas, existe globalización como orden económico mundial, sin embargo, ésta ha quedado atrás, actualmente nos encontramos en la sociedad de la información, que comprende el uso masivo de las tecnologías de la información (cualquier técnica utilizada para procesar, automatizar, archivar, resguardar y transmitir información), como herramienta para difundir el conocimiento y los intercambios en una sociedad.

Los estudiosos de la materia indican que los países más avanzados y con economías desarrolladas, han evolucionado y se encuentran en la sociedad del conocimiento (es



decir un paso adelante de la sociedad de la información), que comprenda la interconexión total, un conocimiento compartido y retroalimentado entre los miembros de una sociedad.

Dentro de la sociedad de la información se debe lograr encuadrar el rol del Derecho, como ciencia, pues éste a lo largo de la historia ha ido avanzando, adaptándose a los nuevos retos, principalmente la incorporación de la tecnología al hombre y el desarrollo de las comunicaciones que han impreso un ritmo muy acelerado al manejo de la información, a la vida y al desenvolvimiento de las sociedades modernas.

El papel del derecho en el desenvolvimiento de las sociedades de la información y del conocimiento es fundamental, debe servir como elemento disciplinador del proceso tecnológico, y cumplir con su función primordial, la de proveer seguridad jurídica y justicia a las sociedades y así lograr el bien común.

La tecnología se ha ido incorporando lenta y limitadamente al campo jurídico, pues el derecho no logra avanzar tan aceleradamente como se quisiera, por ende, los juristas se han visto en la necesidad de enfrentar con mayor profundidad las consecuencias que la tecnología ha generado en las estructuras del derecho y en las figuras jurídicas clásicas que se conocen desde el Derecho Romano.

En tal sentido, se afirma que, el internet es un medio moderno por el cual la sociedad en su conjunto puede expresarse libremente, y recabar información de igual modo, permite procesar, almacenar, recuperar y transmitir información en segundos. Las distancias se

acortaron y se modificó la forma de informarse, trabajar, aprender y enseñar, por ende es objeto importante de estudio en el derecho.



3.8. Derechos básicos y fundamentales en internet

“Los objetivos del desarrollo del milenio reflejan las principales metas específicas y medibles establecidas en distintas conferencias de la Organización para las Naciones Unidas -ONU- sobre el desarrollo”¹⁵, en las cuales se constituyen compromisos para los países con el propósito de luchar más firmemente contra desigualdades sociales, haciendo principal énfasis en la necesidad de la transferencia de tecnologías a los países pobres. Los países deben proporcionar la infraestructura necesaria para reducir la brecha digital, que afecta principalmente a la población.

Es decir que, el tema de la revolución tecnológica y el Internet ha tomado una dimensión muy importante, ya el acceso libre a las tecnologías es un tema de discusión internacional, tanto por su impacto en la economía e inversiones de un país, como en el marco del respeto y garantía de los derechos de los ciudadanos en las sociedades democráticas.

Por ende, se dice que dentro del Internet conviven derechos fundamentales (que derivan de los ya estudiados), pero que tienen un ámbito de aplicación muy especial -el ciberespacio- siendo estos los siguientes: Internet como derecho humano, libertad de

¹⁵ PNUD. Informe sobre desarrollo humano 2003. **Los objetivos de desarrollo del milenio. Un pacto entre las naciones para eliminar la pobreza.** Washington, D.C.: PNUD, 2003. p.27.



expresión y opinión en internet, derecho a la información, y derecho a la privacidad en internet.

En conclusión, en Internet se convive de la misma forma que en el mundo físico, en tal sentido los derechos, obligaciones de las personas, así como los deberes del Estado no cambian, solo se modifica el escenario en el que se realizan las actividades humanas.

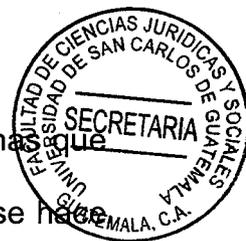
3.8.1. Derecho a la información

Dentro del mismo contexto, con relación por lo expuesto en la resolución de Naciones Unidas, es importante recalcar que la libre emisión del pensamiento conlleva el “derecho a ser informado” el derecho de acceder a información de manera ágil y sin restricciones ni limitaciones. Así lo afirma también la doctrina, el derecho a la información tiene dos perspectivas, desde la perspectiva del informador, el derecho a informar y a difundir información; desde la sociedad su derecho es a recibir información veraz.

Asimismo, el derecho a la información en internet necesariamente debe estar respaldado por las siguientes circunstancias relacionadas con la efectividad de esa información:

- a) La veracidad de lo que se informa;
- b) que no existe ningún obstáculo o elemento que restrinja, altere o impida su transmisión.

