Universidad Hispanoamericana

Facultad de Derecho

Tesis Para Optar por el Grado Académico de Licenciatura en Derecho

Derecho Informático y Protección al Consumidor

Autor: Alberto Elizondo Araya

Tutor: Andrés Ávalos Rodríguez

San José, Costa Rica, 2021

Dedicatoria

Dedico esta tesis a mis padres, quienes impulsaron mi carrera, motivándome y ayudándome en los momentos más difíciles, confiando siempre en mi capacidad y esfuerzo.

A mi hermana Priscilla quien caminó a mi lado y no me dejó caer en el proceso.

A mis amigos Sebastián y Abel, quienes estuvieron pendientes y me dieron apoyo incondicional en todo momento.

A mi tutor Andrés Ávalos, quien desde que fue profesor mío me enseñó a balancear y entender que la carrera va de la mano con la vida misma teniendo siempre las prioridades en orden y manteniendo la calidad humana.

Para ellos este trabajo, fruto de mi esfuerzo e hito en mi desarrollo académico, siendo un escalón más en la vida.

DECLARACIÓN JURADA

Yo Alberto Elizondo Arayes, mayor de edad, portador de la cédula de identidad número 1-1314-0011 egresado de la carrera de Derecho de la Universidad Hispanoamericana, hago constar por medio de éste acto y debidamente apercibido y entendido de las penas y consecuencias con las que se castiga en el Código Penal el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi trabajo de tesis para optar por el título de Licenciatura en Derecho, juro solemnemente que mi trabajo de investigación titulado: Derecho Informático y protección al consumidor

_____

_____

_____, es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 del 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte; articulo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que éstos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Asimismo, quedo advertido que la Universidad se reserva el derecho de protocolizar este documento ante Notario Público.

En fe de lo anterior, firmo en la ciudad de San José, a los 8 días del mes de abril del año dos mil veintiuno.

_____

Firma del estudiante

Cédula: 1-1314-0011

CARTA DEL TUTOR

San José, 5 de abril de 2021

Piero Vignoli Chesler
Director Carrera de Derecho
Universidad Hispanoamericana

Estimado señor:

El estudiante ALBERTO ELIZONDO ARAYA, cédula de identidad número 1-1314-0011, me ha presentado, para efectos de revisión y aprobación, el trabajo de investigación denominado "**Derecho Informático y Protección al Consumidor**", el cual ha elaborado para optar por el grado académico de Licenciada en Derecho.

En mi calidad de tutor, he verificado que se han hecho las correcciones indicadas durante el proceso de tutoría y he evaluado los aspectos relativos a la elaboración del problema, objetivos, justificación; antecedentes, marco teórico, marco metodológico, tabulación, análisis de datos; conclusiones y recomendaciones.

De los resultados obtenidos por el postulante, se obtiene la siguiente calificación:

a)	ORIGINAL DEL TEMA	10%	10%
b)	CUMPLIMIENTO DE ENTREGA DE AVANCES	20%	20%
C)	COHERENCIA ENTRE LOS OBJETIVOS, LOS INSTRUMENTOS APLICADOS Y LOS RESULTADOS DE LA INVESTIGACION	30%	30%
d)	RELEVANCIA DE LAS CONCLUSIONES Y RECOMENDACIONES	20%	20%
e)	CALIDAD, DETALLE DEL MARCO TEORICO	20%	20%
	TOTAL		100%

En virtud de la calificación obtenida, se avala el traslado al proceso de lectura.

Atentamente,

Andrés Ávalos Rodríguez
110790061
16037

Lic. Andrés Ávalos Rodríguez
Abogado
Carné 16037

CARTA DE LECTOR

San José,

Universidad Hispanoamericana
Sede Llorente
Carrera de Derecho

Estimado señor

El estudiante **Alberto Elizondo Araya**, portador de la cédula de identidad: **1-1314-0011**, me ha presentado para efectos de revisión y aprobación, el trabajo de investigación denominado "**Derecho Informático y Protección del Consumidor**", el cual ha elaborado para obtener su grado de **licenciatura en Derecho**.

He revisado y he hecho las observaciones relativas al contenido analizado, particularmente lo relativo a la coherencia entre el marco teórico y análisis de datos, la consistencia de los datos recopilados y la coherencia entre éstos y las conclusiones; asimismo, la aplicabilidad y originalidad de las recomendaciones, en términos de aporte de la investigación. He verificado que se han hecho las modificaciones correspondientes a las observaciones indicadas.

Por consiguiente, este trabajo cuenta con mi aval para ser presentado en la defensa pública.

Atte.

ODITH BOLANDI CASTRO (FIRMA)

Firmado digitalmente por ODITH BOLANDI CASTRO (FIRMA)
Fecha: 2021.05.20 22:12:32 -06'00'

M.Sc. Odith Bolandi Castro.
Cédula: 1-0823-0885.
Carné: 12 179.

UNIVERSIDAD HISPANOAMERICANA
CENTRO DE INFORMACION TECNOLOGICO (CENIT)
CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DE LOS TRABAJOS FINALES DE GRADUACION

San José, 8 de abril, 2021

Señores:
Universidad Hispanoamericana
Centro de Información Tecnológico (CENIT)

Estimados Señores:

El suscrito (a) Alberto Elizondo Araya con número de identificación 1-1314-0011 autor (a) del trabajo de graduación titulado Derecho Informático y protección al consumidor

presentado y aprobado en el año 2021 como requisito para optar por el título de Licenciatura en Derecho; (S) / NO) autorizo al Centro de Información Tecnológico (CENIT) para que con fines académicos, muestre a la comunidad universitaria la producción intelectual contenida en este documento.

De conformidad con lo establecido en la Ley sobre Derechos de Autor y Derechos Conexos N° 6683, Asamblea Legislativa de la República de Costa Rica.

Cordialmente,

1-1314-0011
Firma y Documento de Identidad

Índice

Objetivos

Objetivo General

- Determinar el grado de aplicación del derecho informático en cuanto a la protección de datos y transacciones del usuario o consumidor y su relación con la normativa costarricense.

Objetivos Específicos

- Analizar la integración de normativa internacional mediante el derecho comparado en cuanto a la protección de datos del consumidor y su utilización en cuentas virtuales mediante la red.
- Estructurar el almacenamiento y regulación de datos sensibles y personales junto a su respectiva utilización a nivel global y regional.
- Determinar los casos de aplicación del Derecho informático en cuanto a protección del consumidor en la normativa costarricense mediante sentencias y derecho consuetudinario.
- Comprobar e identificar las áreas de mejora y vacíos legales en cuanto a la protección de datos virtuales aplicable en el cuerpo normativo nacional.

Introducción

En el presente trabajo de investigación se pretende principalmente realizar una síntesis exhaustiva donde se logre identificar la aplicación del Derecho Informático en la normativa nacional, realizando un estudio mediante el método comparativo y analítico de la aplicación legal en diferentes países del mundo y resaltando la importancia de la protección al consumidor en cuanto a la utilización de servicios cibernéticos.

La globalización tecnológica es un tema en constante desarrollo y evolución. Los seres humanos dependen cada día más de la tecnología y las facilidades otorgadas por esta, por lo cual deben también acoplarse a sus ventajas y desventajas. Dentro del desarrollo tecnológico nos hemos tenido que adaptar a el sistema de comunicación más amplio y eficaz de las últimas décadas como lo es la internet y sus diferentes variantes aplicables que van desde ordenadores hasta dispositivos móviles.

Dentro de esta misma red de comunicaciones se han establecido diferentes protocolos los cuales nos permiten realizar todo tipo de actividades cotidianas y a su vez mantenernos conectados con nuestro entorno ya sea inmediato o lejano lo cual va desde revisar nuestra correspondencia virtual, noticias nacionales y mundiales en tiempo real, hasta transacciones bancarias, inversiones millonarias y compraventas, por mencionar unos cuantos.

Si bien todas estas actividades que se realizan a diario cuentan con muchas facilidades y ventajas, también abren un portillo a la hora de manejar información personal, confidencial y sensible, por lo cual ha sido necesario una protección tanto a las personas físicas como las personas jurídicas involucradas en el otorgamiento y manejo de este tipo de información. Si bien miles de instituciones privadas y gubernamentales cuentan con el acceso a nuestros datos tales como

domicilio, estado civil, edad, lugar de trabajo y hasta los bienes que poseemos, no quiere decir que toda la información compartida deba estar al alcance de todas las personas, es por esta razón que la regulación de los medios virtuales es de suma importancia.

En Costa Rica aún y cuando se ha logrado integrar una regulación normativa con un marco jurídico amplio en cuanto a los delitos informáticos y la protección de datos, es necesario que se detalle, conozca, estudie e investigue con más amplitud este tema el cual está en un constante y acelerado cambio.

Es por esta razón que mediante el presente trabajo se abordará, en un sentido crítico y amplio mediante la comparativa del derecho aplicable internacionalmente y las normas jurídicas costarricenses vigentes, las relaciones en cuanto a la creación de cuentas, almacenamiento, protección de datos y compromiso entre los consumidores y quién preste sus servicios a estos últimos, tomando en consideración las actualizaciones y proyectando a futuros cambios que puedan surgir.

Normalmente, aún y cuando se cuenten con leyes muy concretas y bien estructuradas, al estudiar algo tan cambiante como el mundo virtual, se debe realizar un refrescamiento constante el cual acapare las diferentes actualizaciones. Tal y como los mismos dispositivos tecnológicos cuentan con actualizaciones en sus sistemas, nuestro cuerpo legislativo debe permanecer al tanto de cubrir cada implementación que se dé y pueda afectar a los usuarios, tanto negativa como positivamente. Se incluye la parte positiva porque así y como se deben sancionar conductas peligrosas o riesgos cibernéticos, también, con estos cambios mencionados, se pueden adquirir beneficios que impactan de buena manera al usuario, pero que deben ser regulados para cumplir con el índice de justicia y equidad.

Dentro de la misma investigación se realizará un marco estructural que detalle el tipo de información que se maneja de manera virtual, así como las principales herramientas de almacenamiento, protección y utilización que se les brinda tanto a nivel global como nacional y su propia relación con la legislación existente y pertinente.

Es de suma importancia contar con un entendimiento amplio en cuanto a los conceptos utilizados en el mundo virtual, con el fin de aplicar las regulaciones adecuadas. Asimismo, dentro de esos conceptos, es necesario entender cómo funciona un sistema y su impacto en las personas antes de dedicarse a marcar límites jurídicos ya que en el ámbito informático se debe considerar el hecho de que las acciones regulables no existen en un plano físico, más si existen acciones físicas que vinculan a las personas con este mundo cibernético.

Dentro del mismo análisis se pretende esclarecer todas estas herramientas que tienen una relación directa con estos datos, permitiendo un amplio entendimiento de su conexión física y virtual, así como los procesos necesarios para poder manifestarse en ambos ámbitos.

En cuanto a la protección de esta información se busca estudiar la aplicación del Derecho Informático actual en Costa Rica respaldándose no solo en las normas vigentes si no en la reiteración de casos y soluciones aplicadas mediante la jurisprudencia nacional, de esta manera logrando determinar los problemas más comunes y situaciones de riesgo a las cuales se enfrentan los costarricenses diariamente y realizando un análisis a fondo de cuales circunstancias podrían experimentar a futuro.

Mediante los estudios mencionados se realizará un análisis exhaustivo de las áreas cubiertas y de mejora en la jurisdicción nacional, identificando los vacíos y zonas grises de la ley en cuanto a la

protección del consumidor, sus datos sensibles y experiencia relacionada con la red y la informática.

Aún y cuando el tema de la informática y las transacciones virtuales lleve vigente tan poco tiempo, existe una gran cantidad de casos que se han abordado a nivel nacional, aplicando primeramente normas desactualizadas y apostando al raciocinio y lógica de los tribunales. Conforme se ha dado la evolución del tema y la implementación del conocimiento en el área, se ha logrado construir jurisprudencia sólida, concisa y coherente, razón por la cual su inclusión es de suma importancia en el presente estudio.

En vista de lo mencionado anteriormente se decide realizar una investigación a modo de tesis que profundice los temas mencionados en el derecho informático y las diferentes aristas relacionadas al consumidor en su totalidad y su debida protección.

Marco Metodológico

Tipo de investigación:

La finalidad de esta investigación es dirigida a la comparativa histórica y actual en cuanto a la evolución del comercio, tecnología y relación entre el consumidor y los diferentes servicios adquiridos en el transcurso de los años. Debido al tipo de estudio, la dimensión temporal se sitúa bajo el método longitudinal recurriendo a datos históricos alrededor del globo y a un sistema de carácter comparativo y descriptivo el cual permitirá la amplitud y enriquecimiento de la información plasmada dando un respaldo sólido al tema estudiado en cuanto a tiempo y espacio.

Sujetos y Fuentes de Información:

La presente investigación se enfoca en el estudio del consumidor como sujeto principal, haciendo énfasis en su relación las respectivas transacciones comerciales, así como los respectivos comerciantes y proveedores de los servicios, dirigido a la evolución tecnológica y las debidas transacciones mediante medios electrónicos.

No se cuenta con fuentes de primera mano, sin embargo, como fuentes de segunda mano se hará referencia a libros y revistas jurídicas referentes a aspectos relevantes en cuanto al tema en estudio y los diferentes cuerpos normativos nacionales e internacionales relacionados incluyendo jurisprudencia judicial costarricense.

Marco Conceptual

El presente estudio, como se mencionó previamente, se enfoca en analizar la relación jurídico-informático en el tema de regulaciones con énfasis en el estudio y protección al consumidor. Para el correcto entendimiento de esta relación, se considera necesario conceptualizar determinados términos generales los cuales se estarán cubriendo en el desarrollo de la presente tesis.

Es importante aclarar que las definiciones no corresponden a una cita textual de un documento específico si no que presentan la condensación de un conjunto de definiciones sobre el mismo concepto y lo aquí expuesto es acuñado por el redactor.

1. Definición de Conceptos

1.1 Software

El término software ha sido adquirido e incorporado a la lengua hispana primeramente considerado un anglicismo. Podríamos identificar al software como un programa de computadora, el cual fue desarrollado para cumplir ciertas funciones.

La integración de este término en el derecho informático es fundamental, ya que los programas informáticos conocidos como software, pueden contribuir al intercambio de datos entre los ordenadores y la red. Un ejemplo de varios tipos de software vanUn ejemplo de varios tipos de software va desde aplicaciones desarrolladas para un sistema operativa, hasta programas utilizados en la vida cotidiana como lo son los ya reconocidos paquetes de Microsoft Office, tales como Word, Excel, Powerpoint y One Note entre muchos otros.

1.2 Hardware

El hardware es otro término considerado anglicismo, el cual se ha adaptado a el lenguaje informático hispanohablante. Cuando se habla de un hardware se hace referencia al equipo físico

informático directamente. Si bien el software es la parte programable virtual, el hardware es el equipo que se encarga de que este sirva adecuadamente mediante componentes electrónicos. Se analiza a manera de ejemplo, el sistema operativo Windows es considerado un software mientras que la computadora, llámese monitor, CPU (Unidad de Procesamiento Central, por sus siglas en inglés), teclados y mouse serían considerados hardware. El hardware también podría tomarse como los teléfonos inteligentes por medio de los cuales se realizan transacciones de todo tipo mediante sus sistemas o aplicaciones.

La importancia de este concepto en la presente investigación radica en el conocimiento básico de los sistemas utilizados para poder ingresar, almacenar o incluso modificar la información sensible de los usuarios en cuanto a materia regulada en la normativa.

1.3 Ordenador

El ordenador es el dispositivo físico o hardware que ensambla todos los componentes necesarios para poder realizar las funciones necesarias para las cuales fueron determinados. Un ejemplo de ordenador es una computadora en su totalidad la cual junto a sus componentes (hardware), al sistema operativo y al software instalado, les permite a los usuarios realizar diferentes tipos de tareas.

1.4 Sistema Operativo

El sistema operativo, conocido también como OS por sus siglas en inglés, es un tipo de software el cual se encarga de organizar y habilitar las funciones en un dispositivo mediante la realización de tareas las cuales utilizan todos los recursos físicos del equipo que se utilice.

Los dos sistemas operativos más conocidos a nivel mundial en computadores son Windows (de la empresa Microsoft) y iOS (De la empresa Apple). En cuanto a dispositivos móviles, los principales sistemas operativos son Android y iOS.

Los sistemas operativos vienen programados con una interfaz amigable al usuario, de manera que este pueda acceder a las funciones y aplicaciones de su dispositivo de manera cómoda y sencilla, sin limitar las funciones para las cuales fue fabricado el dispositivo. Es importante el conocimiento básico de los sistemas operativos, ya que mediante estos se pueden realizar las gestiones utilizando los diferentes programas o aplicaciones (vistas a continuación).

1.5 Aplicación

Una aplicación es conocida como un tipo de software o programa, cuyo objetivo es realizar funciones determinadas o facilitar trámites para cierta empresa o servicio. Actualmente relacionamos las aplicaciones con los teléfonos inteligentes, ya que son aquellas que instalamos en estos últimos para poder acceder a las redes sociales, banca en línea, mensajería instantánea, llamadas, videollamadas y hasta para comprar o vender. Ejemplos de estas aplicaciones son las desarrolladas por los bancos para poder realizar depósitos, transferencias, pagos y demás servicios directamente utilizando la red.

Al tener estas aplicaciones una relación tan amplia en la vida cotidiana de las personas, son las herramientas más utilizadas a la hora de realizar un fraude o engaño el cual ponga en peligro la información personal de los usuarios y los datos utilizados en estas.

1.6 Servidor

En materia informática actual, los servidores han adquirido extrema importancia, dado a su capacidad de almacenamiento y procesamiento de datos. Antes de entender su funcionamiento se deben categorizar en dos partes, la parte física (hardware) y la parte virtual (software).

El término se refiere al hardware como el equipo necesario para almacenar información o programas para el correcto funcionamiento de un servicio a través de una red. Este consta de memoria física para contar con una capacidad de almacenamiento. Es importante que esté conectado a la red para poder realizar un intercambio de datos. Un servidor es el que almacena los datos de una aplicación o base de datos. Cuando se contrata algún servicio que requiere nuestra información, esta es almacenada en servidores para poder ser accedida en cualquier momento por medio de la red. Un ejemplo es la base de datos con la que cuentan las entidades bancarias, las cuales almacenan la información referente a las cuentas que soliciten los usuarios.

El servidor desde punto de vista de software es el programa que se instala en el dispositivo físico para poder manejar sus datos y sus configuraciones.

1.7 Red

La red informática se puede ver desde un punto de vista simple al citar una red de pesca. En una red de pesca se pueden observar distintos nudos que van uniendo las líneas que la conforman, formando así un sistema donde todos los puntos están conectados entre sí. Así es precisamente como funciona una red informática, solo que, en vez de los nudos, se tienen dispositivos los cuales están conectados entre sí. La red más común, y la que se estará utilizando durante este trabajo es la Internet, la cual es una red a nivel mundial encargada del intercambio de datos en tiempo real. El usuario puede conectarse a la internet mediante una red inalámbrica, la cual puede ser mediante un dispositivo conocido como router o por medio de datos, los cuales son proporcionados

normalmente por un proveedor de servicios; o alámbricas que son redes que se acceden mediante un cable de red conectado directamente al modem.