Es decir que, sería irresponsable difundir información que no tenga el sustento verídico, pues el derecho a la información, implica el derecho a “recibir información correcta”, por



ello, el Internet al autorregularse establece los mecanismos para que las personas que compartan información, se responsabilicen con el contenido de la misma, esto se hace mediante declaraciones unilaterales electrónicas en las páginas de Internet que utilizan de plataforma para informar, evidentemente nos encontramos ante el “deber ser”, pues se supone que el ser humano con valores no difundirá en medios masivos información que no es verídica, por lo que el derecho debe encontrar los mecanismos de protección y solución de los posibles conflictos que se deriven de estas circunstancias, pues el derecho jamás protegerá a quienes abusen de esa libertad de informar y ofendan la moral, el orden público, el honor y demás derechos fundamentales de terceros.

3.8.2. Derecho a la privacidad

El ser humano tiene una tendencia natural a conocer, apropiarse de información, a relacionarla con informaciones anteriores y a producir nuevas informaciones, y la tecnología le ha permitido desarrollar plenamente esa necesidad. Paralelamente a esa necesidad humana, está el deseo connatural del hombre de conservar determinados espacios de información ocultos a todos o a algunos de los seres con los que convive.

A pesar de que en el Internet la información se mueve a velocidades casi equiparables con la velocidad de la luz, toda persona tiene derecho a mantener una privacidad en internet (como un derecho fundamental intrínseco a su ser), por esa razón los sitios de internet, al autorregularse, han desarrollado políticas de privacidad, políticas de acceso, salvaguardas legales al ingresar a ciertos sitios, la solicitud del consentimiento de las personas al momento de ingresar alguna información, la confirmación de los usuarios con



un simple click, todo ello con la finalidad de que en el propio sitio quede constancia de que la persona otorgó su consentimiento o más bien consintió las políticas de privacidad del sitio consultado.

Los problemas legales surgen cuando dicha información privada no es obtenida legalmente, es decir no medió un consentimiento del titular ni su voluntad, pues en la tecnología y en Internet existen mecanismos ilegales para apropiarse de la información privada.

Es evidente que los derechos a manejar información y preservar una esfera de intimidad y de privacidad tienen su sustento en la propia naturaleza del ser humano, que constituyen derechos fundamentales que deben respetarse y garantizarse en todos los medios de interacción del hombre (sean físicos o virtuales). Por ende, la privacidad en Internet también ha sido denominada “Intimidad informática”, está protegida por las declaraciones universales de derechos humanos.

3.9. Modificación y adaptación de las relaciones jurídicas tradicionales al internet

El ciberespacio, mundo virtual, el internet o las nuevas tecnologías, como se le denominen, han tenido un impacto fuerte en las relaciones jurídicas:

- a) Han surgido nuevas figuras desconocidas anteriormente;
- b) Existen terceras personas intermediarias con una injerencia importante (como proveedores de internet, buscadores como Google, redes sociales, proveedores de



correo electrónico, verificadores de firmas electrónicas, etcétera);

- c) Las figuras jurídicas del derecho anglosajón se han equiparado e incorporado al derecho latino, a tal punto que a veces se emiten sentencias en el derecho latino fundamentadas en derecho anglosajón;
- d) Han proliferado las contrataciones electrónicas;
- e) La firma manuscrita ha sido remplazada por la firma electrónica;
- f) El comercio electrónico ha llegado a ser importante para la economía mundial;
- g) Las tendencias en redes sociales generan deberes y obligaciones e incluso la comisión de delitos;
- h) Las imágenes e información de las personas son expuestas eternamente en el mundo virtual, queda un registro de todo, ninguna información se puede eliminar por completo, siempre queda un rastro, una huella.

Con la anterior descripción, no limitativa, se deja abierta la posibilidad para seguir incorporando los posibles problemas jurídicos; dado que diariamente en minutos se crean infinidad de deberes y derechos para los usuarios del internet, las personas se obligan sin darse cuenta, otorgan su consentimiento sin estar conscientes de lo que hacen, transmiten su propiedad intelectual gratuitamente, exponen su vida privada y su información (con o sin su consentimiento), pueden ser víctimas de hackers (o intromisiones a su ordenador e información), o son lesionadas en sus derechos fundamentales, entre otros.

Dentro del mismo contexto haciendo un estudio profundo sobre las relaciones jurídicas online, se afirma que el internet es un territorio donde la inteligencia artificial dota de una



cierta autonomía al medio y eso puede llevar a pensar que es algo etéreo, impulsado en ocasiones por la inercia que no es humana o que condiciona la actividad humana.

También la etiqueta de territorio libre, especialmente apreciable en materia de libertad de expresión y publicación (aunque también con sus peligros) o de acceso al mercado puede llevar a acariciar la idea de defender un espacio desregularizado.

Por ende, con el internet y las nuevas tecnologías, la sociedad se plantea nuevos retos, que el derecho debe asumir, dado que las conductas y comportamientos sociales han evolucionado y ese espacio de interacción, -no físico, sin fronteras ni jurisdicción- ocasiona problemas legales y conflictos entre particulares para los cuales la legislación no está preparada, ni puede resolver.

Ese espacio desregularizado podrá ser normado por los principios de derecho internacional (privado y público), o serán insuficientes. Cuando se trata de regular actos que suceden en el Internet, al derecho le resultan insuficientes algunos principios tradicionales, y es que las características del Internet superan algunos principios generales del derecho internacional, por eso al darse el caso concreto es necesario integrar las normas internas, con las normas internacionales, incluso hacer uso de la jurisprudencia de otros países, como el derecho anglosajón, que en algunas ocasiones resuelve de una forma más eficiente los problemas suscitados en el mundo virtual.

Los aspectos que se han visto más afectados son el reconocimiento y garantía de los



derechos fundamentales, sobre todo los vinculados a los derechos de la persona, pues la intromisión a la intimidad, el menoscabo al honor y la utilización sin autorización de las imágenes de las personas se dan diariamente no sólo a través de periódicos electrónicos, sino que a través de redes sociales, portales, sitios de internet, o cualquier medio de información y comunicación, hasta el punto que a veces esas vulneraciones a los derechos fundamentales son incontrolables y debe requerirse la intervención del Estado para que los tutela, restablezca los derechos y condene a las indemnizaciones correspondientes por los daños ocasionados, sin perjuicio de las responsabilidades penales.

3.10. Deslocalización de los derechos y obligaciones en internet

Con respecto a la deslocalización de las relaciones jurídicas en las nuevas tecnologías, surgen los problemas de jurisdicción y competencia, el Derecho se pregunta quién tiene jurisdicción y competencia para conocer los conflictos surgidos en el Internet, es decir debe determinarse: El juez competente, el derecho que debe ser aplicado, y la ejecución de la sentencia obtenida, en caso de estar destinada a ser cumplida en otro país.

En vista que el Internet no tiene jurisdicciones ni fronteras, la ubicación física de las relaciones jurídicas es irrelevante, la independencia de restricciones geográficas permite que la jurisdicción sea en cualquier país del mundo. Se aprecia que en materia de contratos no existen mayores complicaciones si las partes se sometieron a un fuero especial; ahora bien, la necesidad práctica de buscar la jurisdicción es en materia penal y en materia de derechos humanos, donde las lesiones y el menoscabo a la persona



pueden ser muy serias y es mínima la posibilidad de reclamar una condena en daños y perjuicios.

Para resolver la problemática en el caso de vulneraciones a derechos fundamentales como la intimidad, el honor y la propia imagen, es necesario realizar análisis para definir que jurisdicción y competencia es la idónea, en tal sentido es preciso determinar alguno de los siguientes supuestos:

- a) Lugar donde se ocasionó el daño;
- b) Lugar donde se realizó la publicación;
- c) Si existe un representante del supuesto infractor en el país del afectado.
- d) Las políticas y normas del sitio de internet.
- e) Las advertencias legales incluidas en el sitio de internet.
- f) El consentimiento otorgado por la persona.
- g) Si dentro del sitio de internet se somete voluntariamente a un fuero especial;
- h) El domicilio del sitio de internet infractor, es decir en qué jurisdicción está alojado el servidor.
- i) El país de creación
Del sitio de internet;
- j) A través de mecanismos electrónicos determinar de qué servidor se emitieron las transmisiones electrónicas.
- k) Revisar la legislación local, internacional, y la legislación específica del país donde se determine que se cometió la infracción.
- l) En el caso de Guatemala, la experiencia ha sido que al demandarse a páginas de



internet, el órgano jurisdiccional no analiza los antecedentes virtuales, es decir no determina la titularidad de la página de internet, simplemente busca que exista un representante legal en Guatemala, siguiendo la concepción clásica de la jurisdicción y competencia, con la finalidad de resguardar inmediatamente los derechos fundamentales de una persona, como se analiza a continuación en una sentencia del tribunal constitucional.