1.8 Enrutador/ Modem

El modem es un dispositivo físico el cual se utiliza por el proveedor de servicios para poder brindar al usuario acceso a la red. El modem por otra parte es un dispositivo físico similar, sin embargo, este se encarga de poder distribuir la red proporcionada por el modem a diferentes puntos donde se instale. El enrutador también es el encargado de distribuir la red inalámbrica donde se instale.

1.9 Proveedor de servicios

El proveedor de servicios es aquella compañía encargada de proporcionar un servicio al usuario. En los casos de redes son aquellas compañías que se encargan de proveer servicios de redes telefónicas o de internet mediante la transferencia de datos (Ejemplo: Kolbi, Claro, Movistar) hacia los respectivos dispositivos móviles mediante una tarjeta SIM, la cual se encarga de gestionar los mencionados datos a los usuarios. En el caso de servicios de internet, el proveedor de servicio se encarga de proporcionar un servicio de internet a hogares y compañías por medio del uso de un módem y/o enrutador.

1.10 Nube

La nube es un término comúnmente utilizado hoy en día. Normalmente el almacenamiento de datos en nuestros dispositivos móviles y ordenadores tienen una capacidad limitada, por lo cual es necesario recurrir a diferentes métodos para hacer respaldos. Si bien existen dispositivos los cuales pueden ser utilizados para aumentar la capacidad de almacenamiento, estos pueden ser costosos o incluso incómodos a la hora de ser utilizados, por esta razón es que nació la nube. La nube es una red de servidores los cuales son utilizados para poder almacenar nuestros archivos de manera virtual. La nube no existe físicamente, ya que es un espacio en la internet con una capacidad muy

amplia para poder liberar y dejar de depender del almacenamiento físico. Este almacenamiento es protegido y gestionado por una aplicación, por lo cual en cantidades altas puede tener un costo por capacidad. Al contener archivos personales, es necesario que la nube cuente con su debida protección de datos para sus usuarios.

1.11 Usuario

El usuario en el ambiente informático no se aleja mucho del concepto de usuario en general. El usuario es aquella persona que hace utilización de algún servicio. En términos informáticos, el usuario es aquella persona que utiliza el equipo ya sea móvil u ordenador. También se puede referir a un usuario como el nombre que identifique a una persona a la hora de acceder una aplicación o servicio de manera virtual. Normalmente viene acompañado de una contraseña, con la cual se puede identificar que efectivamente la persona que está accediendo el servicio sea la que lo contrató.

1.12 Datos

Los datos son aquella información cifrada la cual es intercambiada mediante la red. Cuando el usuario se conecta a la red, a la hora de ingresar a una página de internet o utilizar una aplicación existe intercambio de datos el cual permite que se pueda desplegar la información requerida en el dispositivo que estamos usando. También, durante ese intercambio de datos el usuario puede enviar a la red, página de internet o aplicación la información que ingrese. Un ejemplo de intercambio de datos es el siguiente: El usuario necesita buscar información en Google, por lo cual ingresa desde el ordenador. En la barra de direcciones digita la página www.google.com, esto enviará los datos ingresados con la dirección digitada a un servidor mediante el internet. Una vez que el servidor identifique la información ingresada por el usuario por medio de esos datos transmitidos, se encargará de devolver otro paquete de datos el cual desplegará en la pantalla del

usuario la página de internet que estaba buscando y así sucesivamente. Cabe señalar que el intercambio de datos es tan rápido que normalmente toma solo unos segundos acceder a una página que necesitemos.

En cuestiones de internet mediante telefonía, los datos se refieren al plan de datos adquirido, el cual determinará cuantos datos podemos bajar de la red en un tiempo determinado.

1.13 Encriptación de datos

Teniendo un entendimiento básico de cómo funciona el intercambio de datos, se debe asegurar que ese intercambio pueda hacerse de manera segura y efectiva sin que sea interceptado por ningún hacker (término explicado más adelante) o algún usuario de mala fe. En si la encriptación es la alteración de los datos de manera que no cualquier ordenador los pueda cifrar o leer. La encriptación es una manera segura de poder realizar transacciones de datos riesgosas tales como una compra en línea o acceder a la cuenta de un banco, hoy en día incluso las aplicaciones de mensajería instantánea cuentan con encriptación de datos para asegurarse de que nadie pueda interceptar información sensible o privada. La encriptación de datos es aquella protección que brindan los programadores a la navegación en la red.

1.14 Contraseña

Desde tiempos antiguos una contraseña es simplemente una palabra o conjunto de palabras clave la cual solamente una persona o personas seleccionadas conocen para poder acceder a un lugar o información. En el ámbito informático no existe gran diferencia, ya que la contraseña es aquella que en conjunto con un nombre de usuario le permiten a una persona acceder a una página de internet determinada o a los servicios de cierta aplicación que sean exclusivos a esta. Normalmente se solicita que la contraseña que cree un usuario tenga una fortaleza mínima, incluyendo caracteres

difíciles de adivinar como mayúsculas, minúsculas, caracteres especiales y números. La contraseña es el sistema más básico en cuanto a protección de datos mediante la red.

1.15 Token

En ciertas entidades donde la seguridad debe ser priorizada se utilizan dispositivos llamados tokens. Los tokens pueden ser físicos (normalmente con una pequeña pantalla) o incluso una aplicación, la cual se va a encargar de desplegar una serie de caracteres cada cierto periodo de tiempo. Se utiliza junto a la contraseña, de esta forma, si alguien pudiera adivinarla, debe tener acceso al token también ya que la serie de caracteres desplegadas por este está en sincronización con un servidor, y si no se digitan exactamente como muestra la pantalla del dispositivo o aplicación, el sistema deniega el acceso.

1.16 Hacker

Los hackers son confundidos comúnmente con delincuentes cibernéticos. Se debe empezar aclarando que esto es incorrecto hasta cierto punto. El hacker es una persona con amplio conocimiento en redes, los cuales se encargan de verificar o detectar vulnerabilidades en la seguridad de programas o el intercambio de datos mediante la red. Un hacker puede actuar mediante lenguajes de programación avanzados utilizados para la encriptación de datos.

Los hackers, dado su conocimiento amplio pueden actuar de manera contraria a la ley o a la buena fe, por lo cual mediante diferentes herramientas pueden utilizar los datos que acceden para beneficio propio o de personas ajenas que hayan pagado por sus servicios. Gracias a ese conocimiento pueden acceder a datos sensibles, privados y hasta confidenciales, es por esta razón que las empresas que necesitan proteger los datos almacenados (esto incluye a los gobiernos que manejan grandes cantidades de información confidencial) contratan sus servicios para que detecten fallos en su sistema de encriptación y seguridad.

1.17 Virus

En general un virus es un software que altera el funcionamiento de algún programa, sistema operativo o incluso componentes físicos normalmente con fines maliciosos. Haciendo referencia a la palabra original, actúa como los microorganismos infectando el sistema mediante transmisión de datos. El virus informático puede ser desatado abriendo un archivo o ingresando a alguna página de internet sin encriptado de seguridad, entre otros, y puede lograr desde robar nuestros datos protegidos y personales hasta inhabilitar el funcionamiento de nuestro ordenador. Existen varios tipos de virus, los principales detallados a continuación

1.17.1 Malware

El malware es un software malicioso el cual es instalado en el ordenador y realiza funciones dañinas. El malware normalmente altera el funcionamiento adecuado del sistema operativo pudiendo también revelar información confidencial del usuario.

1.17.2 Spyware

El Spyware es un software espía, por su término en inglés. Es un tipo de malware que, al ser instalado en el sistema operativo, puede rastrear la información que se maneje en este y se intercambie por medio de la red. Es sumamente peligroso ya que este puede robar información confidencial o sensible como lo son las contraseñas, nombres de usuario y demás utilizadas en las aplicaciones o la red.

1.18 Phishing

El phishing es considerado como una estafa cibernética. Por medio de engaños se guía a los usuarios a ingresar información sensible la cual puede ser utilizada con fines maliciosos. Un ejemplo de esto son los mensajes que se pueden apreciar cuando se ingresa a una página de internet

donde dice que se es ganador de una suma muy alta de dinero y que solamente deben ingresar al enlace y digitar un número de tarjeta de crédito o similar.

1.19 Scam

El scam es un término muy similar al phishing, considerando que es también un tipo de estafa cibernética. La diferencia del scam radica en que este utiliza recursos o medios conocidos para ejecutar la estafa. Normalmente los ciberdelincuentes envían correos dirigidos al usuario indicándole que son ganadores de un concurso, que deben actualizar sus datos en alguna página o incluso que son herederos de una persona. Estos pueden ser también mediante mensajes de texto, mensajería instantánea por medio de la red o aplicaciones de uso personal. Los mensajes contienen un enlace donde hay que registrar la información solicitada para reclamar su "premio", y es mediante este que los delincuentes roban la información requerida.

1.20 Navegador

Un navegador de internet es el programa utilizado para poder acceder a las páginas de internet o buscadores por medio de la red. Entre los navegadores más populares se encuentran Internet Explorer, Microsoft Edge, Google Chrome y Mozilla Firefox entre otros.

1.20 Cookies

Las cookies son conocidas como "galletas informáticas", son archivos de datos, los cuales se almacenan en un navegador, y se encuentran en páginas de internet los cuales se encargan de mantener la información de acceso de un usuario. Estas cookies son creadas directamente por el sitio web que visita el usuario y recolectan información de ingresos a la página ayudándoles también a determinar el traficotráfico de información que se realizó en la misma. Normalmente son utilizadas para que la página recuerde las preferencias o configuraciones del usuario para facilitar el acceso a las páginas manteniendo una experiencia más eficiente. Las cookies no

recolectan información personal a menos que se trate de una página de internet dañina la cual instale un virus en el dispositivo.

1.21 Antivirus

El antivirus es un programa que se instala en un dispositivo informático, el cual se encarga de borrar o aislar actividades sospechosas o virus informáticos. Este programa presenta actualizaciones periódicas las cuales deben ser instaladas correctamente para lograr su efectividad. Normalmente el antivirus funciona de dos maneras, detectando cualquier intrusión en el equipo y analizando los programas y datos que estén ya instalados en el equipo. Los virus informáticos se asemejan a los virus biológicos, los cuales se reproducen en las células. Esto sucede con el virus informático al infectar archivos e instalarse incluso en funciones primordiales del dispositivo que infecta. El análisis de intrusión se realiza al detectar cualquier tipo de programa que quiera instalarse o abrirse en el dispositivo, por ejemplo, discos duros externos, dispositivos de almacenamiento USB, o incluso cuando el usuario baja información o accede a alguna página por medio de la red. La actualización de la base de datos en un antivirus se realiza por medio de un equipo de trabajo que detecta los nuevos tipos de virus y los decodifica para poder contrarrestarlos, tal y como funciona una vacuna en la vida cotidiana. Si un antivirus no logra determinar el tipo de virus pero detecta un archivo que podría ser dañino, lo coloca en un estado de cuarentena, aislándolo de todos los demás archivos e impidiendo al usuario poder ejecutar o abrir el programa hasta que se actualice la base o el usuario manualmente lo coloque en una “lista blanca”.

1.22 Dirección IP (Internet Protocol)

La dirección de Protocolo de Internet, o IP por sus siglas en inglés es aquel identificador a la hora de transmitir y recibir paquetes de datos. Para poder navegar por la internet, es necesario que el dispositivo envíe paquetes de datos, los cuales serían el comando que el usuario está ejecutando,

y a su vez, la dirección a la que se está accediendo devuelve paquetes de datos para poder desplegar la información en el dispositivo del usuario. La dirección IP es un número asignado aleatoriamente para identificar los equipos que intercambian los paquetes de datos. La dirección IP es asignada por el proveedor de internet y normalmente cambia por medio de comandos o cuando el equipo es apagado por un periodo de tiempo. (algunos equipos y usuarios pueden contar con una IP fija o estática la cual no cambiaría).

1.23 Dirección MAC

La dirección MAC, por sus siglas en inglés “Media Access Control” es un grupo de caracteres alfanuméricos los cuales sirven de identificación. Estos caracteres son únicos y asignados los equipos por el fabricante. Cuando un usuario accede a la red, la dirección MAC queda registrada, haciendo más sencilla la identificación de los equipos a la hora de navegar en caso de existir alguna actividad sospechosa o ilícita.

1.24 Data Mining (Minería de Datos)

La minería de datos es un término que nació a partir del almacenamiento de datos a nivel global.

Desde tiempos antiguos el mercadeo se enfoca en el concepto de oferta y demanda el cual es generado a causa de las necesidades del cliente. Estos intereses, preferencias y necesidades son transformados en datos los cuales pueden ser utilizados para determinar futuros productos, implementaciones, servicios los cuales pueden beneficiar al consumidor o a la población. Con la integración de las nuevas tecnologías, esos datos son almacenados en la nube o en bases de datos que pertenecen a las grandes compañías, no obstante, a nivel mundial este tipo de recolección y almacenamiento fue implementado por los gobiernos alrededor del mundo.

Con las facilidades de la internet, la transferencia y manejo de datos se convirtió en un tema que puede ser utilizado de manera muy positiva. La minería de datos es un conjunto de técnicas, las cuales, aplicadas a los datos recolectados, permiten a las empresas o gobiernos organizar, verificar y acceder a los datos proporcionados de manera sencilla con el fin de manejar estadísticamente estos datos, facilitando su comprensión y aplicándolos para beneficio de los usuarios.

Claramente la minería de datos puede ser utilizada de manera negativa, es por esta razón que es importante que las empresas o entidades que se encarguen de su recolección y utilización cuenten con sus debidas cláusulas de confidencialidad y transparencia en cuanto al empleo de la información recolectada.

Un ejemplo claro de minería de datos podría consistir en información en cuanto a interacciones en redes sociales con respecto a interacciones con cierto producto, tendencias e incluso hasta demografía para calcular el área donde se requiera trabajar.

1.25 Consumidor

El consumidor en si es aquella persona que consume un bien o servicio por parte de un proveedor, vendedor o productor que lo ponga a disposición por medio de una transacción para suplir alguna necesidad. El consumidor normalmente ofrece algo a cambio de los servicios o productos que adquiere, pero no solamente se limita a sumas dinerarias u objetos. Cuando una persona adquiere una tarjeta de crédito se está convirtiendo en un consumidor del banco o de la empresa crediticia y, aunque muchas veces se pague una membresía o anualidad para contar con esa tarjeta, en muchos casos pueden contar con esta sin necesidad de brindar nada a cambio. De igual forma en la actualidad existen servicios donde se brinda entretenimiento por medio de la red, ya sea por medio de videos, imágenes o contenido de interés general. En muchos casos el contenido es

gratuito (solamente debemos contar con acceso a internet), sin embargo, estamos consumiendo el servicio de entretenimiento brindado por el autor de dicho contenido.

En el ámbito informático el consumidor es aquella persona que consume el material brindado virtualmente ya sea de manera gratuita o paga. Este puede acceder a los servicios tales como compra y venta, contratos, alquileres, almacenamiento de datos y hasta prestación de servicios.

Capítulo 1 - Generalidades Derecho Informático y protección de datos

1.1 Definición de Derecho informático y ámbito de protección

Antes de adentrarse en el tema de la protección de datos en el área informática, es necesario contar con un entendimiento en cuanto al tema de la regulación jurídica y cómo funciona.

El Colegio de Profesionales en Informática y computación brinda la siguiente definición del Derecho Informático:

> El Derecho informático, es una Ciencia y rama autónoma del Derecho que abarca el estudio de las normas, jurisprudencias y doctrinas relativas al control y regulación de la informática en aspectos como la regulación del medio informático en su expansión y desarrollo, y la aplicación idónea de los instrumentos informáticos que cada vez nacen más frecuentemente.
>
> La informática está estructurada por ciertas reglas y normas que regulan su fin, así pues, el Derecho en su aplicación se asiste de la misma, por ese motivo nace la informática jurídica. Crea principios y conceptos que dan autonomía propia al Derecho informático. (Zuñiga, M. citando a Bustamante, A. (2019). https://www.cpic.or.cr/Posts/Details/La%20legalidad%20del%20Derecho%20informC3%A1tico%20y%20su%20relaciC3%B3n%20con%20los%20ingenieros%20en%20TIC%E2%80%99s#)

Si bien es una definición clara y concisa se debe empezar por aclarar que el Derecho Informático no toca temas informáticos a fondo, es decir, no es necesario ser un profesional en informática para poder entender el marco jurídico que protege esta rama. No obstante, es importante el conocimiento de terminología básica y principal la cual nos llevará a una cobertura amplia en el

margen de regulación ya que, como se ha mencionado anteriormente, el mundo vive una constante evolución y globalización tecnológica la cual abarca un amplio plano el cual se encuentra en un cambio perpetuo.

Se debe entender también el concepto de informática como aquella rama de la ciencia que estudia los datos e información en formato digital incluyendo su procesamiento, transmisión y almacenamiento. Estos conceptos son reforzados por Horacio Fernández de la siguiente manera:

> Podríamos definir al derecho informático como el conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el derecho y la informática. Y que la informática es una ciencia que estudia métodos, proceso y técnicas, con el fin de almacenar, procesar y transmitir informaciones y datos en formato digital. Sin embargo, muchos consideran al derecho informático como un punto de inflexión del derecho, ya que todas sus áreas se han visto afectadas por la aparición de la computadora, Internet y la consecuente Sociedad de la Información. (Fernández, 2014, p. 1)

El objetivo principal del Derecho Informático se centra en la protección y regulación de las acciones que puedan impactar a las personas físicas y jurídicas que se relacionan con las transacciones tecnológicas que involucren una interacción informática. Si bien se han creado normas que protejan este ámbito legal, los cambios suceden a pasos agigantados, lo cual enfatiza la importancia de mantener un marco legal actualizado constantemente, incluyendo temas dentro del Derecho Penal, Laboral, Civil y Mercantil. Dentro del Derecho Penal se encuentran nuevos tipos de delitos, o modificación en la comisión de los ya existentes tales como la estafa cibernética, la extorsión o el robo de datos personales. En el Laboral se puede mencionar la inclusión de nuevas

tecnologías que impactan las labores del trabajador. En el Derecho Civil y Comercial se encuentra el tema de los contratos electrónicos, transacciones virtuales e incluso la firma digital.

Como origen, el derecho informático empezó con la inclusión de ordenadores y computadoras a la habitualidad de la vida cotidiana. Se debe recordar que la existencia del internet surgió tiempo después de la creación de la primera computadora y su creación se remonta a la época de la Guerra Fría, aproximadamente en los años 60 donde Estados Unidos inventa una red militar para intercambio de información confidencial y poder estar preparados ante un ataque Ruso. Hoy en día es complicado imaginar una computadora sin acceso a internet, tomando en cuenta la facilidad que hay a redes incluso gratuitamente en ciertos lugares. Es por esta razón que en la actualidad no se puede vincular el Derecho Informático solamente a las computadoras, si nosino a todo lo que se relacione con estas, incluyendo un gran número de dispositivos que funcionan como un ordenador y como almacenamiento de datos de manera digital.