3.11. Los derechos fundamentales, la intimidad, el honor y la propia imagen, en las nuevas tecnologías

Los derechos fundamentales asisten al hombre, sin importar circunstancias, factores externos, condiciones, o el medio en el que se desenvuelva, siendo este el espacio virtual dentro de la red, los Estados a nivel mundial debe sentar las bases y políticas públicas para que esas garantías que reconocen la dignidad del hombre se sigan respetando, es decir la tutela jurídica debe ser preventiva y supranacional.

Es recurrente que en la actualidad tecnológica se violen los principios inspiradores y filosóficos relacionados con los valores del hombre, pues los daños a la intimidad, al honor y a la propia imagen a veces son eternos, dado que en el internet queda guardada dicha información permanentemente, por lo que si no se otorga una tutela judicial efectiva a los afectados, los daños morales serán incuantificables e irreparables, pues no existiría indemnización suficiente para reparar un daño tan interno y tan vinculado con la esencia de la persona.



Definir y demarcar el contenido de estos derechos en la actualidad no es fácil y la forma de protegerlo es todavía más compleja, si se visualiza dentro de la “sociedad de la información” en la que se convive actualmente. Según la doctrina, dicho ambiente informativo produce riesgos imprevisibles de manera continua que condenan a la ciencia del derecho a permanecer rezagada detrás de la tecnología y dificultan una concepción unívoca o estática de la intimidad.

Las propias doctrinas que analizan la libertad de emisión del pensamiento¹⁶ establecen que el avance técnico, que permite una difusión prácticamente mundial de la información, ha comenzado a plantear diversos problemas jurídicos desde la atribución y defensa de los derechos y autor, hasta la posibilidad de publicar por todos los rincones del globo mensajes injuriosos y delictivos, pasando por el debate sobre control de los contenidos, la seguridad de la transmisión de información y transacciones comerciales o la propia idiosincrasia y normativización de las propias redes telemáticas, el ciber espacio, y dentro del periodismo electrónico, han promovido un debate jurídico.

Si bien la legislación vigente y jurisprudencia como fue analizada contiene un buen número de disposiciones que regulan la materia de la intimidad y la información, es evidente que hay lagunas creadas por el avance tecnológico que deben ser llenadas con legislación específica sobre todo en materia de intimidad, honor e imagen en las nuevas tecnologías, que establezcan y regulen los derechos de los individuos.

¹⁶ Armañanzas, EMY, DÍAZ NOCI, JAVIER, MESO, KOLDO. **El periodismo electrónico. Información y servicios multimedia en la era del ciberespacio.** Barcelona, España: Ariel Comunicación. Editorial Ariel, S.A. 1ª. Edición, 1996

De conformidad con lo analizado en capítulos anteriores, ya se conoce doctrinaria y legalmente los alcances y límites a la intimidad, el honor y la propia imagen, por lo que se abordarán soluciones desde la perspectiva constitucional, para minimizar los riesgos frente a los avances de las nuevas tecnologías.

3.12. Riesgos de las nuevas tecnologías y vulneración de derechos fundamentales

A finales de los sesenta, se empieza a reconocer internacionalmente por parte de Naciones Unidas el potencial peligro que, para los derechos de las personas, y en especial para la intimidad personal suponían las nuevas tecnologías, por lo que los debates la incidencia del uso de la electrónica en los derechos individuales iniciaron en ese momento y a la fecha continúan.

Se puede indicar que, el uso de la tecnología presenta dos grandes retos para el derecho, uno derivado de la protección de los derechos de la personalidad del individuo y la dignidad de la persona, y otro relativo al sistema de garantías y contrapesos de un estado democrático.

Cada vez más la intimidad se ve amenazada por la sociedad de la información, pues se reconoce la utilidad de la información y el derecho de acceder a esa información, también se reconoce la intimidad, pero ¿cuál es el equilibrio perfecto? Por otra parte, el posible mal uso de la tecnología en manos del Estado, que detenta información sensible de los ciudadanos, como en manos de particulares (como entidades financieras, empresas de auditoría, entre otras), crea diversos riesgos que pueden suponer una amenaza de

agresión a la intimidad de los gobernados o de los usuarios de los servicios.



A continuación, se perfilan una descripción no limitativa de los posibles riesgos en el uso de las nuevas tecnologías:

- a) Intromisión, con o sin consentimiento a la vida privada e íntima;
- b) Sustracción, legal o ilegal, del bien intangible más importantes en la era tecnológica, la información;
- c) Menoscabo de la condición digna de ser humano, al transmitirse en segundos datos, imágenes, noticias, correos electrónicos, tendencias en redes sociales y demás información, veraz o no, que afecten directamente lo más sagrado de la persona, su honor y su propia imagen;
- d) Daño irreparable al honor y a la propia imagen de la persona, pues toda la información queda registrada en el ciberespacio virtual de forma permanente, para siempre;
- e) Falta de control del individuo sobre la información de su persona que circula en la red;
- f) Sociedad vigilada y controlada por los gobiernos, lo cual puede generar otras implicaciones y persecuciones de tipo político;
- g) Estafas y fraudes en línea;
- h) Rastreo y monitoreo en línea e identificación de los usuarios, sus gustos, preferencias, y demás, pues se crean perfiles de los usuarios en internet (los posibles responsables son las entidades participantes en el Internet y en la sociedad de la información como buscadores, correos electrónicos, redes sociales,



localizadores, etcétera); este tema del rastreo ha sido discutido internacionalmente, a tal punto que las conferencias internacionales en materia de protección de datos y privacidad emitieron recomendaciones para minimizar esta clara intromisión a la intimidad, que consisten en respetar los límites de los derechos fundamentales, contar con herramientas de seguridad informática, abstenerse de utilizar las herramientas de rastreo, garantizar la transparencia, proteger los derechos de menores, entre otros.

3.13. Protección jurídica de la persona y sus derechos fundamentales, a través de normas legales nacionales e internacionales

Al haber delimitado y definido las dos posturas sobre el control que el Estado puede ejercer sobre el internet, es decir la regulación legal y la autorregulación, queda evidenciado que el Internet no puede restringirse ni limitarse.

Acotando en aspectos doctrinarios finales, existen posturas que establecen que, para proteger a la persona y sus derechos fundamentales, existen vías de solución el derecho positivo, las cuales son: técnica de balance, exigencia de consentimiento del individuo, el principio de gratuidad, la superación del interés del individuo por el de la humanidad (humanidad no debe ser confundida con colectividad).

Se considera que una posible solución es crear legislaciones tendientes a regular la conducta de los participantes en el Internet, que son tres:



- a) Proveedores de Servicios de Internet.
- b) Los servidores, que actualmente tienen una participación más activa, por la utilización de la nube virtual, como un archivo de la información mundial;
- c) Usuarios.

Dentro de esta regulación de la conducta y el comportamiento de los participantes, puede incluirse el control cruzado entre participantes; responsabilizar directamente las acciones de los usuarios; responsabilizar a los proveedores de servicios, es decir que estos sean los responsables civilmente de las indemnizaciones por los daños y perjuicios ocasionados; que el Estado sea el ente rector que tutele estas conductas sociales; y por ende responsabilizar a los Estados por violaciones a derechos humanos.

En tal sentido, dichos aspectos doctrinarios ejemplifican posibles formas de protección, como:

- a) Emitir una regulación legal mínima que rijan sólo determinadas conductas de los participantes.
- b) Fomentar principios generales del derecho que colaboren con el desarrollo de la autorregulación, es decir que el Derecho asista y asesore la autorregulación.
- c) Que el Estado sea el garante de la protección de los derechos humanos individuales, y que asegure su ejercicio frente a terceros, es decir que exista un efectivo Estado de Derecho que permita reclamar las vulneraciones a los derechos fundamentales como intimidad, honor y propia imagen, y responsabilizar civilmente a quien corresponda, para lograr una reparación de los daños ocasionados.



En síntesis, se matiza en que los derechos de la personalidad derivados de la dignidad del ser humano, es decir la intimidad, el honor y la propia imagen son derechos independientes pero pueden interrelacionarse como un todo, son inalienables e inseparables a la persona, son imprescriptibles y se han visto seriamente afectados por la tecnología, por lo que el Estado como ente rector, debe garantizarlos y tutelarlos, definiendo los mecanismos legales y las políticas públicas necesarias, no sólo para garantizarle a los ciudadanos un libre ejercicio de estos y un pleno desarrollo de su personalidad, sino también para sancionar a los responsables y restituir el menoscabo a las víctimas, mediante el pago de las indemnizaciones correspondientes que reparen los daños y perjuicios ocasionados.

3.14. Desarrollo y masificación de las nuevas tecnologías de la información

Con el desarrollo y masificación de las nuevas tecnologías de la información debemos realizar un verdadero análisis de la suficiencia del ordenamiento jurídico guatemalteco actual para regular las nuevas posiciones, los nuevos escenarios, en donde observamos los problemas del uso y abuso de la actividad informática y su repercusión en el territorio guatemalteco. Por esta razón han surgido una serie de acciones delictivas, que en algunos casos son de difícil tipificación en las normas penales, sin recurrir a aplicaciones analógicas prohibidas por el principio de legalidad, regulado en el Artículo número siete del Código Penal, Decreto 17-73 del Congreso de la República.