El Derecho Informático, dentro de su desarrollo y crecimiento, se ha tenido que enfocar principalmente en los usuarios, los cuales han encontrado retos en cuanto a la protección de sus datos en la red, la seguridad y los contratos cibernéticos principalmente entre muchos otros puntos, razón por la cual se busca una protección equivalente a estos mencionados retos en un ámbito general.

Si bien los datos personales son considerados la información privada de los usuarios, desde mucho antes de la existencia de las redes se ha buscado protegerlos por cuestiones de seguridad. En Costa Rica se buscó una regulación en cuanto al trato de los datos personales con la creación de la Ley 8968, Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales en el 2011, enfatizando la importancia de la protección a la información personal, esto debido al tráfico de

datos tan impresionante que se estaba manejando a través de la internet, por esta razón se puede indicar que el Derecho Informático centra su eje de estudio en la regulación de la información.

Todo este recelo en cuanto a la protección de datos radica desde hace algún tiempo atrás, donde se ha proclamado la importancia de proteger el Derecho a la intimidad. Si bien el ser humano normalmente es un ser social, que comparte a diario con sus círculos, ya sea de trabajo, familia, amigos, se ha determinado que hay información privada que prefieren no compartir con nadie o con sus círculos más cercanos. La importancia de esta privacidad data de años atrás con la creación del liberalismo, donde se marcó la línea de acción e intervención del Estado en la vida personal de los individuos, esto conlleva a analizar el Derecho a la autodeterminación informativa la cual se mencionará más adelante.

El objetivo principal en el Derecho Informático es la unificación o conexión del mundo virtual con el mundo real, o sea, tomar esa información o datos y plasmarlos en una regulación jurídica física. Esto se logra mediante la aplicación de mecanismos comparativos los cuales puedan plasmar situaciones reales y replicarlas en las situaciones virtuales vividas en la red, esto implica que mediante la evolución tecnológica esta rama adquiere más fuerza y forma.

Se puede resaltar igualmente que esta ciencia jurídica acapara múltiples procesos vinculados a los datos per se, sin embargo, no se encuentra totalmente limitados a estos casos. Dentro de sus derivaciones de estudio se puede incluir la protección de dominios, libertad de expresión, obligaciones y responsabilidades, propiedad intelectual, derecho a la privacidad, documentos y contratos electrónicos, protección y tutela de sitios web, firma digital, comercio digital, datos personales y tutela de transacciones electrónicas entre muchos otros.

Cabe mencionar que el Derecho informático puede analizarse desde dos puntos de vista a la hora de ejecutar su debido estudio ya sea como derecho informático puro o propio y derecho informático impuro o impropio. Ante esto, Fernández cita a Guillermo Zamora de la siguiente manera:

> El derecho informático puro o propio sería aquel cuyos elementos que lo componen no tienen paralelo con otra rama del derecho, el mismo requiere del elemento tecnológico/informático, sin él no tiene características propias ni es factible su caracterización, la tecnología o el elemento informático es imprescindible para que se configure el hecho que acarrea responsabilidad, para entenderlo de otra manera, es aquel hecho que no podría configurar ilícito o daño, hace por ejemplo 30 años atrás por la inexistencia del medio para llevarlo a cabo. (Fernández mencionando a Zamora, 2014, p. 3)

Se entiende entonces por derecho informático puro o propio aquel que nace directamente del medio tecnológico mediante el cual se efectuó el acto. En otras palabras, es aquel que depende directamente de este medio mencionado para que el delito pueda llevarse a cabo. Es complicado que exista este tipo de derecho informático ya que muchos de los delitos cometidos mediante tecnologías son delitos ya existentes. Zamora también se refiere al derecho informático impuro:

> El derecho informático impuro o impropio sería aquel que tiene elementos con puntos de contacto con otras ramas del derecho y le son aplicables normativas de éstas, por ejemplo el spam (envío masivo de publicidad no deseada), ya se practicaba con otra modalidad desde hace años en EEUU e Inglaterra, la diferencia es que el correo no era electrónico sino postal, el por entonces "spammer", ensobraba su publicidad, le ponía estampillas y remitía la misma a todos aquellos que seleccionaba de la guía telefónica, como se puede apreciar el método era similar

> al spam actual, pero sin. la herramienta tecnológica/informática. (Fernández mencionando a Zamora, 2014, p. 3)

Por otro lado, se puede encontrar con más normalidad el Derecho Informático impuro o impropio, ya que este es más abierto a la hora de involucrar otras aristas y puntos relacionados a otras ramas del Derecho. Zamora menciona el spam, sin embargo, las estafas electrónicas es otro ejemplo claro, ya que las estafas son un ilícito regulado en la normativa mucho antes de que existieran las computadoras siquiera.

Otro punto importante por tratar es la relación de las diferentes ramas de conocimiento, las cuales en el transcurso del progreso tecnológico se han ido adaptando. Tanto la medicina, la ciencia, los deportes e incluso la enseñanza se han adaptado a los cambios y aclimatación que ha tenido la tecnología en las vidas de los seres humanos, es por esta razón que el derecho, con más razón, debe ser parte de este progreso y mantenerse de la mano con los cambios constantes que pueda conllevar.

Este tipo de Derecho es actual, ya que se forma y fortalece con la aparición de las nuevas tecnologías en cuanto a informática y comunicación mediante la red y así continuará, como se ha mencionado anteriormente, conforme estas tecnologías continúen progresando. Esto también vincula este tipo de derecho con la globalización tecnológica que se vive en la actualidad, ya que las redes tienen un alcance al mayor parte de la población. Gracias a este constante cambio, el derecho informático debe ser regulado por medio de normas o leyes especiales, dada su versatilidad que no permite que se plasme en normas pétreas.

Es por eso por lo que la base de este Derecho radica en la mencionada actualidad y su reconocimiento como tal. Horacio Fernández cita a Ernesto Liceda y Noemi Olivera en su trabajo "Reflexiones sobre el carácter del derecho informático":

> El derecho informático existe independientemente de su reconocimiento por parte de los actores del derecho. El uso creciente de las TICs en las sociedades hace imposible sostener por más tiempo la fantasía de que el derecho informático es sólo lo mismo que existía antes pero en versión digital, esto sólo nos aleja de la sociedad y nos niega la posibilidad de brindarle soluciones a las necesidades que aparecen a diario. Mientras parte de nosotros sigue negando la existencia del derecho informático como rama autónoma, los sujetos que se encuentran en una situación de poder en cuanto al uso y prestación de servicios de TICs contratan su personal on line en Argentina bajo el supuesto de locación de servicios; mientras discutimos si existe, la jurisdicción para resolver conflictos es, por default, California (entre otras); mientras discutimos si existe, a diario personas incapaces de hecho (ej: menores de edad) firman licencias de uso asumiendo, teóricamente, responsabilidades (podemos no saber dónde está la empresa que creó la licencia y cómo es el régimen de capacidad en la jurisdicción fijada por la misma), y los ejemplos siguen y siguen. En este trabajo presentamos lo que creemos son el objeto y el método del derecho informático y bosquejamos sus principios, esperando colaborar de este modo en la superación de discusiones infructíferas y con la apertura del nuevo debate que ansiamos, en poco tiempo, lleve a la toma de decisiones necesarias para mejorar la situación jurídica de aquellos que, en o desde

> Argentina, utilizan las TICs. (Fernández mencionando a Licedi y Olivera, 2014, p. 5)

El extracto es de suma relevancia al brindar una perspectiva en cuanto a la inclusión del Derecho Informático en la legislación actual por medio de normas actualizadas y ajustadas a la realidad, enfocando su creación a futuros posibles cambios para acaparar la mayor parte de los bienes jurídicos tutelados. Si bien cada país lleva un régimen evolutivo jurídico diferente gracias a su demografía, costumbres e historia, es de suma importancia aprovechar la revolución tecnológica, que permite una globalización al poner en manos de gran parte de los ciudadanos la capacidad de poder de obtener información a tiempo real. Es necesario que se asignen los estudios y se enfoquen los recursos en el desarrollo de esta rama, especialmente considerando el amplio desarrollo y como la humanidad depende cada día más de la virtualidad y demás tecnologías.

1.2 El Derecho a la Autodeterminación Informativa

1.2.1 Derecho a la privacidad

Antes de detallar a fondo el Derecho a la Autodeterminación Informativa es importante comentar acerca del Derecho a la Privacidad. Este último está constituido y protegido en la Declaración Universal de los Derechos Humanos, la cual establece lo siguiente:

> Artículo 12: Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataque. (Asamblea General de la ONU, 1948)

Con este artículo queda claro la protección a la vida privada, pero ¿cuál es el ámbito de esa privacidad? En sí, se podría determinar que la privacidad acapara todo el ambiente íntimo. La

privacidad se relaciona con la información que no es pertinente ni importante para otros. Podemos rescatar los Lineamientos Generales para la Clasificación y Desclasificación de la Información de las Dependencias y Entidades de la Administración Pública Federal en México, emitida por el Instituto Federal de Acceso a la Información Pública, la cual en su artículo trigésimo segundo establece una definición de lo que podemos considerar como información privada:

> Trigésimo Segundo.- Será confidencial la información que contenga datos personales de una persona física identificada o identificable relativos a:
>
> I. Origen étnico o racial;
>
> II. Características físicas;
>
> III. Características morales;
>
> IV. Características emocionales;
>
> V. Vida afectiva;
>
> VI. Vida familiar;
>
> VII. Domicilio particular;
>
> VIII. Número telefónico particular;
>
> IX. Patrimonio;
>
> X. Ideología;
>
> XI. Opinión política;
>
> XII. Creencia o convicción religiosa;
>
> XIII. Creencia o convicción filosófica;
>
> XIV. Estado de salud física;
>
> XV. Estado de salud mental;
>
> XVI. Preferencia sexual, y

> XVII. Otras análogas que afecten su intimidad, como la información genética. (Estados Unidos Mexicanos.- Instituto Federal de Acceso a la Información Pública, 2003)

Cuando se habla de privacidad e intimidad se debe considerar el fuero interno y fuero externo de la persona. En cuanto al fuero interno se establece una relación con la psiquis de la persona, sus pensamientos. Todos son libres de pensar lo que gusten y de tener su perspectiva de las situaciones que los rodean, nadie puede ser penalizado o castigado por lo que pasa en su mente, por ende, podríamos concluir que el fuero interno de las personas pertenece a la privacidad. Ahora, cuando se analiza el fuero externo, la situación podría cambiar. El fuero externo es lo que todas las personas transmiten o exteriorizan de su fuero interno. Este podría relacionarse a la materialización de los pensamientos mediante acciones, omisiones o expresiones y aquí radica la regulación y necesidad de aplicar la relevancia o importancia de estas acciones o expresiones para los demás. Si bien el domicilio, fecha de nacimiento, documentos de identificación, negocios, pertenencias y demás son de suma importancia para un aparato estatal y control para su debida actualización y regulación, los temas como creencias religiosas, preferencias sexuales, ideologías y demás no lo son. Bajo este parámetro es donde se mide la privacidad de los sujetos miembros de una sociedad.

Este tema es regulado con más profundidad en el Pacto Internacional de Derechos Civiles y Políticos, el cual establece lo siguiente en su artículo 17:

> 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.
>
> 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques. (Pacto Internacional de Derechos Civiles y Políticos ,Ley N° 4229, Costa Rica, 17 de diciembre de 1968)

Este último apoyado por la Convención Americana sobre Derechos Humanos en su artículo 11:

> 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
>
> 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.
>
> 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques. (Convención Americana sobre Derechos Humanos, Ley N° 4534, Costa Rica, 22 de noviembre de 1969)

Como se puede analizar, la información personal y privada ha tomado una importancia fundamental en cuanto a protección y tutela de los derechos. En los artículos mencionados anteriormente se hace una inclusión a la protección de la familia y el honor y a la debida protección de esa vida privada. Toda esta protección toma un escalón más en la actualidad gracias a la facilidad de acceso a la información. Si bien, como se mencionó anteriormente, la globalización tecnológica ha facilitado el acceso a la información al alcance de la mayoría de las personas, también habilita y amplía vulnerabilidades en cuanto a la vida personal, razón por la cual se ha ido integrando tutela en cuanto a la protección de datos en diversos cuerpos normativos. Uno de estos es la ley 787 de Protección de los datos personales, la cual nos brinda una definición de Autodeterminación informativa en el artículo 2, inciso a) como: el derecho que tiene toda persona a saber quién, cuándo, con qué fines y en qué circunstancias toman contacto con sus datos personales.

Esta definición la podemos complementar con las palabras de Jacopo Gamba, en su obra Panorama del derecho informático den América Latina y el Caribe quién lo indica de la siguiente manera:

> El derecho de acceso a la información pública de que se trata en este contexto, es una dimensión de la transparencia y consiste en la facultad que tiene toda persona de acceder a la información (que se refiera o no a ella misma) en poder de las instituciones públicas; es decir, es el derecho de solicitar y recibir la misma sin necesidad de acreditar que se tiene un interés legítimo ni de justificar la finalidad para la que se solicita la información. (Gamba, 2010, p. 17)

1.2.2 Autodeterminación informativa y protección de datos

Al referirse a la autodeterminación informativa queda en claro que se abarca la generalidad de los datos privados y personales disponibles a terceros. Esta es la potestad que tienen las personas de ejercer un control total ante la información privada ya antes mencionada y el empoderamiento en cuanto al manejo de esta.

La importancia de esta radica en tutelar la veracidad de los datos y la manera de compartirse. Si bien es de conocimiento general que los diferentes gobiernos y entidades estatales manejan los datos personales del pueblo, esto no significa que deban ser de conocimiento de todas las demás personas pertenecientes a la población.

Lo interesante en cuanto al derecho de la autodeterminación informativa es que, con el crecimiento tecnológico, las personas cada vez comparten más datos personales con diferentes entidades sin siquiera darse cuenta. Con el solo hecho de que participen de un juego en una red social, muchas aplicaciones se aprovechan de la ingenuidad de las personas para solicitar el acceso a sus perfiles y a su información personal que se encuentre en estos, y muchas personas se saltan esa advertencia para poder continuar con su actividad en la red.

Por esta razón es importante no solamente analizar el trato que se le da a la información personal por parte de los gobiernos, si no el mismo usuario, quien ya ha perdido la noción e importancia de la privacidad de sus propios datos.

Un caso relacionado al trato de los datos personales en Costa Rica se dio a principios del año 2020, donde el presidente Carlos Alvarado creó la UPAD (Unidad Presidencial de Análisis de Datos), dependencia gubernamental dedicada a la recolección de datos de la sociedad costarricense, desmantelada luego de que se dio a conocer el manejo de datos confidenciales del pueblo.

La UPAD se encargaba de ejercer la minería de datos con el fin de recolectar información de la realidad del país en cuanto a sus servicios, intereses de los costarricenses, crecimiento y proyecciones, sin embargo fue mal interpretado como un tipo de espionaje, lo cual no es un término correcto, ya que no se manejaba información personal sensible ni era con fines de ejercer control u opresión sobre la población, sin embargo un grave error cometido por parte del gobierno fue la falta de comunicación con el pueblo y la transparencia en cuanto a la creación y funciones de esta.

En si los datos recolectados por parte de la UPAD tenían el fin de ayudar a la reactivación económica, manejo de recursos e identificación de problemáticas sociales e intereses generales del pueblo, sin embargo, el manejo de esta dependencia estatal se percibió como algo negativo al contar con esa secrecía la cual generó clara desconfianza, temor e incertidumbre por parte de la sociedad costarricense, crucificando algo que pudo resultar muy positivo.

Incluso el Colegio de Abogados de Costa Rica decretó que la UPAD es ilegal e inconstitucional, indicando que el manejo de datos personales se puede dar únicamente bajo respaldo normativo legal contando con el consentimiento de la persona.

AúnAun así, el ministro a la presidencia, Victor Morales, se refirió al tema de transparencia, texto publicado en la página de la presidencia de Costa Rica:

> (…) aseguró que el trabajo realizado por el equipo de análisis de datos "nunca fue secreto, no estuvo en la clandestinidad, ha sido público, colgado también en una página pública, de acceso a quienes lo quieran consultar", aunque reconoció que "no tuvo el amplio alcance necesario hacia toda la población".
>
> Morales informó que hubo presentaciones "ante periodistas, la Contraloría General de la República, la sociedad civil de Puntarenas, la Organización Internacional del Trabajo, en algunos congresos especializados y universidades, ante el Banco Interamericano de Desarrollo, sindicatos, el Banco Mundial, entre otros". (2020, Trabajo a partir de la ciencia de datos ha sido en beneficio de la mayoría de las personas. https://www.presidencia.go.cr/comunicados/2020/03/trabajo-a-partir-de-la-ciencia-de-datos-ha-sido-en-beneficio-de-la-mayoria-de-las-personas/)

Asimismo, justificó la creación de la entidad haciendo referencia al crecimiento tecnológico y aplicación de elementos similares alrededor del mundo y por parte de países de primer mundo tales como Francia, Estados Unidos y Reino Unido, justificando y respaldando el crecimiento "como la elaboración de unos 35 productos en materia de seguridad, empleo, finanzas públicas, carreteras, migración, MYPIMES, desarrollo territorial, pobreza, educación, entre otros."

No obstante, a pesar de las aclaraciones, comunicaciones y demás, el pueblo perdió la confianza en el proyecto, alimentado de dudas por parte de diversas opiniones, lo cual logró que la UPAD desapareciera.

> Si bien la recolección de información constituye una necesidad imprescindible de ser satisfecha por el Estado a la hora de adoptar decisiones que conciernen a la sociedad, debe establecerse un límite que determina la legitimidad del acopio, procesamiento y transmisión de tal información, de forma que tales operaciones compatibilicen los derechos fundamentales de las personas con el fin último del Estado, cual es propender hacia la mayor realización espiritual y material posibles de los integrantes de la comunidad, con pleno respeto de los derechos que a estos correspondan. (Cerda Silva, A. 2003 p. 51)

La autodeterminación informativa llega a un punto donde se puede considerar un acuerdo entre el Estado y el usuario o poblador. Este acuerdo en si consta se basa en la adquisición de datos personales por parte del Estado, a cambio de completa discrecionalidad, seguridad y transparencia en cuanto al uso de estos datos, limitando al Estado a utilizarla con fines internos y no para usos ajenos a beneficios de su propio pueblo evitando así un acuerdo unilateral donde el estado monopolice y utilice esta sin ningún control ni mesura hacia los usuarios.

La inclusión de empresas privadas y trasnacionales ha obligado a replantear el esquema de derecho a la privacidad. A diferencia del manejo de la información por parte del Estado, las empresas privadas utilizan esta información con otros fines, tales como ventas, compras, desarrollo de productos, tipos de cliente y públicos meta entre otras.

Se debe comprender que la manera de obtener la información por parte de las empresas privadas varía mucho de la forma en que un gobierno puede hacerlo, por el simple hecho de la confidencialidad y transparencia antes citada en cuanto a la información recolectada. El Estado no puede venderle o brindarle información personal de sus habitantes a una empresa debido 0al acuerdo de protección de datos y por el simple hecho de que estaría brindando esa información

para fines de lucro. Las empresas privadas buscan incrementar su capital con base a estos datos recolectados y desarrollar su empresa a expensas de esta.