Por medio del Decreto 33-96 del Congreso de la Republica, se reformó el Código Penal vigente, modificando el Artículo número doscientos setenta y cuatro e implementando los



delitos contra los derechos de autor, la propiedad industrial y algunos delitos informáticos, entre los que podemos citar: la destrucción de registros informáticos, la alteración de programas, la reproducción de instrucciones o programas de computación, los registros prohibidos, la manipulación de información, el uso de información y los programas destructivos.

La implementación de estos delitos informáticos fue un verdadero avance para la legislación guatemalteca en materia penal e informática, ya que establece un antecedente para la tipificación de delitos informáticos que surgen a raíz del progreso de la tecnología, como en el presente caso, que se pretende la implementación del delito informático de robo de identidad dentro del ordenamiento jurídico guatemalteco.

Es muy importante que se lleve a cabo la tipificación del delito informático de robo de identidad dentro del ordenamiento jurídico guatemalteco, debido a que este es uno de los ilícitos que ha tenido mayor crecimiento en la red alrededor del mundo. Este delito es una forma de engañar a los usuarios para que revelen información personal o financiera de carácter confidencial, mediante un mensaje de correo electrónico, algún sistema de mensajería instantánea o sitio web fraudulento.

Los delincuentes informáticos conocidos como hackers, obtienen por medio de engaños dentro de la internet los datos personales privados del sujeto pasivo, para que después este individuo pretenda ser o hacerse pasar por el sujeto pasivo y realizar operaciones o acciones en su nombre para cometer fraudes, causando un daño patrimonial y en otras ocasiones también puede darse un daño de carácter moral, ya que se pueden utilizar los



datos del sujeto pasivo para cometer algún delito y causar sentimientos en las víctimas como la humillación, la ira y la frustración, al no poder realizar ninguna acción contra el delincuente que ha utilizado su información. Cualquier persona que ingrese sus datos confidenciales a la red puede ser víctima de este delito y sufrir sus consecuencias.

3.15. ¿Qué es robo de identidad? Tips para no caer en esta estafa

“El robo de identidad o usurpación de identidad es la apropiación de la identidad de una persona. Hacerse pasar por esa persona, asumir su identidad ante otras personas en público o en privado, en general para acceder a ciertos recursos o para la obtención de créditos y otros beneficios en nombre de esa persona. Esto es un delito grave que ha aumentado en los últimos años, por lo que debes cuidar de tu información personal. La forma más habitual en que los estafadores obtienen tu información personal es a través de enlaces maliciosos incluidos en un correo electrónico “Phishing”, filtraciones de datos de sitios en los que tienes cuentas o hardware sin protección. Tu cuenta bancaria y tarjeta de crédito se pueden usar para crear cuentas falsas o para hackear las cuentas que tienes actualmente”.¹⁷

3.15.1. Diez tips para evitar ser víctima de esta estafa

1. Cuida tu correo electrónico, es importante que cuides de la información que

¹⁷ <https://blog.corporacionbi.com/seguridad/tips-para-no-caer-en-robo-de-identidad>. **¿Qué es Robo de Identidad? Tips para no caer en esta estafa.** (Consultado el 22 de abril de 2022).



tienen adjunta en tus correos, como por ejemplo: DPI, contraseñas o recibos de servicios en donde se muestre tu dirección.

2. En tal caso te hayan robado o hayas extraviado tu DPI, repórtalo con la Policía y guarda la denuncia en caso te sirva más adelante.
3. Evita publicar en tus redes sociales información sensible como dirección de casa o trabajo, números de teléfonos, fotografías que muestren el lugar donde vives o donde estudian tus hijos, lugares que frecuentas entre otros.
4. Cierra las sesiones de tus plataformas tecnológicas cuando no las estés utilizando, tales como redes sociales, banca en línea, correo electrónico o tiendas virtuales. Nunca marques la opción “recordar” usuario o contraseña en navegadores públicos.
5. Evita proporcionar tus credenciales de acceso en sitios sospechosos o descargar adjuntos que provengan de un correo electrónico, con esto evitas el peligro de phishing e infección de malware que pueda comprometer tu información confidencial.
6. Aplica las configuraciones de privacidad que ofrecen las distintas plataformas tecnológicas, esto para evitar que desconocidos visualicen tu información personal y confidencial. (quienes ven tu perfil, como pueden contactarte, fecha de nacimiento, números telefónicos, entre otra información).
7. Desactiva los servicios de localización como Bluetooth y GPS, salvo cuando los necesites
8. Crea contraseñas seguras, que tengan como mínimo 8 caracteres, combinando mayúsculas, minúsculas, números y caracteres especiales.
9. Actualiza el software y el antivirus periódicamente.



10. Ten cuidado con la publicidad engañosa, los ladrones la utilizan para infectar tu computadora por medio de un “Ransomware”, es un virus que infecta tu computadora mediante archivos adjuntos que envían por correo electrónico.

3.16. Robo de identidad: Sacó un préstamo por Q400 mil con documentos falsos pero fue sorprendido y capturado en la zona 10

De acuerdo con publicación de Sany Pineda, de fecha 2 de diciembre de 2022, a víctima había denunciado el robo de sus documentos personales y tarjetas de crédito, indicaron las autoridades sobre el caso.

Un hombre deberá enfrentar un proceso penal, acusado de robo de identidad y estafa. Un hombre sospechoso de fraude fue detenido el 30 de noviembre, justo cuando pretendía recoger los fondos de un préstamo que habría requerido a una institución bancaria. El único inconveniente es que lo hizo con documentos falsos, según informaron las autoridades.

El caso inició en julio pasado, cuando Jorge Alberto Calderón Campos, quien está acusado de tres delitos, hurtó el Documento Personal de Identificación (DPI) a su víctima, entre otras pertenencias.

“El sindicato habría aprovechado, en julio pasado, la distracción de una persona para sustraerle su documento personal de identificación y varias tarjetas de crédito”,



describió la fiscalía en torno a los primeros indicios.

Fue entonces que, según los investigadores, Calderón Campos habría utilizado la identificación de la víctima para gestionar un crédito de Q400 mil ante un banco del sistema.

3.16.1. Confirman detención por robo de identidad y estafa

“Pasado un tiempo, cuatro meses después, el sospechoso recibió un aviso para presentarse a una sede de la entidad financiera. Fue ahí que se procedió a su captura por la Policía Nacional Civil (PNC), “cuando se presentó a recibir los cheques del préstamo que había solicitado”, dice el informe”.¹⁸

El hombre fue detenido en una entidad ubicada en la zona 10 de la Ciudad de Guatemala el 30 de noviembre. El Ministerio Público indicó que la fiscalía presentó los indicios ante un juzgado durante la audiencia de primera declaración de Calderón Campos, que se celebró el 1 de diciembre. Ahora el detenido está ligado a proceso penal por los cargos.

Calderón Campos enfrentará proceso penal por los delitos de estafa propia, uso ilegítimo de documento de identidad y uso público de nombre supuesto. El delito de estafa propia, regulado en el Código Penal guatemalteco, hace referencia a que induciendo a error a

¹⁸ <https://www.prensalibre.com/guatemala/robo-de-identidad-saco-un-prestamo-por-q400-mil-con-documentos-falsos-pero-fue-sorprendido-y-capturado-en-la-zona-10/>. **Robo de identidad: Sacó un préstamo por Q400 mil con documentos falsos pero fue sorprendido y capturado en la zona 10.** (Consultado el 28 de abril de 2022).



otro, mediante ardid o engaño, defraude a otra persona en su patrimonio en perjuicio propio o ajeno.

El responsable de este delito será sancionado con prisión de seis meses a cuatro años y una multa de Q200 a Q10 mil.

Los casos especiales de estafa como uso ilegítimo de documento de identidad ajena y uso de nombre supuesto, conlleva una pena de prisión de uno a tres años de prisión.

Con la realización de esta tesis se ha podido evidenciar cómo el robo de identidad se ha incrementado, valiéndose los delincuentes, de la cibernética, y creando estrategias para delinquir, que no se atacan por la dificultad de no contar con herramientas el ente investigador, para combatirlos.

Estos delincuentes actúan con libertad al tener presente que sus estrategias pasan inadvertidas, y que están a la vanguardia con la tecnología, con la cual pueden llevar a cabo todo lo necesario para conseguir sus propósitos.

Esta es una situación lamentable, que tiene en zozobra a la ciudadanía, porque no se les respeta su privacidad y derecho de contar con datos personales; y por el contrario hacen uso de ellos, como que fueran propios, cometiendo todo tipo de fechorías, escudándose en un nombre que no les pertenece y que dejan una serie de problemas a la víctima; quien tiene que apersonarse en los juzgados para determinar que no fue quien realizó ese tipo de hechos, que van desde librar o cambiar cheques, retirar dinero y la utilización



de tarjetas de crédito, que de la noche a la mañana aparecen vacías; existiendo discrepancias en el sentido de que, pudiera darse el caso de que algunos cajeros pagadores de los bancos estén de acuerdo o amenazados de parte de estos criminales.