Basándose en esta inclusión de las empresas privada y la adaptabilidad a los nuevos medios de transmisión y almacenamiento de datos, surge la siguiente pregunta. ¿Se debe aplicar un nuevo derecho fundamental para explicar las leyes protectoras de datos o debemos trabajar con la protección de la privacidad que existe actualmente?

Algo constante en el ámbito jurídico es la adaptación de las leyes al contexto actual que se vive. Para esto se puede tomar como ejemplo la Ley de Censo de Población de 1982 en Alemania, la cual permitía que contenía preguntas que violaban la información personal de la población, razón por la cual el Tribunal Constitucional Alemán tuvo que realizar una revisión, llegando al punto de su anulación, protegiendo el derecho de la Autodeterminación informativo de sus pobladores. El tribunal Constitucional Alemán estimó:

> "… el derecho general de la personalidad… abarca… la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuando y dentro de qué límites procede revelar situaciones referentes a la propia vía… la libre eclosión de la personalidad presupone en las condiciones modernas de la elaboración de datos la protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitada de los datos concernientes a la persona" y que "…este derecho a la autodeterminación informativa no está, sin embargo, garantizando sin límites … el individuo tiene pues que aceptar en principio determinadas limitaciones de su derecho a la autodeterminación informativa en aras del interés preponderante de la comunidad" (Cerda Silva, A. 2003 p. 54)

Si bien, como se determinó anteriormente, es necesario que las personas compartan su información y que el Estado recolecte y almacene los datos de su población, esta recolección debe apegarse a la información debe apegarse a los datos estrictamente necesarios, dejando por fuera cualquier otra solicitud que involucre datos irrelevantes a la investigación.

Esta resolución resalta la facultad al individuo a decidir cual información puede o desea compartir, respetando las pautas antes mencionadas también en cuanto a la información necesaria para el Estado.

Estas limitaciones en cuanto a la protección de datos personales también van muy de la mano con el desarrollo tecnológico. Aún y cuando millones de datos se transmiten en la red a diario, es necesario entender hasta qué punto existe la libertad de acceder o compartir estos datos, lo cual ayuda a comprender el tribunal Constitucional de España en 1998, donde se refiere a los primeros indicios de relación informática con respecto a la autodeterminación informativa de la siguiente manera:

> "… un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática… un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona…, pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos". (Cerda Silva, A. 2003 p. 55)

Ya desde finales del siglo XX se contaba con pinceladas de inclusión de la tecnología de datos a nivel mundial, por lo cual era necesario recurrir a la protección de derechos fundamentales ante ataques informáticos y manejo de datos a nivel virtual.

Para esas épocas ya existía una noción del cauce que podía conllevar el desarrollo de la red mundial de datos, mejor conocida como la internet. Ya gran cantidad de personas contaban con ordenadores y acceso a la red desde sus casas u oficinas y la era de las transacciones virtuales estaba empezando y desarrollándose de manera desmesurada. Por esta razón se empezó a regular y a plasmar mediante jurisprudencia, sentencias que empezaran a forjar cambios en cuanto a la inclusión de los esquemas cambiantes que se referían a la protección de los datos ya mencionados.

Este fue uno de los ejemplos más claros en cuanto a la utilización de datos personales, sin embargo, también debe tomarse en cuenta que existen otros parámetros bajo los cuales se aplican, tomando como ejemplo de esto el Derecho Procesal Penal:

> La autodeterminación reviste un particular sentido hoy en día en el proceso penal, ya que a veces, para lograr los fines de la investigación de un hecho delictuoso se utilizan medios no admisibles o con violación a las reglas de la autodeterminación que también forman parte directa de las reglas del debido proceso. Un procesamiento de datos que no respete estos derechos, y utilice datos tanto sensibles como no sensibles para los efectos de la realización de perfiles de conducta para demostrar la participación criminal en un determinado hecho, debe ser considerado violatorio del debido proceso. Esto no significa que haya una carta blanca para que los delincuentes se rearmen con la herramienta informática o que estos queden fuera de la acción del Estado, sino que también en materia de derecho probatorio, y, sobre todo, cuando se trata de un procesamiento de datos con ese fin, se deben cumplir una serie de reglas y principios que forman parte integral del derecho procesal como derecho constitucional aplicado. (Gamba, 2010, p. 17)

Existen situaciones donde talvez ni siquiera se imaginaría como un detalle tan minúsculo como la utilización de algún dato podría traerse todo un proceso abajo, sin embargo, en el marco jurídico basta con un punto o una coma mal empleada para poder volcar totalmente un veredicto o perspectiva emitida en un proceso judicial. El proceso penal es un tema delicado y como ejemplo se puede utilizar la existencia de doctrinas como la del "Fruto del Árbol Envenenado", la cual hace referencia a las pruebas obtenidas de manera ilícita, estas últimas quedando totalmente fuera del contexto legal, nulas e inutilizadas para su empleo en cuanto a la deliberación de un tribunal, haciendo referencia a un árbol envenenando, ya que, un árbol envenenado daría frutos envenenados.

Este tipo de doctrina va también de la mano con el hecho de que ninguna prueba puede ser contraria a la ley, es decir, la prueba debe ser lícita. Tomando en consideración esta premisa, en el proceso se debe respetar y seguir a cabalidad la estructura legal, por lo cual en el momento que se viole el principio de protección a la información privada, ya podría poner en peligro la legitimidad del mismo. Esto no quiere decir que no se pueda utilizar medios informáticos probatorios que contengan información personal del imputado, más estos medios probatorios deben ser obtenidos de manera correcta y enfocarse en datos que el mismo acusado haya revelado o publicado.

La autodeterminación informativa es un campo amplio el cual abarca muchas aristas a la hora de emplear su debido análisis. Se puede observar cómo hay una relación tanto de parte de los usuarios, población, gobierno, empresas privadas y hasta procesos judiciales. Por esta razón es necesario comprender que este tema abarca el mismo derecho que tiene cada individuo sobre el manejo de su información y como podría afectar o influenciar otros temas que podrían estar vinculadas a este derecho, el cual será complementado y titulado con la creación del recurso de Hábeas Data.

1.3 Hábeas Data

1.3.1 Delimitación del Hábeas Data

Ya habiendo definido y comprendido el término de privacidad, el manejo de datos y diferentes normativas que los definen y protegen, se puede introducir el término de hábeas data.

Como se mencionaba anteriormente, existe información que puede ser compartida, almacenada y manejada por otras entidades, ya sea por voluntad propia o por régimen estatal. Por esta razón es importante que, las entidades que contengan esta información vinculada a las personas se encuentren de forma actualizada y veraz.

El hábeas data es el mecanismo de protección a la certeza de esa información almacenada, ya que es un recurso el cual puede ser utilizado para solicitar la remoción, corrección, protección o actualización de la información almacenada por alguna entidad. Para un mejor entendimiento se puede recurrir al siguiente concepto:

> (…) a través del hábeas data el legitimado (persona física o jurídica) puede acceder al conocimiento de sus datos personales y los referidos a sus bienes y al destino de tal información que se encuentren asentados en archivos, registros, bancos de datos u otros medios técnicos, electrónicos y ópticos, de carácter público o privado, de soporte, procesamiento y provisión de la información; y, en determinadas hipótesis (por ejemplo, falsedad o uso discriminatorio de tales datos), exigir la supresión, rectificación, actualización o el sometimiento a confidencialidad de los mismos. (Bazán, V., 2005, p.90)

En cuanto al origen del concepto, Bazán también cita los siguiente:

> La expresión "hábeas data" es utilizada a modo de empréstito terminológico de la de "hábeas corpus". Recordamos que esta última significa que "se tenga, traiga, exhiba o presente el cuerpo (ante el juez)", mientras que en el caso del "hábeas data" se quiere connotar "que se tenga, traiga, exhiba o presente los datos" (Bazán, V., 2005, p.90)

Con base a estas definiciones mencionadas se puede determinar la importancia del almacenamiento y protección de datos personales ya que, al momento de que un usuario acceda a proporcionar este tipo de información se genera automáticamente un deber recíproco en cuanto al manejo de esta. De aquí radica la funcionalidad de un recurso como hábeas data y abre las puertas para poder regular más a fondo la materia de protección de datos.

Este recurso implícitamente regula el manejo de las bases de datos donde se encuentra la información de los usuarios, ya sean públicas o privadas y sin importar el fin para el cual fueron creadas, amparado mediante la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, la cual en su artículo 2 menciona lo siguiente:

> Esta ley será de aplicación a los datos personales que figuren en bases de datos automatizadas o anuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos.
>
> El régimen de protección de los datos de carácter personal que se establece en esta ley no será de aplicación a las bases de datos mantenidas por personas físicas o jurídicas con fines exclusivamente internos, personales o domésticos, siempre y cuando estas no sean vendidas o de cualquier otra manera comercializadas. (Ley N° 8968, Costa Rica, 7 de Julio de 2011)

El aporte es de suma importancia ya que confirma y aclara el ámbito de protección que brinda el mencionado cuerpo normativo, pero también acapara la utilización posterior de los datos. Esta delimitación permite amparar el derecho a la protección de los datos no solamente al momento que se almacenan, si no a toda utilización que se le pueda dar después de ese almacenamiento, brindando seguridad a los usuarios, a que no importa lo que suceda, siempre se encontrarán protegidos ante cualquier utilización ilícita de su información.

Otro punto importante a tener en cuenta es el hecho de que el Hábeas Data siempre irá de la mano con las demás regulaciones, derechos y limitaciones relacionado a las demás normas tales como la libertad de expresión e información entre otras, priorizando y enfocando su marco jurídico en la transparencia.

Una definición que trata la mencionada ley en su artículo 3 es la de "Deber de confidencialidad" de la siguiente manera:

> Obligación de los responsables de bases de datos, personal a su cargo y del personal de la Agencia de Protección de Datos de los Habitantes (Prodhab), de guardar la confidencialidad con ocasión del ejercicio de las facultades dadas por esta ley, principalmente cuando se acceda a información sobre datos personales y sensibles. Esta obligación perdurará aun después de finalizada la relación con la base de datos. (Ley N° 8968, Costa Rica, 7 de Julio de 2011)

La misma ley delimita la responsabilidad y acredita el deber de los responsables de mantener la confidencialidad debida en cuanto a la salvaguarda de los datos de todo tipo, no solo los personales o sensibles, lo cual es de suma importancia considerando la facilidad con la cual se puede

transmitir, compartir o revelar la información, resaltando la protección posterior mencionada anteriormente.

En cuanto a los responsables que menciona la definición escrita, se debe entender que se refiere a las personas que tienen un contacto con esa información, sin importar el puesto, relación o nivel de involucramiento que se tenga con esta información. En otras palabras, se refiere a cualquier persona que tenga acceso o posible acceso a los datos almacenados. Ante esto la ley ampara la definición en el mismo artículo 3:

> Responsable de la base de datos: persona física o jurídica que administre, gerencie o se encargue de la base de datos, ya sea esta una entidad pública o privada, competente, con arreglo a la ley, para decidir cuál es la finalidad de la base de datos, cuáles categorías de datos de carácter personal deberán registrase y qué tipo de tratamiento se les aplicarán. (Ley N° 8968, Costa Rica, 7 de Julio de 2011)

En cuanto al tratamiento de datos personales, la ley hace referencia a cualquier tipo de operación que esté relacionada a los datos, sin importar la naturaleza, fin o tipo. En otras palabras, se puede interpretar la definición de tratamiento de datos como aquella que emerge por la relación de un individuo con los datos almacenados, esto se respalda con el artículo mencionado:

> Tratamiento de datos personales: cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o

> la interconexión, así como su bloqueo, supresión o destrucción, entre otros. (Ley N° 8968, Costa Rica, 7 de Julio de 2011)

1.3.2 Protección del Hábeas Data

Cuando hablamos del Hábeas Data, es imperante tomar en cuenta que este debe proteger intereses de los usuarios tomando en cuenta varios puntos de suma importancia. Lo primero y más importante es el tema relacionado al derecho a la intimidad. Se mencionó anteriormente lo que implica la intimidad, sin embargo, es necesario cubrir la relación entre ambos términos.

Con solo contar con el número de cédula de un individuo ya es posible acceder a cantidades gigantescas de información personal, incluyendo cuentas bancarias, deudas con entidades financieras y hasta lugar de residencia, relaciones familiares y estado civil entre muchas otras. Si bien, el portar el documento de identidad es algo exigido por la ley para nuestra identificación, el número de cédula es un dato que se está habituado a brindar sin el más mínimo cuidado debido al uso constante y a la costumbre. La intimidad es puesta en peligro con algo tan simple y normal como lo es compartir el número de cédula a terceros, razón por la cual es necesario incluir estos rubros bajo la protección del recurso de hábeas data.

Otro punto por tomar en cuenta en cuanto a la protección de derechos por medio del hábeas data es la libertad informática. Se mencionó lo sencillo que es para las personas acceder a la información personal con un simple dato como el número de identificación de una persona, ya sea física o jurídica, sin embargo, es importante también resaltar la facilidad de las personas para poder acceder a esos datos por medio de un ordenador o hasta desde un teléfono móvil. Se debe tomar en cuenta que el internet es una herramienta global y a la cual tiene acceso más del 50% de la población a nivel mundial. Es necesario que los recursos normativos encargados de proteger datos

consideren y tengan en cuenta la libertad de las personas de acceder a los datos al simple alcance de cualquier persona, lo cual conecta también con la recolección, procesamiento y manejo de datos.

Dentro del recurso mencionado recae responsabilidad de tomar en consideración la manera de recolectar los datos de las personas de manera correcta, mantener las bases de datos actualizadas y asimismo mantener a los usuarios al tanto de cualquier cambio que se pretenda hacer en la información de carácter sensible. Si existe algún cambio significativo en los perfiles, es necesario que las entidades que manejan los datos procedan a corregir esta información y de igual manera mantenga la comunicación de los debidos cambios con los usuarios a quienes pertenecen.

Por último, en caso de existir información que no sea de carácter público la cual el usuario desee eliminar o limitar, este tiene la potestad de solicitar su exclusión de una base de datos o de solicitar que cierta información que considere necesaria no sea compartida sin necesidad de tener una justificación.

El Habeas Data es un recurso de fácil acceso y de suma importancia para proveer a los ciudadanos de una manera eficaz de protección jurisdiccional ante un tema tan cambiante como lo es el almacenamiento de datos. Hace unos cuantos años no se imaginaba el crecimiento tan amplio que tendría el tema de la informática en cuanto a la capacidad de información que se podría guardar de manera virtual, razón por la cual recursos que sean eficaces y sencillos como lo es el Habeas Data deben ir en constante desarrollo de la mano con la evolución de las necesidades sociales, cabe resaltar que este tema es regulado en la normativa costarricense bajo el recurso de amparo por autodeterminación informativa, lo cual será detallado más adelante en la presente investigación.

Capítulo 2 – Delitos Informáticos

2.1 Definición y alcance de los Delitos Informáticos

Sin profundizar en el área del Derecho Penal en sí, es necesario tener un entendimiento básico del funcionamiento de un delito. A grandes rasgos, se sabe que el delito en si es una conducta que va en contra del ordenamiento jurídico la cual cuenta con las características de ser típica, antijurídica y culpable, compuesta por un sujeto activo (quién ejerce u omite la acción o quienes cooperan con esta) y un sujeto pasivo (quien sufre perjuicios en relación con esa conducta o terceros involucrados afectados).

Si bien se podría decir que el delito informático es aplicar la definición penal a cualquier conducta de esta índole relacionada directamente con la aplicación o utilización de un medio informático, contamos con la definición de Santiago Acurio citando a Ruiz Vadillo que indica: “es todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos”. (Acurio, S, (sin fecha), p. 9). Con esta definición se amplía el concepto para incluir no solamente la acción delictiva en relación con un medio informático, sino que también con relación a los datos que se han mencionado previamente. Ante esto es de suma importancia volver a citar a Acurio en su obra *Delitos Informáticos: Generalidades*, quien cita a Miguel AngelÁngel Dávara, quien explica de manera clara y con bases sólidas la importancia de la información, la cual será el eje principal en la presente investigación:

> “La intangibilidad de la información como valor fundamental de la nueva sociedad y bien jurídico a proteger; el desvanecimiento de teorías jurídicas tradicionales como la relación entre acción, tiempo y espacio; el anonimato que protege al delincuente informático; la dificultad de recolectar pruebas de los hechos delictivos de carácter universal del delito informático; las dificultades físicas, lógicas, y

> jurídicas del seguimiento, procesamiento y enjuiciamiento en estos hechos delictivos; la doble cara de la seguridad, como arma de prevención de la delincuencia informática y, a su vez, como posible barrera en la colaboración con la justicia. Todas ellas son cuestiones que caracterizan a este nuevo tipo de delitos y que requieren –entre otras- respuestas jurídicas. Firmes primeros pasos ya que se están dando a niveles nacionales, quedando pendiente una solución universal que, como todo producto farmacológico que se precie, se encuentra en su fase embrionaria de investigación y desarrollo" (Acurio, sin fecha, p. 6)

Tal y como se mencionó con anterioridad, no se puede limitar el Derecho Informático a los ilícitos cometidos solamente mediante una computadora o mediante la red, si nosino también por otros medios informáticos o telemáticos. También es importante estar conscientes que estos delitos pueden ser de ámbito civil o penal.

Entendiendo la importancia de la información y los datos como bien tutelado, podemos entonces detallar y fortalecer la definición de delitos informáticos, haciendo referencia a la conducta típica, antijurídica y culpable, que se realice mediante el involucramiento y manipulación de datos, relacionada con medios informáticos. Al concatenar esta definición se debe también resaltar la importancia de la tipificación como parte de la teoría del delito, lo cual complica el tema en muchas normativas internacionales al no existir una un cuerpo normativo que respalde el concepto como tal de delito informático, no obstante, ahí radica la importancia de la constante actualización en las ramas del derecho a nivel mundial.

Cuando se habla de la materia penal en relación con el Derecho Informático, se debe tomar en cuenta la dificultad que ha tenido la debida identificación y tipificación ya que su regulación ha

sido diferente alrededor del mundo, esto ya que alrededor del mundo existen diferentes normas, penas e ilícitos.

Entre otros aportes a esta problemática se puede mencionar el paso al que avanzan las tecnologías en comparación a la implementación del marco jurídico a nivel mundial y no solamente tomar en cuenta esa velocidad de cambio, si no también de ejecución delictiva. Se puede poner como ejemplo un robo a un banco. La ejecución del crimen en forma física requiere presencia de los delincuentes y una planeación totalmente diferente en cuanto a comisión y preparación. Los asaltantes deben presentarse, ocultar su identidad, llevar sus respectivas bolsas de dinero y demás. Por otro lado, un robo cibernético no es necesaria una presencia física en muchos de los casos.

Fernández en su libro “Manual de Derecho Informático“ cita a Téllez Valdés para describir las características de los delitos informáticos:

> a) Son conductas criminales de cuello blanco, porque sólo un determinado número de personas con ciertos conocimientos técnicos puede llegar a cometerlas.
>
> b) Son acciones ocupacionales, porque en muchas veces se realizan cuando el sujeto se halla trabajando.
>
> c) Son acciones de oportunidad, porque se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
>
> d) Provocan serias pérdidas económicas.
>
> e) Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

> f) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
>
> g) Son muy sofisticados.
>
> h) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
>
> i) En su mayoría son imprudencias y no necesariamente se cometen con intención.
>
> j) Ofrecen facilidades para su comisión los menores de edad.
>
> k) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
>
> 1) En algunos casos siguen siendo ilícitos impunes ante la ley. (Fernández, 2014, p. 195)

En el mismo tema es determinante comprender diferentes características para su debida identificación. En primera instancia se debe entender que los delitos informáticos no son de acceso a cualquier persona, ya que para poder ejecutarlos se necesita un amplio conocimiento en el área de la informática o la debida complicidad en el medio. También este tipo de delitos es cometido como brechas en seguridad de protección a los usuarios, en otras palabras, el delincuente busca oportunidades mediante la vulnerabilidad del sistema. Uno de los detalles más importantes es la inmediatez y accesibilidad para la comisión del delito, ya que el delincuente puede acceder a la información, realizar el hecho delictivo desde la comodidad de su hogar o sitio con acceso a la red, y en cuestión de segundos, realizar lo necesario para concluir su objetivo sin importar el día o la hora. Ante esta circunstancia, se dificulta rastrear al delincuente de manera inmediata, y, aún y

cuando existen métodos para determinar de donde se realizó el ataque, normalmente el conocimiento de estos es tan amplio que saben cómo ocultarse.

Ahora bien, debido a la complejidad en cuanto al conocimiento necesario y la ejecución de la conducta delictiva, en su gran mayoría este tipo de delitos son dolosos. Las personas que los realizan están conscientes de lo que están haciendo y poseen el debido conocimiento de saber las repercusiones que puede conllevar, esto excluyendo, claramente, a los cómplices o personas que puedan engañar para que realice el delito en su lugar.

Cabe indicar que como se ha mencionado en varias ocasiones, varios delitos informáticos están regulados bajo otras figuras ya existentes sin embargo hay ilícitos muy específicos los cuales Dentro de estos delitos se contempla en su mayoría situaciones relacionadas de la siguiente manera (Estos delitos se verán con más detalle más adelante):

1. Daño informático
2. Fraude informático
3. Falsificación de documentos electrónicos.
4. Delitos contra la privacidad y daño a la imagen
5. Robo o suplantación de identidad
6. Espionaje
7. Extorsión
8. Acoso
9. Pornografía infantil

2.2 Daño informático

El daño informático se trata de dañar un sistema informático ya sea con el fin de robar información o de provocar perdidas o perjuicios a una empresa o persona. Un ejemplo de daño informático se puede lograr mediante un virus con el cual se deshabiliten los sistemas de cómputo de una empresa con el fin de alterar su producción.

Es necesario entender que existen dos sistemas que deben regularse en este sentido ya que existe la destrucción física y la destrucción virtual de un sistema. En cuanto a la destrucción física se pude hacer referencia al daño directo y físico que se le pueda dar a un equipo de cómputo, discos duros, servidores y dispositivos de almacenamiento, entre otros, que maneje datos o información de algún valor o importancia. Por otro lado, la destrucción virtual se refiere directamente a la información almacenada la cual puede ser dañada de diversas formas, desde el mencionado virus informático hasta la destrucción de los datos virtualmente imposibilitando su recuperación o generando un perjuicio en cuanto a la productividad del dueño o administrador de la base de datos.

Debido a estos tipos de daños, es imperante identificar y delimitar el bien jurídico que se protege a la hora de hablar de daño informático. El eje principal cuando se habla de este delito es el procesamiento de los datos los cuales son manejados por la empresa o administrador de estos últimos. La razón principal detrás de esta delimitación se enfoca a que, no se puede considerar un daño informático si la información almacenada sigue funcionando de manera correcta o para los fines principales. Como ejemplo se puede indicar un caso donde se dañe un disco duro, pero se pueda recuperar la información ya que hubo daño físico del dispositivo de almacenamiento, pero el bien jurídico que es la información guardada se mantiene intacta. Ahora bien, no se debe malinterpretar esta premisa considerando que si hay un daño físico no sería punible, todo lo

contrario, la regulación jurídica costarricense tipifica en el Código Penal el delito de daño y de daño agravado en sus artículos 228 y 229:

Artículo 228.- Daños

Será reprimido con prisión de quince días a un año, o con diez a cien días multa, al que destruyere, inutilizare, hiciere desaparecer o dañare de cualquier modo, una cosa, total o parcialmente ajena.

Artículo 229.- Daño agravado

Se impondrá prisión de seis meses a cuatro años:

1) Si el daño fuere ejecutado en cosas de valor científico, artístico, cultural o religioso, cuando, por el lugar en que se encuentren, se hallaren libradas a la confianza pública, o destinadas al servicio, la utilidad o la reverencia de un número indeterminado de personas.

2) Cuando el daño recayere sobre medios o vías de comunicación o tránsito, sobre puentes o canales, sobre plantas de producción o conductos de agua, de electricidad o de sustancias energéticas.

3) Cuando el hecho fuere ejecutado con violencia en las personas o con amenazas.

4) Cuando el hecho fuere ejecutado por tres o más personas.

5) Cuando el daño fuere contra equipamientos policiales.

6) Cuando el daño recayera sobre redes, sistemas o equipos informáticos, telemáticos o electrónicos, o sus componentes físicos, lógicos o periféricos. (Así adicionado el inciso 6) anterior por el artículo 2° de la Ley N° 9048 del 10 de julio de 2012, "Reforma de la Sección VIII, Delitos Informáticos y

> Conexos, del Título VII del Código Penal") (Ley N° 4573, Costa Rica, 4 de mayo de 1970)

Como se puede observar, el daño a equipo informático se añadió a la norma hasta la creación de la ley 9048 y se debió añadir el artículo 229 bis para brindar el respaldo jurídico necesario al delito de daño informático, ya que antes solamente se hablaba de bienes muebles e inmuebles en general.

> Artículo 229 bis.- Daño informático.
>
> Se impondrá pena de prisión de uno a tres años al que sin autorización del titular o excediendo la que se le hubiera concedido y en perjuicio de un tercero, suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos.
>
> La pena será de tres a seis años de prisión, si la información suprimida, modificada, destruida es insustituible o irrecuperable.
>
> (Así adicionado por el artículo único de la Ley "Adición de los artículos 196 BIS, 217 BIS y 229 BIS al Código Penal, Ley N° 4573 para reprimir y sancionar los delitos informáticos"; N° 8148 de 24 de octubre del 2001. Posteriormente reformado en la forma indicada por el artículo 1° de la ley "Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal"; N° 9048 del 10 de julio de 2012,) (Ley N° 4573, Costa Rica, 4 de mayo de 1970)

Estos artículos brindan el fundamento necesario cuando se hace la diferenciación entre daño y daño informático, basándose en el bien jurídico tutelado mencionado anteriormente. La inclusión

del delito en específico hace alusión a la ampliación del tema manifestando la necesidad de cubrir la información virtual o el espacio cibernético, ya que al tratarse solo bienes físicos no se podía cubrir las nuevas necesidades en cuanto a protección de equipos informáticos en específico o su debido contenido. Es de suma importancia también resaltar el artículo 229 bis ya que hace mención del hecho de que la información debe ser insustituible o recuperable, por lo cual, como se hizo mención anteriormente, si existe una manera de respaldo o se puede recuperar la información, el tipo penal no pertenecería a este rubro y, en el caso de que el daño hubiera sido solamente físico, aplicaría la pena indicada bajo el tipo de daño agravado.

Un punto que hay que tomar en cuenta es que existen muchas formas de cometer el delito de daño informático mediante la virtualidad. Una de las principales formas que utilizan los delincuentes es mediante virus informáticos. Este último es un programa diseñado con el fin de alterar, robar, destruir o copiar información en un sistema informático y se puede transmitir por medio de la red fácilmente. Los virus pueden transmitirse mediante dispositivos de almacenamiento o por medio de descargas generadas en la red, es por esta razón que siempre se recomienda tener un antivirus actualizado y no ingresar a sitios web sospechosos ya que con un simple click se podría descargar un software maligno que destruya la información. En estos se estaría frente a un gran reto ya que es extremadamente complicado poder determinar donde fue originado el virus o quién lo puso ahí. Actualmente existen programas de rastreo, pero a cómo evolucionan estas tecnologías, también evolucionan los métodos para mantener a los responsables ocultos, ya sea mediante VPNs, ocultando sus IPs o identificaciones de los sistemas de cómputo utilizados. Los VPNs son programas virtuales creados para proteger la privacidad e incluso simular tener una ubicación la cual no es actual, su nombre viene de sus siglas en inglés Virtual Private Network o Red Privada Virtual. Por esta razón es importante mantener el sistema normativo actualizado de la mano con

las investigaciones y progreso en cuanto a detección y erradicación de los delitos tales como el daño informático.

2.3 Fraude Informático

El fraude informático consiste en perjudicar a un tercero con el fin de obtener un beneficio económico mediante medios informáticos. Adentrándose más en el tema, se identifica la necesidad de que exista un perjuicio patrimonial y que no debe confundirse con una tentativa o preparación para efectuar el ilícito. Con esto se debe aclarar que el objetivo del fraude debe ser cumplido para poder ser penalizado.

Otro punto importante por tomar en consideración es el hecho de que el fraude informático se relaciona directamente con otros comportamientos cibernéticos que ayudan a que se cumpla su ejecución.

La utilización del término se mantiene en constante debate con la estafa informática, ya que varias legislaciones consideran a la estafa como un engaño y el fraude como manipulación de datos para cumplir su cometido. Normalmente el fraude informático se ve desglosado en las siguientes formas más conocidas para cometerlos:

a. Phishing: Este tipo de fraude donde la fuente a la cual se accede se hace pasar por una fuente confiable también conocido como “suplantación de identidad”. Normalmente se comete por medio de correo electrónico donde el emisor modifica su información engañando al receptor quien piensa que es un medio conocido el que lo contacta. El emisor mediante este método engaña al receptor para que comparta información confidencial tal y como cuentas o tarjetas bancarias entre otras. Cuando el usuario recibe este correo normalmente mediante el temor infundido les hacen creer que sus datos, información o

cuentas, por poner varios ejemplos, se encuentran en peligro y les indican que deben acceder a un hipervínculo para poder acceder con sus credenciales (usuario y contraseña), información que es transmitida a los delincuentes inmediatamente y pueden acceder al sistema con los credenciales robados. Normalmente esto sucede con entidades bancarias, entonces, cuando el usuario decide acceder al sistema, los delincuentes roban su información y pueden hasta saquear sus cuentas.

Un aspecto interesante del phishing es el hecho de que no solamente son necesarios los conocimientos técnicos en cuanto a diseñar un sistema que transmita los datos a los delincuentes, si no que deben conocer la manera en que funciona la mente del usuario, ya que gran porcentaje de éxito a la hora de cometer el delito depende de la manera de actuar del este manipulándole para que sea él mismo quien comparta la información.

b. Carding: Este es un tipo de estafa donde el delincuente utiliza una tarjeta de crédito/ débito, cuentas o movimientos bancarios sin autorización del usuario y sin que este se percate. Esa información en muchas ocasiones es obtenida por medio del phishing o páginas de ventas fraudulentas. Por esta razón se recomienda que cualquier compra por internet se realice por medio de un servidor protegido y encriptado, y a su vez que se realicen en sitios de prestigio y renombre.

   No obstante, se debe recordar que aún y cuando una empresa de ventas en línea cuente con un servidor encriptado y mantengan prestigio, las vulnerabilidades informáticas siempre son un riesgo, por lo cual siempre es responsabilidad del usuario monitorear sus transacciones y asegurarse de que sus cuentas o tarjetas no sean utilizadas indebidamente. Se recomienda en el momento de detectar alguna transacción sospechosa, contactar al

emisor de la tarjeta o cuenta bancaria inmediatamente e incluso proceder a la cancelación de la cuenta o tarjeta de manera inmediata.

c. Pharming: es un sistema bastante similar al phishing, pero con la diferencia que en el pharming se realiza una copia idéntica o muy similar a una página de internet confiable. Esta página de internet puede instalar un virus en el equipo para poder obtener la información requerida o almacenar los credenciales de los usuarios.

   Otra diferencia en el pharming con respecto al phishing es que el engaño se produce por medio suplantación de protocolos de búsqueda en la red, los cuales dirigen al usuario a la página falsa ocasionando que en la mayoría de los casos estos ni siquiera se percaten que la página es una réplica a la original.

   Una manera de proteger a los usuarios contra el pharming es mediante la verificación del sitio web al que se está accediendo y asegurándose que siempre esté encriptada mediante el protocolo HTTPS.

En Costa Rica se modificó el delito de “fraude informático” a “estafa informática” por medio de la Ley N° 9048 del 10 de julio de 2012, publicada en el Alcance 172 a La Gaceta N° 214 del 06 de noviembre de 2012, con el fin de especificar y delimitar acciones que están contempladas en el primer tipo, esto lo explica la sala en su sentencia:

> (…) el fraude informático, se creó mediante Ley N° 8148 de 24 de octubre de 2001, publicado en La Gaceta de 21 de noviembre de 2001. La estafa informática, amplió su configuración típica, al incluir acciones que no estaban en aquel otro delito, porque integró la acción de "manipular o influir en el ingreso" pero mantuvo el " influir en el procesamiento o en el resultado de los datos". Asimismo, para los casos en que se trate de sistemas de información bancaria, como es este asunto, elevó la

> pena mínima, a cinco años de prisión, (párrafo segundo del artículo 217 bis del Código Penal), en lugar del año que tenía como extremo menor, el derogado fraude informático (Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José, 08-016097-0042-PE, 2015)

La Sala Tercera de la Corte también realiza un pronunciamiento importante al especificar los delitos que incluye el fraude, los cuales no deberían estar contemplados dentro de la estafa.

> La palabra "fraude" hace referencia a la realización de un modus operandi que caracteriza a un determinado comportamiento, el cual se encuentra encaminado, orientado y encauzado a la obtención de un beneficio patrimonial antijurídico, propio o para un tercero, utilizando para ello el error y el ardid, acciones que resultan ser en definitiva, falsas y engañosas. Por su parte, el fraude informático no representa cualquier tipo de acción fraudulenta que surge al utilizar un medio informático, sino únicamente cuando se refiere al perjuicio económico ocasionado a consecuencia del fraude. Entre el fraude informático y la estafa informática existe una relación de género a especie, ello presupone que toda estafa informática es un fraude informático, pero no todo fraude informático es una estafa informática. Es preferible que en lugar denominar fraude informático al ordinal 217 del Código Penal, se utilice la denominación de "estafa informática", para delimitar de mejor manera el concepto, logrando diferenciarlo del fraude informático, vocablo por demás amplio que incluye una diversidad de conductas como lo son la propia estafa, el sabotaje, los daños y el hurto informático. (Sala Tercera de la Corte, 02-003942-0647-PE, 2009)

La norma costarricense tipifica los delitos de estafa informática mediante el artículo 217 bis del Código Penal:

> Artículo 217 bis.- Estafa informática
>
> Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.
>
> La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.
>
> (Así adicionado por Ley "Adición de los artículos 196 BIS, 217 BIS y 229 BIS al Código Penal, Ley N° 4573 para reprimir y sancionar los delitos informáticos"; ley N° 8148 de 24 de octubre del 2001. Posteriormente reformado en la forma indicada por el artículo 1° de la ley "Reforma de la Sección VIII, Delitos Informáticos y

> Conexos, del Título VII del Código Penal"; ley N° 9048 del 10 de julio de 2012,) (Ley N° 4573, Costa Rica, 4 de mayo de 1970)

2.4 Falsificación de documentos electrónicos

Con la aparición de la firma digital y sumando el involucramiento cibernético en las labores diarias de los ciudadanos, surge la necesidad de determinar el delito de falsificación de documentos electrónicos.

Normalmente cuando se habla de falsificación de documentos, en su generalidad ha sido tipificada alrededor del mundo haciendo referencia a cualquier alteración, modificación, simulación o falsificación de un documento ya sea parcialmente o en su totalidad. En otras palabras, el delincuente puede basarse en un documento existente o en la creación de uno totalmente nuevo.

La protección en cuanto a este delito es de suma importancia ya que, en la actualidad, la base documental es un medio probatorio bastante confiable y brinda un respaldo a transacciones, acuerdos contractuales y bases de datos entre muchos otros.

La enciclopedia jurídica nos brinda una definición amplia de documento:

> (…) en sentido lato denomínase documento a todo objeto susceptible de representar una manifestación del pensamiento, con prescindencia de la forma en que esa representación se exterioriza.
> Por lo tanto, no sólo son documentos los llevan signos de escritura, sino también todos aquellos objetos que como los hitos, planos, marcas, contraseñas, mapas, fotografías, películas cinematográficas, etcétera, poseen la misma representativa. (Rogers, David. 2020. Enciclopedia jurídica. http://www.enciclopedia-juridica.com/d/documento/documento.htm)

En este extracto se detalla ampliamente la diversidad de documentos que pueden existir, cuyo principal factor común o punto vinculante es la manifestación de pensamiento. El documento normalmente es un medio por el cual se expresa voluntad o plasma esa manifestación de manera física.

A través de la evolución histórica de la humanidad se la falsificación de documentos ha encontrado facilidades y complicaciones. En épocas antiguas los documentos se escribían a puño y letra con la firma de su emisor como principal medio identificador. Escrituras, traspasos, compraventas y hasta acuerdos internacionales basaban su autenticidad en el papel y tinta. Incluso nació la figura del grafólogo, quién es un experto que se encarga de analizar los rasgos en la escritura para determinar quién escribió un documento e incluso rasgos propios de su personalidad.

Conforme los tiempos fueron cambiando, se inventaron nuevas formas de documentación, entre esas la máquina de escribir y la computadora. Con el desarrollo de estas últimas también se crearon otros dispositivos tecnológicos que permitían falsificar no solo documentos, si no también billetes con valor monetario. Entre estos dispositivos estuvieron el desarrollo de fotocopiadoras, las cuales generaban una réplica del documento original, permitiendo no solo adulterarlo si no crear documentos desde cero. Ahora bien, aún y cuando una fotocopiadora podía generar una copia, la firma continuaba siendo la principal problemática para los delincuentes.

Cuando se habla de la falsificación de documentos es importante reafirmar el hecho de que esos documentos deben ser puestos en circulación o cumplir el fin para los cuales se falsificaron, esto lo confirma la sala de Casación Penal de Cartago por medio de la jurisprudencia:

> Para que el delito de falsedad ideológica (…) o falsificación de documento (…) se configuren, es preciso que dicha acción “pueda resultar perjuicio”, lo cual sólo

> ocurre cuando el documento es puesto en circulación o es usado. De modo que, si el sujeto no lo puso en circulación o no lo usó, no se configuran esos ilícitos. Por su parte, el uso de documento falso (…), consiste en el empleo de un documento cuya falsedad puede ser en su contenido o su materialidad, por lo que el uso de documento falso abarca el uso tanto de los documentos queque, falsificados o adulterados, o bien que siendo originales contienen declaraciones falsas. (Tribunal de Casación Penal de Cartago, 06-200097-0454-PE, 2011)

Con los avances tecnológicos y la era del internet, se ha llegado a tramitar los llamados documentos electrónicos, haciendo referencia a aquellos cuyo soporte, creación y almacenamientos son mediante un dispositivo electrónico. Estos son conocidos también como documentos digitales y se caracterizan también por contener un contenido codificado, brindándole seguridad y autenticidad.