Por lo anterior, se hace necesario que el ente investigador se provea de herramientas para poder tener la ventaja de contrarrestar este tipo de hechos delictivos.





CONCLUSIÓN DISCURSIVA

El derecho a la intimidad o vida privada, es la facultad que la ley le reconoce a una persona para que su vida íntima sea respetada y que sus actos no sean objeto de observación; a efecto de que nadie pueda entrometerse en la existencia ajena, publicando retratos, divulgando secretos, difundiendo correspondencia, mortificando a otro en sus costumbres y perturbando de cualquier otro modo su intimidad; así como robar su identidad para cometer actos fuera de la ley. La intimidad está conformada por aquella parte de nuestra vida que no está consagrada a una actividad pública y que por lo mismo no está destinada a trascender e impactar a la sociedad de manera directa y en donde en principio los terceros no deben tener acceso alguno, toda vez que las actividades que en ella se desarrollan no son de su incumbencia, ni les afectan.

El robo de identidad en Guatemala se refleja en un alto índice de robo de dispositivos móviles o dispositivos electrónicos y con ello la muy probable comercialización, dado que se brinda la oportunidad, de bases de datos, información, fotografías, claves, pines, contactos y una gran cantidad de datos importantes en materia de seguridad, para el usuario del medio electrónico; por lo que es muy fácil robarle la identidad.

Derivado del creciente número de denuncias de incidentes relacionados con el robo de identidad, se requieren métodos adicionales de protección: asimismo que, el ente investigador se provea de tecnología especial para poder combatir a estos delincuentes.



BIBLIOGRAFÍA



ABAD YUPANQUI, Samuel B. **La Constitución de 1993. Análisis y comentarios.** Comisión Andina de Juristas. Serie: Lecturas sobre temas Constitucionales. Primera edición. 1994. Lima Perú.

ARMAÑANZAS, Emy, Díaz Noci, Javier, Meso, Koldo. **El periodismo electrónico. información y servicios multimedia en la era del ciberespacio.** Barcelona, España: Ariel Comunicación. Editorial Ariel, S.A. 1ª. Edición, 1996

BARCO PÉREZ, Edi Lili, **Análisis del derecho a la intimidad en el ordenamiento jurídico guatemalteco referido a entidades mercantiles que comercializan datos personales,** Guatemala, Universidad Rafael Landívar, 2009.

BARRIOS OSORIO, Omar Ricardo. **Derecho e informática.** Aspectos Fundamentales. Guatemala: Ediciones Mayte, 2007.

HERRERO TEJEDOR, Fernando. Texto traducido y citado. **Honor intimidad y propia imagen.** Madrid: Colex, 1994.

<https://blog.corporacionbi.com/seguridad/tips-para-no-caer-en-robo-de-identidad>. **¿Qué es Robo de Identidad? Tips para no caer en esta estafa.** (Consultado el 22 de abril de 2022).

<https://www.prensalibre.com/guatemala/robo-de-identidad-saco-un-prestamo-por-q400-mil-con-documentos-falsos-pero-fue-sorprendido-y-capturado-en-la-zona-10/>. **Robo de identidad: Sacó un préstamo por Q400 mil con documentos falsos pero fue sorprendido y capturado en la zona 10.** (Consultado el 28 de abril de 2022).

PÉREZ LUÑO, Antonio. **Derechos humanos, Estado de Derecho y Constitución.** Madrid: Tecnos, 1984.

PNUD. Informe sobre desarrollo humano 2003. **Los objetivos de desarrollo del milenio.** Un pacto entre las naciones para eliminar la pobreza. Washington, D.C. Estados Unidos de América: PNUD, 2003.

RAMÍREZ, William, **Libre acceso a la información, protección de datos y data**, Guatemala, Fundación Myrna Mack, 2003.



Legislación:

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

Código Penal. Decreto 17-73 del Congreso de la República y sus reformas. 1973.

Ley de bancos y grupos financieros y sus reglamentos: Decreto número 19-2002 del Congreso de la república, Clasificación en Biblioteca Landívar, Guatemala, Librería Jurídica, 2007.

Ley de Acceso a la información pública: versión comentada, Gramajo Valdés, Silvio René coordinador, Clasificación en Biblioteca Landívar, Guatemala, Vicepresidencia de la República, 2011.

Ley de Acceso a la Información Pública, Decreto 57-2008 del Congreso de la Republica.

Ley Orgánica de la Policía Nacional Civil. Decreto 11-97. 1997.