Por otro lado, la firma digital es un instrumento virtual el cual identifica al creador del documento mediante formulasfórmulas matemáticas de encriptación. Al contar con dos tipos de claves y mediante mecanismos criptográficos, la firma digital logra substituir la firma física en documentos de este índole.

Aún y cuando estos documentos electrónicos cuenten con sus debidos métodos de seguridad, se encuentran propensos a su falsificación mediante métodos cibernéticos. En la legislación costarricense se sigue utilizando la regulación mediante el delito de falsificación de documentos, sin embargo, cada día son más las personas que incursan en la firma digital y los documentos electrónicos, por lo cual deberá regularse con más detalle la falsificación de este tipo de documentos. Esta normativa penaliza en el Código Penal la falsificación de documentos tanto públicos, en el artículo 366, como privados en su artículo 368.

2.5 Delitos contra la privacidad y daño a la imagen

Anteriormente se cubrió de manera amplia la importancia de la privacidad y la imagen, así como el amparo ante este derecho. Los delitos contra estos derechos se han incrementado y ampliado con la creación de los nuevos métodos de comunicación vigentes. En la actualidad basta con unos cuantos segundos para transmitir imágenes y documentos mediante alguna aplicación de mensajería utilizada en un teléfono móvil con el solo requisito de tener acceso a internet. Si bien la privacidad y la imagen han sido protegidas desde hace mucho tiempo atrás, esta protección se ha tenido que magnificar y perfeccionar con el fin de cubrir la evolución tecnológica.

Se han dado situaciones a nivel nacional donde la difusión de imágenes se ha convertido en un problema difícil de controlar. En el año 2020, en Costa Rica ocurrió una situación donde más de 3000 usuarios de una aplicación llamada Telegram (aplicación de mensajería instantánea la cual funciona por medio del Internet) compartían fotografías y videos de mujeres desnudas sin su consentimiento. Este fue un caso bastante controversial, por varias razones en general. La primera es que los usuarios de dicha aplicación podían ocultar su nombre verdadero y número de teléfono, por lo cual identificarlos con solo tener acceso al grupo era prácticamente imposible. La segunda premisa caía en el análisis de culpabilidad ya que, se debía identificar, de los miembros de ese grupo, quienes habían compartido el material sin autorización. Por último, se encuentra el análisis de la cantidad de casos existentes actualmente. Ese fue un caso muy mediático por contener tantas personas involucradas, tanto los que cometieron el ilícito como las víctimas, pero diariamente a nivel mundial rondan miles de casos.

Por esta razón se ha ido regulando estas situaciones en la normativa y en Costa Rica se penaliza de uno a tres años este delito. La normativa costarricense fue agregada al Código Penal, en su artículo 196 bis de la siguiente forma:

Será sancionado con pena de prisión de uno a tres años quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos.

La pena será de dos a cuatro años de prisión cuando las conductas descritas en esta norma:

a) Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

b) La información vulnerada corresponda a un menor de edad o incapaz.

c) Las conductas afecten datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona.

No constituye delito la publicación, difusión o transmisión de información de interés público, documentos públicos, datos contenidos en registros públicos o bases de datos públicos de acceso irrestricto cuando se haya tenido acceso de conformidad con los procedimientos y limitaciones de ley.

> Tampoco constituye delito la recopilación, copia y uso por parte de las entidades financieras supervisadas por la Sugef de la información y datos contenidos en bases de datos de origen legítimo de conformidad con los procedimientos y limitaciones de ley." (Ley N° 4573, Costa Rica, 4 de mayo de 1970)

Es necesario resaltar con respecto a ese artículo la referencia a la información que sea de carácter público, ya que como se mencionó en el capítulo anterior, existe información que, por su razón y propósito, pierde su carácter confidencial y privado.

2.6 Robo o suplantación de identidad

El delito de robo o suplantación de personalidad es un ilícito que ha crecido exponencialmente con la aparición de las redes sociales, ya que estas han facilitado los pasos para lograr cometerlo. Este se comete en el momento que una persona se hace pasar por alguna otra con el fin de cometer algún fraude, obtención de información, acoso o incluso abuso sexual a personas mayores de edad o menores.

Haciendo mención a las redes sociales, un ejemplo muy claro y bastante común en la actualidad es la creación de perfiles falsos en redes sociales. Esos perfiles falsos pueden ser utilizados para ocasionar diferentes daños. En ocasiones, esto podría conllevar a dos o más víctimas involucradas. En estos casos contaríamos con tres partes, la primera sería la persona a quién roban la identidad, la segunda sería el sujeto que roba la identidad creando el perfil falso y por último, si ocasionan daños a un tercero, implicaría la relación directa de una víctima a quién engañen con ese perfil falso.

Existen casos mucho más delicados a los cuales podría llevar este robo de identidad tales como el grooming. También conocido como ciberacoso sexual, este consiste en la utilización de un perfil

falso para poder tener un acercamiento con un menor de edad con el fin de ganar su confianza y poder obtener una cita con este logrando un secuestro, abuso sexual o hasta producción de pornografía infantil.

Normalmente los delincuentes se hacen pasar por figuras públicas que tengan afinidad con los niños, parientes cercanos o incluso otros niños, logrando con esto mostrar una imagen que inspire más confianza y poder obtener información muy delicada como domicilio, vínculos familiares y cercanía con miembros de la familia, entre otros.

La suplantación de identidad fue incorporada en el Código Penal costarricense en su artículo 230, con penas de uno a tres años e involucra la identidad no solamente de una persona física, si no también una persona jurídica o marca haciendo referencia a la utilización de esa identidad en una red social, internet, medio electrónico o tecnológico de información.

2.7 Espionaje

Al tener un acercamiento más amplio con el término “espionaje” se puede determinar que no solamente es la acción de acechar u observar a alguien o algo, si no que esto debe ser con un fin de obtener información secreta con respecto a alguna acción, comportamiento o información confidencial de importancia para quién espía. Esta información puede ser de más gravedad si lo que se intenta es conseguir información confidencial de una empresa o un país en general. En épocas de guerra el espionaje era utilizado para conseguir información acerca de estrategias o técnicas que iban a ser utilizadas por los países enemigos, brindando al bando del espía una ventaja a la hora de un enfrentamiento.

Estas técnicas no solo se han utilizado en guerras, en los deportes también se han dado casos donde se espía al equipo rival para determinar cómo contrarrestar la estrategia que van a poner en

práctica. Misma situación sucede con las empresas, ya que una manera de conocer las movidas que va a realizar la competencia es mediante el espionaje para poder anticiparse ante cualquier sorpresa que puedan dar.

El bien jurídico protegido con el delito de espionaje es la información o más específico, el secreto y la violación de este. El secreto puede ser definido como información confidencial conocida por pocas personas la cual puede ocasionar perjuicio en caso de ser divulgada a un círculo más amplio de personas.

El espionaje informático es el concepto de espionaje adaptado a las nuevas tecnologías de información. Antes un espionaje era llevado a cabo por una persona especializada en el engaño quién podía hacerse pasar por una persona de confianza, o simplemente por una persona que tenía capacidades de observación y análisis mediante el sigilo. Hoy en día el espionaje informático es llevado a cabo por personas con amplios conocimientos en informática, conocidos como Hackers. El hacking es la acción de estos hackers quienes, mediante códigos complejos y conocimientos de vulnerabilidades informáticas, pueden obtener información de sitios web encriptados y protegidos ya sea gubernamentales o empresariales.

Existe una línea muy delgada en la comisión del delito y esta se marca en la acción de espionaje y con qué fin se utiliza ese acceso a la información privada. La Revista Chilena de Derecho y Tecnología brinda el siguiente extracto:

> Si el espionaje informático supone tanto acceder a como conocer (indebidamente) los datos contenidos en un sistema informático, su obtención implicaría, en principio, una conducta ulterior y diferenciada del solo acceso y conocimiento. Según su sentido natural y obvio (véase el del Diccionario de la lengua española),

> obtener es «alcanzar, conseguir y lograr algo que se merece, solicita o pretende» o «tener, conservar y mantener» una cosa. En esa línea, si bien podría estimarse que quien conoce los datos en algún sentido los obtiene, los casos relevantes de obtención son aquellos que implican almacenar e incluso transferir datos de un sistema informático a otro. Por ende, respecto del espionaje informático, la obtención de datos sería un caso de agotamiento del delito. (Vera, J. y Mayer, L. Revista Chilena de Derecho y Tecnología vol. 9, 2020, p.227)

De esta manera surge el análisis donde se debe encuadrar el delito en el tipo correcto, tomando en consideración que solo acceder a información confidencial no podría ser tomado en cuenta en el caso de espionaje, si no el almacenamiento y divulgación de esa información, perjudicando a el autor original o quien guardaba esa información en modo secreto.

En la normativa costarricense fue incluido el espionaje informático en el año 2012 en el Código Penal, artículo 231 indicando:

> Se impondrá prisión de tres a seis años al que, sin autorización del titular o responsable, valiéndose de cualquier manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle información de valor para el tráfico económico de la industria y el comercio. (Ley N° 4573, Costa Rica, 4 de mayo de 1970)

2.8 Extorsión

El Código Penal de Costa Rica regula la extorsión en su artículo 214:

> Será reprimido con pena de prisión de cuatro a ocho años al que para procurar un lucro obligue a otro, con intimidación o con amenazas graves, a tomar una disposición patrimonial perjudicial para sí mismo o para un tercero.
>
> La pena será de cinco a diez años de prisión cuando la conducta se realice valiéndose de cualquier manipulación informática, telemática, electrónica o tecnológica. (Ley N° 4573, Costa Rica, 4 de mayo de 1970)

La extorsión es aquel delito donde se logra la manipulación sobre una persona para que esta efectúe un ilícito o una acción que impacte a un tercero o a si misma, obteniendo un beneficio económico o de otra índole, mediante violencia o intimidación. El delito de extorsión protege tanto a la libertad y la integridad física del individuo extorsionado como el bien patrimonial que se pretende atacar u obtener mediante la generación del ilícito, por esta razón se admite la tentativa según indica el Tribunal de Apelación de Sentencia Penal citando a Creus y Boumpadre:

> "La tentativa se determina por la formulación intimidatoria de la exigencia a través del comienzo de la formulación de la amenaza o de la falsa invocación de autoridad u orden de ella. Aquí sí es necesario examinar con detenimiento la idoneidad del procedimiento intimidatorio empleado, pues, si el fracaso de la intimidación se origina en su inidoneidad, estaremos ante una tentativa de delito imposible (art. 44, Cód. Penal), en tanto que, si el fracaso depende de otras causas ajenas a la voluntad del agente, siendo el medio idóneo para intimidar, estaremos ante una tentativa de delito imposible (art. 44, Cód. Penal), en tanto que, si el fracaso depende de otras causas ajenas a la voluntad del agente, siendo el medio idóneo para intimidar, estaremos ante la figura principal de tentativa (art. 42, Cód. Penal). Se ha sostenido

> que esa idoneidad depende de la posibilidad intimidatorias del procedimiento utilizado, según el criterio del hombre medio, lo cual no deja de ser exacto, siempre y cuando no se tome ese criterio como medida absolutamente objetiva: la idoneidad depende de las circunstancias concretas de cada caso, tanto de las subjetivas que atañen a la particular víctima, como de las objetivas que rodean el hecho y que, como tales, pueden influir sobre esa subjetividad; pero, como lo vimos en el delito de amenazas, el hecho de que la víctima no se haya intimidado de manera efectiva nada dice contra la idoneidad del medio intimidatorio utilizado, si es que pudo haber producido ese estado en un individuo corriente: la gravedad de las amenazas en correlación con los bienes jurídicos que pueden ser atacados por el delito asumirá aquí importancia, según dijimos precedentemente" (cf. CREUS, Carlos; BUOMPADRE, Jorge Eduardo. Derecho Penal. Parte General. Buenos Aires, Astrea, 7° edición revisada y actualizada, Tomo I, 2007, pp. 493 a 494.) (Tribunal de Apelación de Sentencia Penal III Circuito Judicial de Alajuela San Ramón, 00188 - 2016, 2016)

La extorsión podría estar incluida dentro de los delitos de estafa, sin embargo, se debe individualizar por los bienes jurídicos que tutela, entre estos el peligro ante la integridad del extorsionado, tomando en consideración que, sin esa violencia o intimidación mencionada, no se podría considerar como este delito en específico.

2.9 Acoso cibernético

El acoso ha sido una conducta bastante normalizada desde tiempo atrás en todas las sociedades del mundo. Normalmente el acoso es una problemática por la cual pasan muchos jóvenes en su infancia y adolescencia, y en muchos casos se debe a una presión social o estereotipos marcados

en contra de una aceptación a la diversidad de géneros, gustos, comportamientos o estilo de vida entre muchos otros, sin embargo, no se debe ignorar la existencia de este en la vida de las personas de cualquier edad. El acoso cuenta con varias subdivisiones tales como la índole sexual, verbal, social, físico, psicológico y cibernético.

El acoso en general puede resultar en una problemática de gran magnitud a nivel mundial y especialmente entre personas menores de edad, donde se está formando y desarrollando la persona, lo cual podría crear marcas y trastornos psicológicos tanto en el momento como años después de experimentarlo. Se ha demostrado que el acoso logra tener varios efectos adversos en quienes lo reciben como depresión, problemas de autoestima, ansiedad, bajo desempeño académico y en casos muy extremos, el suicidio.

La sociedad diariamente es bombardeada con estereotipos de una vida perfecta tanto mediante redes sociales, internet como en la televisión y otros medios de comunicación. Con los avances en tecnologías y creación de estas mencionadas redes sociales, las personas tienen un acceso inmediato a la vida de otras personas, ocasionando la percepción de una falsa imagen de tendencias que deberían seguir. Esto ha provocado que el abuso cibernético o “cyber bullying” como se le conoce en inglés, adquiera más importancia en cuanto a atención y regulación.

Al acoso cibernético funciona muy similar al acoso directo en cuanto a intimidación y agresión nos referimos, solo que, al contar con un dispositivo electrónico entre ambas personas, genera un sentimiento de seguridad y protección a quién lo comete. Es más sencillo escribir e intimidar a una persona por un medio electrónico ya sea con un perfil o correo electrónico falso ya que en muchas ocasiones la víctima no reconocería al acosador. Cómo se ha mencionado en otros delitos, también el acosador cuenta con la ventaja de la inmediatez para actuar, pudiéndolo hacer desde cualquier lugar y a cualquier hora.

En Costa Rica el acoso en sí no se encuentra regulado, sin embargo, si se hace mención al acoso sexual en el Código Penal, modificado gracias a la Ley contra el acoso sexual callejero y en la Ley 9404 donde se protege a los menores de edad del acoso en los centros educativos. La primera cubre situaciones tales como exhibicionismo, masturbación en espacios públicos, persecución y producción de material audiovisual, más aún no se incluye dentro del tipo el acoso sexual cibernético. La segunda cubre el acoso escolar o "bullying" y el acoso cibernético mediante protocolos de atención y acción en el caso de ser identificado los diferentes casos, imponiendo a los centros educativos medidas a tomar en estos mencionados casos en conjunto con los padres o guardianes de los involucrados.

2.10 Pornografía infantil

La pornografía infantil es un delito que se encuentra en crecimiento con el avance en los medios de comunicación mediante la tecnología y el internet, razón por la cual las normativas han tenido que actualizarse y mantener una protección amplia y fuerte ante los delincuentes que incurran en estos actos. Dentro de este delito se debe incluir toda representación de manera visual que involucre a un menor de edad con índoles sexuales ya sea real, simulada o simulada.

En Costa Rica se ha implementado una actualización a la legislación penal mediante la reforma y adición de artículos que lo contemplan al Código Penal cubriendo casos como violación a menores, abuso sexual y la tenencia, producción o reproducción de material pornográfico que involucre menores de edad, estos últimos regulados en el artículo 173 y 173 bis donde específicamente resuelven:

> Será sancionado con pena de prisión de tres a ocho años, quien fabrique, produzca o reproduzca material pornográfico, utilizando a personas menores de edad, su imagen y/o su voz.

> Será sancionado con pena de prisión de uno a cuatro años, quien transporte o ingrese en el país este tipo de material con fines comerciales.
>
> Para los efectos de este Código, se entenderá por material pornográfico infantil toda representación escrita, visual o auditiva producida por cualquier medio, de una persona menor de edad, su imagen o su voz, alteradas o modificadas, dedicada a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de una persona menor de edad con fines sexuales.
>
> Será sancionado con pena de prisión de seis meses a dos años, quien posea material pornográfico en el que aparezcan personas menores de edad, ya sea utilizando su imagen y/o su voz." (Ley N° 4573, Costa Rica, 4 de mayo de 1970)

Es importante recalcar la protección que dan al menor en su totalidad, incluyendo el material auditivo o escrito, cubriendo en su totalidad cualquier actividad sexual relacionada con este. También se logra recalcar que se cuenta con una amplia normativa n cuanto a al protección de delitos contra menores de edad, manteniendo el país a la vanguardia en cuanto a la protección de estos derechos de amplia importancia.

Capítulo 3 - Almacenamiento y regulación de datos virtuales

3.1 Manejo y utilización de datos informáticos

Al manejar un entendimiento en cuanto a la clasificación de datos generales, personales o sensibles, es de suma importancia conceptualizar esta división en el ámbito informático con el fin de determinar el almacenamiento y manejo de estos. Si bien se ha llegado a una era tecnológica donde un alto porcentaje de información es manejada virtualmente, esto conlleva a la distribución y salvaguarda por parte de las diferentes entidades que los almacenan. Si bien son ejemplos que se detallarán más adelante, se puede tomar en consideración un banco, el cual cuenta con información personal de sus clientes e incluso información financiera muy delicada la cual, si cayera en malas manos, podría ser utilizada para cometer todo tipo de delitos.

Esto nos lleva a la pregunta principal; ¿cómo se puede estar seguro de que nuestros datos se encuentran a salvo?

En sí, esto se torna principalmente en un tema de confianza, ya que, es necesario para un usuario estar seguro de que no importa lo que suceda, sus datos no serán divulgados ni liberados a ninguna otra persona ajena a su exclusiva relación con la compañía que los trata. La confianza se obtiene mediante un sistema de seguridad eficiente. Por ejemplo, un banco puede tener años de trayectoria y prestigio, pero si en esta migración de datos físicos que se ha dado a virtuales en los últimos años comete errores críticos y son víctimas de estafas y robos cibernéticos sus clientes perderán la confianza y eventualmente buscarán otros bancos con un mayor respaldo, esto debido a que como se ha mencionado anteriormente, la globalización tecnológica es tan avanzada que poco a poco todos los servicios y transacciones se realizan por medio de la red.

Por otro lado, compañías de compras en línea como Amazon, bancos nacionales, sistemas de pago como PayPal, por poner ejemplos, han logrado mediante una constante red de seguridad, brindar

tranquilidad a sus usuarios lo cual se convierte en confianza a mediano o largo plazo en la utilización de sus servicios.

Otro punto muy importante para establecer una confianza sólida entre la entidad y el consumidor es por medio de sistemas y facilidades que ayuden a los usuarios a mantener sus datos a mano y a poder realizar transacciones al alcance de un mando.

Aún y cuando los cambios a modo virtual se han venido dando desde un par de décadas atrás a la fecha, las empresas y proveedores de servicios deben adaptar las herramientas que ponen a disposición de sus usuarios. Ante la pandemia vivida en el presente año 2020 se tuvo que implementar una modalidad virtual y una facilidad para realizar cualquier trámite desde la comodidad y seguridad del hogar. Un ejemplo son las compañías de ventas de alimentos preparados, las cuales, aún y cuando el servicio a domicilio ha existido desde hace muchos años, actualmente tuvieron que fortalecer esta facilidad. Lo mismo sucedió con las tiendas de abarrotes, comestibles, diarios, etc., por mencionar unas cuantas.

Estas transacciones hace unos años se podían hacer por medio de una llamada telefónica, sin embargo, los servicios tuvieron que evolucionar, empezando desde la comodidad de un ordenador con acceso a internet hasta la actualidad donde la mayoría de las personas tienen acceso a su dispositivo inteligente de telefonía en todo momento. En estos teléfonos inteligentes, por medio de aplicaciones, se ha logrado consolidar una variedad de servicios con una gran facilidad de acceso desde cualquier parte del mundo donde estemos.

Gracias a esta transformación se puede determinar la importancia de una estructura sólida en cuanto a la implementación de la confianza del consumidor, la cual debe ir de la mano y debidamente equilibrada entre la seguridad y la facilidad de los servicios brindados.

Para lograr una protección adecuada de la información de sus consumidores , es necesario cumplir con ciertos principios en cuanto al manejo de los datos, especialmente a la hora de adentrarse en el área informática.

Como se mencionó anteriormente, es importante que los datos almacenados sean correctos, verdaderos y que cuenten con legitimidad, esto sin olvidar que deben ser utilizados de manera correcta y de ninguna manera con fines ilícitos. También es importante mantener con claridad los fines para los cuales se van a utilizar. Si se habla de una entidad bancaria que solicite datos privados a un cliente, de ninguna manera debería utilizar esos datos para cuestiones fuera del ámbito financiero relacionado al banco. La precisión de estos datos es fundamental, teniendo en cuenta que no se debe exceder la cantidad información necesaria para realizar una transacción. Como ejemplo se puede utilizar una compra por internet, donde claramente pueden solicitar los datos como el nombre, edad, número de tarjeta de crédito a utilizar y sus respectivos agentes identificadores, pero si solicitan información como nombres de familiares, domicilios ajenos, lugar donde se labora y demás, es información fuer a del ámbito de la compra que se desea realizar.

En la legislación costarricense, dentro de la protección brindada por la autodeterminación informativa, se reitera la importancia de la información sensible, la cual incluye la raza, salud, afiliación política, preferencia sexual o creencias religiosas. Esto permite que no se utilice este tipo de información como un medio de discriminación a la hora de efectuar transacciones virtuales o de ningún otro tipo.

Dentro de las funciones fundamentales de las empresas que almacenen datos de sus usuarios es sumamente importante la confidencialidad a la hora de manejarlos. Esto aplica para todos los empleados que vayan a tener contacto con este tipo de información. Muchas empresas recurren al contrato de protección e información confidencial, este es un medio por el cual la empresa asegura

que sus empleados no puedan divulgar datos que manejen a la hora de desempeñar sus funciones laborales. Cabe resaltar que este tipo de contratos son atípicos ya que no se encuentran regulados en la legislación costarricense. Asimismo, este tipo de contratos lo utilizan a nivel mundial las empresas trasnacionales que manejan información sensible. Muchas de estas empresas también utilizan como medio de protección la política de "no uso de papel". Esta política consiste en que en el área laboral no se permite ningún artículo, implemento (físico o electrónico) o medio por el cual los empleados puedan anotar ningún tipo de dato obtenido durante su jornada laboral. Las computadoras también cuentan con una encriptación especial la cual no permite acceder a sitios web que no sean referentes al trabajo, de esa manera se controla el flujo de información maneada por sus trabajadores.

Dentro de esta protección también se incluye el contar con equipo de alta tecnología, acceso a softwares de antivirus, actualización constante de los sistemas utilizados y capacitación constante a su equipo de trabajo.

Los usuarios deben contar con un acceso a su propia información y a poder corregirla o cambiarla en el momento que vean oportunos, así como estar en desacuerdo con el tipo de información que se brinda a una entidad con la que estén tratando. Aquí forma parte importante el consentimiento, ya que toda información almacenada debe contar con el debido consentimiento del usuario para que sea almacenada. En muchos casos se aplica el consentimiento tácito a la hora de compartir los datos, sin embargo, este consentimiento tácito no puede ser utilizado para divulgar, manejar o compartir la información brindada sin el permiso expreso para hacerlo. Dentro de este consentimiento debe ir el derecho del usuario de exigir el cumplimiento de la finalidad para la cual se brindó los datos, asegurándose que no sean utilizados de forma ajena a su origen.

Cabe mencionar que el usuario debe contar con la debida tutela y protección jurisdiccional, la cual les brinde un respaldo para acceder a su derecho de recibir la debida indemnización en el momento que exista un incumplimiento de protección por parte de la empresa.

3.2 Responsabilidad de los usuarios en los delitos informáticos

Dentro del ámbito de manejo y protección datos es de suma importancia recalcar la función o papel que cumplen los usuarios. Si bien es determinante la seguridad, confianza y protección que brinden las compañías a sus usuarios, es necesario comprender que no toda la responsabilidad recaerá en estas ya qué, no importa cuán segura sea una transacción, si no se siguen los pasos adecuados o no existe protección de la información por parte del usuario, el delito informático será de fácil comisión.

> (…)se suele creer los hacker , cracker , solo atacan las grandes compañías, pero resulta que cualquier persona con algún interés particular puede obtener programas de fácil manejo que le permitan acceder a claves, cuentas de correos del usuario, numero de cuentas bancarias con sus respectivas contraseñas y a mucha más información personal.
>
> Estas vulnerabilidades son en su gran mayoría errores de usuario, los cuales tiene malos hábitos de seguridad en el manejo de información, en el simple uso de claves los usuarios cometen errores como el de asignar claves predecibles (nombres de los hijos, fechas de nacimiento, placa del vehículo, etc...) información que mucha gente conoce, o aún peor claves numéricas como 1234, 9876, 1357 etc. (Lopez Bulla, R. 2013, p. 25)

En el artículo del ingeniero López de su obra “La seguridad de la Información Responsabilidad de Todos” se resalta un tema muy importante en cuanto a la vulnerabilidad de la información. Años atrás, un poco avanzada la revolución cibernética, se veía bastante lejano que alguien más aparte de las grandes compañías, contaran con la facilidad de manejo de información con la que cuentan ahora los usuarios comunes o usuarios finales. Con esto se refiere directamente a lo lejano que puede un usuario percibir un fraude informático aplicado a su información personal.

No obstante, la informática al evolucionar con pasos agigantados, tal y como se ha mencionado varias veces, el manejo de información personal a nivel informático ha incrementado considerablemente, compartiendo la responsabilidad de protección de datos con los usuarios finales. Con esto se quiere decir que no se puede atribuir un delito informático en su totalidad a la empresa que almacena los datos, ya que el usuario es responsable de salvaguardar y manejar de manera correcta su propia información. Este descuido o mala utilización de la información o procesos a la hora de emplearla, genera vulnerabilidades las cuales facilitan el robo y acceso a los datos personales. Los delincuentes cibernéticos pueden adquirir una gran cantidad de información con el solo hecho de tener acceso a una contraseña mal empleada o débil.

López hace referencia a los malos hábitos los cuales facilitan las vulnerabilidades a la hora de manejar la mencionada información personal. Entre estas se puede encontrar desde el rango más básico al más elaborado.

El criptoanálisis se considera como la razón más básica a la hora de robar información mediante la red. En sí, esto consiste en la decrepitación e interpretación de los datos que trafican en la red, por medio de programas maliciosos como los virus, con el fin de acceder a información sensible.

Dirigiéndose a los usuarios directamente, López hace referencia a la Ingeniería Social de la siguiente manera:

> Otra técnica muy común de ataque es la Ingeniería Social la cual está definida como la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos, haciendo uso de la persuasión, muchas veces abusando de la ingenuidad o confianza de un usuario, para obtener información que pueda ser utilizada para tener acceso autorizado a la información de las computadoras y/o a sistemas de información que les permitan realizar algún acto que perjudique o exponga a personas u organismos. (Lopez Bulla, R. 2013, p. 26)

El tema de manipulación de usuarios es extenso y de suma importancia a la hora de investigar acerca la responsabilidad en cuanto al almacenamiento y trato de los datos cibernéticos. La tecnología no se detiene en cuanto a funciones y sistemas nuevos, los cuales se mantienen en constante cambio. La realidad actual en este 2020 ha obligado a las personas a migrar a sistemas que anteriormente, hace algunos años podían parecer imposibles tales como las videollamadas, video consultas, clases, reuniones, graduaciones virtuales hasta el desempeño de la jornada laboral desde la comodidad del hogar mediante el teletrabajo. Con este ejemplo, se puede determinar que los cambios normalmente toman por desprevenida a la gente. Si tomamos en cuenta la pandemia que ha afectado a nivel mundial, a principios de este año 2020 ni siquiera imaginaban el cambio tan drástico que iban a tener las personas en cuanto a relaciones sociales y comunicación.

Si bien los cambios pueden ser drásticos y repentinos, así mismo las personas tardan en adaptarse a estos, y es que no solamente ha sucedido con la pandemia, si no como se ha mencionado en reiteradas ocasiones, desde que empezó el tema de la globalización tecnológica, esta ha avanzado

sin freno. Esto conlleva a los engaños y abusos por parte de los delincuentes, quienes aprovechan esa falta de información y experiencia para poder obtener información con fines delictivos.

En Costa Rica se han dado miles de casos de estafa por falta de información o por convencimiento. Por poner varios ejemplos se puede empezar con el tema de las estafas con el Ministerio de Hacienda mediante llamadas telefónicas provenientes del Sistema Penitenciario. Los estafadores realizaban llamadas cuando empezó la migración a la nueva norma Tributaria haciéndose pasar por funcionarios del Ministerio de Hacienda. En la llamada brindaban todos los datos al usuario y les indicaban que debían actualizar el perfil para que pudieran tributar en una página de Internet. Esa página de internet era creada por los mismos estafadores o equipos que trabajaban en conjunto con ellos haciéndola casi idéntica a la original, con la única diferencia que cuando el usuario ingresaba los datos personales, estos eran robados por los delincuentes.

Otro ejemplo es el de las entidades bancarias. Los estafadores llaman haciéndose pasar por un empleado bancario el cual le solicita acceder a un enlace, llamen a un número de teléfono o que brinden cierto tipo de información para confirmar su identidad. Los delincuentes logran incluso emular el número telefónico del banco para que aparezca como tal en el identificador de llamadas. El usuario al seguir las instrucciones del estafador ingresa datos muy sensibles los cuales pueden prestarse incluso para tener acceso a su cuenta bancaria.

Una situación diferente sucede con la extorsión. Se mencionó anteriormente que existe información que es pública y de fácil acceso a todas las personas. A esto sumamos las tan de moda redes sociales, donde las personas comparten situaciones muy personales, desde su estado sentimental, creencias, trabajo, familiares y demás. El producto es un sinfín de posibilidades para que un delincuente logre descifrar y adquirir información clave y utilizarla para extorsionar a una persona, obligándola a proporcionar información más privada y sensible en el proceso.

Digamos que una persona en horas de la noche, nuestros hijos y esposa no han regresado a casa. La persona que llama nos indica que sabe dónde vivimos, el color y matrícula de nuestro vehículo, el nombre de nuestros hijos y esposa, el lugar donde trabajamos, el número de documento de identificación e incluso los lugares que frecuentamos. El delincuente nos indica que tiene acceso a hacerle daño a nuestros familiares y que, si no le brindamos nuestras claves bancarias, procederá al acto de agresión. Muchas personas acatarán que se trata de una extorción y estafa telefónica, pero alguien ingenuo o asustadizo podría fácilmente brindar la información que solicitan con tal de contar con seguridad para sí mismo y su familia.

Hoy en día es muy popular para las personas compartir todos los detalles de su vida mediante redes sociales. Algunas muy ingenuamente hasta comparten fotografías que contienen información muy personal o sensible tales como números de tarjetas de crédito o cuentas bancarias. Mediante las biografías, fotografías, publicaciones y demás, las personas están dando a conocer públicamente detalles que permiten a los delincuentes investigar más a fondo su estilo de vida, domicilios, ingresos, posesiones materiales, etc. Existen incluso personas que comparten contenido de sus hijos, e cual puede ser utilizado y visto por personas con trastornos o enfermedades, resultando en potenciales abusadores de menores.

Es importante limitar el acceso a la información que se brinda, intentando a toda costa limitar el contenido que otras personas pueden ver, de esta manera dificultando y bloqueando herramientas que los delincuentes podrían utilizar en su contra.

Otra modalidad que se ha puesto muy de moda en la actualidad, tomando en cuenta la virtualidad, falta de tiempo y hasta facilidad, son las aplicaciones de citas por la red. Las citas por internet tuvieron un auge muy amplio en el momento que los usuarios ya contaban con acceso a la red desde sus hogares. En aquel entonces los usuarios creaban un perfil, ponían una descripción de su

vida, sus intereses y en algunos casos hasta grababan un pequeño video el cual subían con una presentación personal. Si bien cuando el tema de las citas en línea empezó, los casos por estafa no eran tantos, siempre existían robos de identidad o engaños a la hora de conocer a la persona.

Los servicios de citas en línea evolucionaron hasta el punto de convertirse en aplicaciones al alcance de los teléfonos inteligentes. Ahora estos servicios son más accesibles, ya que, con un dispositivo móvil y un plan de datos, se puede conocer a miles de personas a través de estas aplicaciones. La modalidad es similar, las personas se crean un perfil donde ponen sus intereses, suben sus fotografías y una reseña del tipo de persona que buscan conocer.

Al existir una facilidad de acceso a estas aplicaciones, es complicado regular el tipo de usuarios que la utilizan, y tomando en cuenta que la evolución de estas aplicaciones va de la mano con la evolución de las aplicaciones móviles para otro tipo de trámites tales como compras en línea, aplicaciones bancarias y demás, las estafas y delitos cibernéticos fueron creciendo en proporción con esta línea evolutiva.

Los delincuentes actúan de manera parecida a como actuaban hace unos años, sin embargo, poseen más herramientas para cometer la estafa. La estafa más común es aquella donde al estar conociendo a la persona, inventan una historia la cual pueda generar compasión o una reacción empática por el usuario. De esta manera, y gracias a la facilidad en cuanto a las transferencias bancarias, el usuario procede a depositar dinero en una cuenta. Han existido incluso casos donde el usuario y el estafador comparten fotografías íntimas (el estafador enviando fotografías o contenido falso) y seguidamente extorsionan al usuario para que les deposite más dinero o de lo contrario, procederán a difundir las fotografías y las conversaciones con personas allegadas tales como familiares y amigos. En otras ocasiones van aún más lejos y le indican al usuario que la persona con la que hablan es menor de edad y que, de no proceder a depositarles una cantidad de dinero, procederán

a un juzgado penal a interponer la debida denuncia por delito de pornografía infantil. Existen casos incluso donde adquieren tanta confianza con el usuario que logran que este les pague diferentes tipos de gastos como boletos de avión, dinero para viajar, cirugías estéticas o gastos médicos, que paguen alguna deuda que tienen pendiente, y muchas otras situaciones similares.

Es importante también saber que ese tipo de estafas se pueden realizar mediante otros métodos de transferencia de dinero. Si bien un depósito bancario es más fácil de rastrear, ya que la cuente está vinculada a un usuario con su respectivo número de cédula y datos personales, existen aplicaciones y páginas de internet que ofrecen un servicio más privado y exclusivo para realizar pagos por internet. Un ejemplo de estas aplicaciones es Pay Pal, donde se vincula un método de pago a la cuenta y esta se puede generar por medio de Internet sin necesidad de trámites que verifiquen la identidad de quién las crea.

Si bien es necesario vivir de acuerdo al progreso, eso también implica la de las personas de adaptarse y proteger sus bienes tanto patrimoniales como personales. No se puede responsabilizar al 100% a las empresas que brindan los servicios al usuario o consumidor, ya que esto se debe ver como un trabajo en equipo. Fuera del área cibernética, si se facilita la llave de nuestro hogar a un desconocido, se está fomentando a un eventual robo o invasión de nuestra propiedad privada. De igual manera funciona con la actividad virtual, cada usuario debe asegurarse de poner de su parte para la protección de sus datos sensibles.

Dentro de las recomendaciones a los usuarios se pueden resaltar las básicas y principales a continuación:

1. No compartir información personal o sensible en redes sociales, grupos de mensajería instantánea, por medio de fotografías. Dentro de esta información considerar los datos de

familiares, allegados, lugares de trabajo, estado civil, residencia, lugares de estudio y demás.

2. Nunca compartir números de cuentas bancarias, tarjetas de crédito, usuarios o contraseñas con otras personas a menos que se cuente con un protocolo de seguridad para manejar dicha información.
3. Si se conoce a alguien mediante aplicaciones de citas por internet, asegurarse de que la persona sea alguien real, cuya identidad sea comprobable y verificable. Si se acuerda a tener una cita cara a cara, es necesario contar con total certeza de quién es la persona a la que van a ver por primera vez y verse en un lugar público, de ser necesario acompañados de alguien conocido.
4. Si van a realizar compras o ventas de segunda mano por internet, asegurarse de entregar el producto después de verificar el pago. Si deben entregar el producto cara a cara, asegurarse de que la transacción se haga en un lugar público, así como el comprador comprobar que está recibiendo el artículo que pactaron en el acuerdo.
5. A la hora de hacer compras por internet, asegurarse de que la página se de prestigio, conocida, de confianza y si es necesario realizar una transacción con tarjeta de crédito, que la página muestre una encriptación de seguridad mediante el protocolo HTTPS.
6. Si se recibe un mensaje de texto o llamada sospechosa indicando que ha sido ganador o ganadora de un premio, que debe actualizar datos bancarios o incluso que se debe realizar transacciones tributarias, nunca dar información personal o sensible por teléfono. Se debe llamar a la entidad bancaria o la compañía de donde se supone estaba recibiendo la llamada sospechosa, utilizando los canales de comunicación oficiales.

7. Si recibe un enlace por correo, mensaje de texto o mensajería instantánea, verificar que sea un vínculo legítimo ya que podrían ser víctimas de robo de información por parte de hackers informáticos.
8. Si utiliza redes sociales, restringir el contenido compartido, limitar las amistades que se tienen agregadas, así como implementar la seguridad a la hora de compartir publicaciones. No compartir material relacionado a familiares o allegados y tener excesiva cautela cuando estas publicaciones involucren menores de edad.
9. De recibir una llamada de extorsión, mantener la calma y proceder a realizar la respectiva denuncia ante las autoridades. Nunca encarar al delincuente o ceder ante sus requisitos, ya que puede empoderar al criminal a continuar e incluso solicitar una recompensa mayor.

Capítulo 4 - Comercio Electrónico

La mencionada “globalización tecnológica” es una revolución que ha arrastrado los principales aspectos en la vida de los seres humanos. Las transacciones diarias no son la excepción y también han sido impactadas por la facilitación de procesos y disponibilidad de recursos. No obstante, con cada nuevo panorama evolutivo en cuanto a interacción social, siempre viene de la mano problemáticas y desafíos los cuales es necesario abordar.

Cuando se menciona la evolución del comercio, se puede datar a muchos años atrás desde el intercambio de bienes conocido como trueque hasta tiempos de la revolución industrial. Junto a todos esos capítulos en la historia comercial, se ha visto acompañamiento por parte de las diferentes tecnologías acopladas a la época. Un ejemplo de esto es como se solía entregar mercadería por medio de animales de carga, seguidamente por transportes masivos como cargamentos por tren y barcos. De igual manera muchos de esos medios se siguen utilizando, pero las facilidades de la época permiten lograr transacciones millonarias en cuestión de minutos y entregas de mercadería desde el otro lado del mundo en cuestión de unas horas o días.

Uno de los principales aspectos evolutivos con respecto a las transacciones comerciales ha sido la comunicación. Gracias a la red es posible enviar una orden de compra o comunicarse con otro comerciante en tan solo unos segundos. Si bien ya contábamos con las telecomunicaciones, ahora es mucho más accesible y mucho menos costoso realizar transacciones internacionales.

Un ejemplo de este mencionado aspecto evolutivo era la disponibilidad de mercadería en países como Costa Rica. Hace algunos años, entre mediados de los años 80 y 90, los artículos más recientes implementados en otros países tardaban meses en ser conocidos en nuestro país. Incluso en el mundo cinematográfico ocurría que grandes películas fueran estrenadas meses y a veces años después de su estreno en su país natal.

En los tiempos actuales, gracias al surgimiento de la computación y la internet, se ha creado una red amplia que permite el involucramiento de varios sujetos a la hora de realizar una transacción, reduciendo costos y comunicando directamente a los sujetos intervinientes, dejando por fuera intermediarios innecesarios.

En términos generales, el comercio electrónico se le conoce como las transacciones comerciales, tales como la compra y venta o intercambio de bienes y/o servicios, efectuadas por medio de un recurso electrónico como correo electrónico, aplicaciones o páginas de internet o cualquiera relacionado a una red informática. Este concepto se debió ajustar, ya que antes incluso eran consideradas las transacciones por medio de fax y telefonía entre otros, los cuales ya han ido quedando obsoletos con la integración de los nuevos sistemas lo cual refuerza Horacio Fernández citando a José Heriberto García Peña:

> Algunos expertos opinan que: en cierta forma el Comercio electrónico comenzó antes de la Internet, mediante transacciones comerciales por télex, teléfono y fax, pero el desarrollo de la WEB global motivó que alcanzara mayor auge, por su masividad y rapidez de operación. Su acepción más general es "acercar el comprador al fabricante por medios electrónicos" (Fernández, 2014, p. 448)

Aún y cuando estos conceptos son debatibles y bien fundamentados, el estudio en la presente investigación será dirigido al comercio electrónico mediante tecnologías informáticas, tomando en cuenta las transacciones comerciales que han surgido con el pasar del tiempo.

Un aspecto primordial a la hora de la aparición del comercio electrónico es el dinero electrónico. El tiempo también se ha encargado de erradicar el dinero en efectivo, aún y cuando se siga utilizando a diario. Desde la aparición de las tarjetas de crédito o débito, los usuarios han mostrado

preferencia al contar con más seguridad y comodidad al momento de efectuar transacciones. Esto se facilitó aún más con la aparición de los depósitos bancarios, ya que con solo contactar al banco era posible depositar a la cuenta de alguien la suma requerida de dinero. Esto evolucionó aún más con la aparición de las páginas de internet bancarias y las aplicaciones donde con solo contar con una conexión de internet se puede realizar dicha transacción de manera inmediata mediante el sistema de depósito, SINPE o SINPE móvil. EL Sistema Interbancario de Negociación y Pagos Electrónicos (SINPE) consta de una plataforma desarrollada con el fin de lograr transacciones entre diferentes bancos. Por otro lado, el SINPE móvil es la vinculación de una o varias cuentas del usuario a su número de teléfono para poder realizar una transacción bancaria solamente con contar con el número de teléfono de receptor, dejando atrás la necesidad de números de cuenta. Impresionantemente, en la actualidad, el pago electrónico se puede realizar en un par de minutos facilitando las transacciones comerciales de manera segura, ya que una de las principales razones por la cual una persona no desea contar con efectivo a mano es por la posibilidad de perderlo o ser víctima de un robo o hurto.

Fernández brinda una división del comercio electrónico de la siguiente manera:

> Comercio electrónico completo o directo, en el cual tanto la transacción como el pago se realiza mediante el sistema electrónico; las tres primeras fases de la venta (promoción, pedido y pago) se realizan a través de medios electrónicos. La cuarta fase (distribución /entrega) será electrónica o no, dependiendo del producto que compremos.
>
> Comercio electrónico incompleto o indirecto, no todas las etapas de la transacción se realizan electrónicamente, ya que aquí solo la transacción utiliza el medio electrónico, pero el pago se realiza fuera del sistema. (Fernández, 2014, p. 449)

Es importante mantener una compresión de estas dos tipos con el fin de identificar cuales acciones estarían contempladas a la hora de hablar del tema. Se debe considerar que, en primera instancia, tal y como lo definimos, el comercio electrónico completo o directo la transacción en su totalidad sería por medios electrónicos. Otro aspecto importante mencionado son las 4 partes de la transacción, promoción, pedido y pago. Un ejemplo de este tipo de acuerdos sería una compra por medio de un sitio de internet. El usuario se encargará de seleccionar el artículo por medio de la tienda virtual, lo agrega a su orden virtual, decide el método de pago y realiza el pago inmediatamente. Existen productos digitales los cuales pueden ser enviados inmediatamente o productos físicos los cuales deberán ser entregados directamente a la persona, razón por la cual la entrega no influye a la hora de definir si la transacción es directa.

Por otro lado, un ejemplo de comercio electrónico incompleto o indirecto sería en el caso de que una persona vea un artículo en línea, lo reserve y se presente a la tienda físicamente a completar la transacción, realizar el pago y llevarse el artículo.

La disponibilidad de servicios cambia el esquema y subdivisiones cuando se habla de comercio electrónico. Como primera subdivisión se encuentra la transacción efectuada entre empresas, donde se realiza una conexión entre dos o más empresas facilitando la disponibilidad de artículos y transacciones entre sí. Otro método existente es la relación entre la empresa y el consumidor, donde la empresa pone a disposición de los usuarios su mercadería y/o servicios mediante catálogo o página de internet.

Existen también relaciones comerciales entre las empresas y el gobierno, y el gobierno y el ciudadano, estas son transacciones que se realizan entre el gobierno y las demás entidades o población.

Actualmente el comercio electrónico cuenta con varios desafíos y ventajas. Entre los principales desafíos se pueden mencionar la seguridad, inmediatez, adaptación, competencia, disponibilidad de personal y seguimiento, principalmente.

4.1 Transacciones electrónicas

Aún y cuando actualmente se cuentan con protocolos de seguridad muy altos a nivel mundial, cuando se realiza una transacción electrónica siempre se corren riesgos de los ciber delitos. Si el usuario carece de cuidado podría ser víctima de una estafa o un robo informático ya que, se debe recordar que estas transacciones normalmente median métodos de pago como uso de tarjetas de crédito/ débito o transferencia bancaria.

Aunque la transacción se realice en forma inmediata, el envío de los artículos podría tomar días e incluso semanas, afectando la inmediatez a la hora de recibir el producto. Esto difiere de cuando se realiza una compra directa físicamente, ya que, al presentarse a la tienda, normalmente cuando se paga el producto el comprador lo lleva consigo mismo.

En cuanto a la adaptación, se debe resaltar que, aunque los compradores cada vez se familiarizan más con la tecnología, existen muchas personas que aún no se adaptan a esta evolución ya sea por complicaciones o porque simplemente no lo desean. Esto puede ser una desventaja a la hora de considerar el alcance de la empresa al público, dependiendo del producto que se esté ofreciendo.

Para las empresas ha sido muy ventajoso el hecho de tener más alcance a los usuarios, sin embargo, esto también puede impactar negativamente al negocio a la hora de considerar la competencia. Al brindar muchas facilidades mediante la red, la empresa puede contar con mucha más competencia de la que tendría por medio del comercio físico, razón por la cual deben extender un estudio bastante amplio a la hora de determinar el alcance.

La disponibilidad de personal y seguimiento de una transacción electrónica es un poco más complicada ya que se deben implementar medios tecnológicos para asegurarse de que el producto llegue a su destino. A diferencia de las compras físicas, donde se entrega el producto inmediatamente, el comercio electrónico debe asegurarse de que el producto llegue a las manos del comprador necesitando, en algunas ocasiones, más recursos.

En cuanto a los beneficios, se pueden enumerar múltiples pero los más importantes son la disponibilidad de productos y su actualización, facilidad de mercadeo, optimización de tiempo, cobertura y costos.

Al estar al alcance de un ordenador, es mucho más simple para una persona encontrar lo que busca mediante la red. Las páginas usualmente cuentan con un buscador donde solamente deben digitar palabras claves o el producto que desean. Esto es un beneficio para las empresas ya que el inventario se actualiza automáticamente mediante un sistema informático.

Cuando se habla del mercadeo a nivel empresarial, se debe definir el público meta y la manera de alcanzarlo. Mediante la red es más fácil programar algoritmos que definan este alcance basado en las preferencias de la compañía. Las redes sociales son un ejemplo de este sistema, ya que normalmente la publicidad está dirigida a edades, ubicaciones e intereses definidos.

El comercio electrónico brinda la facilidad de tiempo al poner a disponibilidad del usuario los productos de manera inmediata y a cualquier hora del día. Aún y cuando exista una contradicción con los tiempos de espera a que el producto sea entregado, existe una compensación ya que el usuario no debe desplazarse a la tienda y realizar la compra.

Una de las ventajas más importantes en cuanto a esta modalidad comercial es la cobertura y los costos. Cuando se define n sistema de ventas en línea se ahorran muchos costos en comparación

con una tienda física ya que no se necesita tanto personal ni pagar servicios públicos. Existen productos que en determinada localidad no se encuentren disponible, ampliando las opciones de artículos para ofrecer al cliente.

Dentro de las características de una transacción median los mismos requisitos que un contrato normal, donde deben existir los sujetos, objeto y un consentimiento, el cual puede ser expreso o tácito. Este consentimiento mutuo es lo que se conoce como "manifestación de la voluntad". Se podría definir esta manifestación como una exteriorización de un pensamiento o deseo plasmado oralmente, por escrito o cualquier otro método.

El comercio electrónico tiene una particularidad que lo define y es que, esta manifestación, es externada normalmente a la distancia. Esto quiere decir que la transacción electrónica es una manera impersonal de realizar un contrato, en el cual el acuerdo se media a través de una comunicación virtual.

Tomando como ejemplo una compraventa en una página de internet, se debe considerar el hecho de que la transacción electrónica se realiza de manera internacional. Los comercios han generado maneras de lograr que exista una aceptación o manifestación de voluntad a la hora de realizar un trámite virtual mediante diferentes métodos. El método más normal es la aceptación de términos y condiciones, donde se le presenta al usuario una página con un contrato electrónico el cual indica las consecuencias y términos que entrarían a regir en el momento que se presiona "Acepto". Este método no solo es utilizado en páginas de comercio si no como medio de contratación virtual global. Dentro de estos términos normalmente se explica el proceso de compra y las responsabilidades del comercio y del comprador. También se indica que al momento de que el usuario presione el botón de "ordenar", automáticamente está aceptando la compra, por lo cual estaría expresando su consentimiento.

Otra manera de manifestar ese consentimiento son los contratos empresariales. Cuando una compañía compra los servicios de otra se debe plasmar en un contrato cuales son los servicios incluidos. Normalmente los ejecutivos revisan los servicios y envían el contrato firmado por medio de firma digital, aceptando en ese momento el consentimiento y haciendo efectivo ese contrato.

Actualmente en Costa Rica no existe una regulación específica al comercio electrónico, sin embargo, al ser considerado parte del comercio normal, se cuentan con regulaciones a través del Código de Comercio, Código Civil y la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor entre otras. Esto lo confirma la sala constitucional en la sentencia

> (…) dentro del comercio electrónico, y por ende, en la emisión y difusión de mensajes de datos, convergen no sólo variadas y profusas ramas del derecho, sino además, la tecnología. Dentro de ese orden de ideas, y a nivel jurídico, las notas típicas sobre información, comunicación, persuasión, mensaje e intencionalidad del emisor y carácter comercial, traen aparejado que, a esta rama del derecho, en defecto de norma especial, se le deban aplicar las consideraciones que deriven de normativas propias del derecho preexistente, como lo serían la civil, la comercial, las reglas sobre protección al consumidor, el derecho de la competencia, la protección de datos de carácter personal y el derecho de la publicidad, por mencionar algunas. (Sala Constitucional, 11-000724-0007-CO, 2011)

Internacionalmente se cuenta con más respaldo en el tema mediante leyes como: La Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, La Directiva de la Unión Europea sobre Comercio Electrónico y las Recomendaciones del Consejo de la Organización para la Cooperación y el Desarrollo Económico entre varias otras, algunas de las cuales serán mencionadas más adelante.

4.2 Contratos electrónicos

Dentro del tema del comercio electrónico se ha valorado la transformación a la cual se ha visto forzada la humanidad con el crecimiento de sistemas tecnológicos cada vez más capaces y más accesibles. Poco a poco las áreas de interacción y necesidades humanas se ven forzadas a involucrarse y a adaptarse con estos medios. El contrato, al representar un compromiso entre dos o más partes mediante la manifestación de su voluntad, no se queda atrás cuando se habla de estos cambiantes sistemas.

Cuando se habla de contratación electrónica se encuentran dos aristas las cuales pueden ser un poco confusas. Por un lado, en cuanto a elaboración, funciones y alcance, un contrato electrónico no difiere de un contrato normal, mas cuando se dirige el estudio a la legitimación y representación de la voluntad de las partes, es donde es necesario realizar un análisis más detallado.

En otras palabras, cuando se trata con los contratos electrónicos se debe estudiar el medio para su realización antes que el objeto, razón por la cual se debe considerar dos características importantes las cuales son el lugar donde se realizan y la relación que tienen con medios informáticos. Al mencionar el lugar se reitera lo mencionado en cuanto al comercio electrónico, se pueden celebrar a la distancia y desde cualquier lugar con solo contar con una conexión a internet, lo cual conlleva a una segunda necesidad, la cual es contar con un dispositivo informático con el cual pueda realizarse el acuerdo.

Aún y cuando exista una regulación contractual en la normativa, es necesario involucrar los cambios a la hora de ejecutar un contrato electrónico. Con el tiempo han ido surgiendo figuras las cuales no han sido tipificadas y se han convertido parte de la interacción diaria. Fernández brinda un ejemplo cotidiano:

> Son por otra parte, el medio de celebración de múltiples contratos. Encontramos entre ellos a los llamados click-wrap agreements o point-and-click agreements, que basan su validez en el acto de pulsar el botón de aceptación por el usuario, y tienen gran similitud con las licencias shrink-wrap utilizadas en la comercialización de software empaquetado, que se aceptan mediante el desprecinto y la apertura del sobre o envoltorio que contiene los soportes físicos donde va el programa. (Fernández, 2014, p. 416)

Este tipo de contratos corresponden a un gran porcentaje de transacciones diarias. Normalmente son utilizados para términos generales para obtener cierto beneficio. Peligrosamente la mayoría de los usuarios no leen las condiciones antes de pulsar "Acepto", ya que se han acostumbrado a encontrar estos contratos en aplicaciones móviles, videojuegos, redes sociales, compras en línea y en general sitios web donde soliciten que se genere un perfil de usuario que identifique a la persona. También es de suma importancia resaltar que estos acuerdos son válidos por una única vez, es decir, por cada nueva transacción, acuerdo, renovación o negocio involucrado, se requiere una nueva aceptación. Por ejemplo, si un usuario adquiere una membrecía a un sitio de transmisión de películas por internet, deben acceder a los términos y condiciones para el perfil de usuario que generan, sin embargo, si crean un perfil nuevo, con otros datos, nuevamente tendrán que estar de acuerdo con los términos y condiciones.

En Costa Rica se exige a los comerciantes a ser claros en cuanto a los términos y condiciones de la transacción, esto es tutelado en el artículo 250 la ley 7472, donde especifica lo siguiente:

> Artículo 250.- Información sobre la transacción. El comerciante debe informar al consumidor de manera clara y completa acerca de los términos y condiciones de la

> transacción. Los consumidores deben tener acceso fácil a esta información en cualquier etapa de la operación.
>
> Según resulte aplicable y apropiado a la transacción, la información debe incluir los siguientes elementos:
>
> a) el sistema de tratamiento de las reclamaciones adoptado por el comerciante, incluidos los datos de contacto donde se atiendan las quejas del consumidor;
>
> b) los procedimientos de pago, entrega y ejecución;
>
> c) cuando proceda, la fecha para la entrega del bien o el inicio de la prestación del servicio.
>
> d) los términos del contrato en idioma español;
>
> e) las condiciones, el plazo y los procedimientos para ejercer el derecho de retracto;
>
> f) un recordatorio de la existencia de una garantía legal de conformidad para los bienes, así como las condiciones para hacerla valer;
>
> g) cuando proceda, la existencia de asistencia posventa al consumidor, servicios posventa y garantías comerciales, así como sus condiciones;
>
> h) la duración del contrato y, cuando proceda, el plazo mínimo de duración del mismo. Si el contrato es de duración indeterminada o si se prorroga de forma automática, las condiciones para su resolución. (Ley 7472, 1995, Reglamento a la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor)

La importancia en cuanto al respaldo jurídico de los contratos electrónicos radica principalmente en términos de seguridad y responsabilidad mediante una aplicación actual de las leyes existentes.

La protección del usuario en cuanto a seguridad varía ampliamente con respecto a los contratos físicos, ya que los medios para efectuarlos se prestan para diferentes ilícitos. La manipulación contractual de forma electrónica es de más facilidad por la ausencia de las partes a la hora de efectuarse la transacción, abriendo las puertas para delitos como fraudes o suplantación de identidad y haciendo mucho más difícil encontrar a la persona responsable del delito.

El lugar donde se efectúa el contrato también impacta la regulación que debe dársele, ya que si es dentro del mismo país entraría a regir la normativa local, pero si por el contrario, el contrato se realizó entre personas ubicadas en países distintos, entraría a regir el Derecho Internacional Privado.

En cuanto a la consolidación de los contratos por medios electrónicos, se cuenta con la ampliación normativa mediante la Ley modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional la cual en su artículo 11 hace mención a la formación y validez de este tipo de contratos:

> En la formación de un contrato, de no convenir las partes otra cosa, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación un mensaje de datos. (Ley Modelo de la CNUDMI sobre Comercio Electrónico, 1996)

Al tratar el tema de esta consolidación o perfeccionamiento de un contrato electrónico se debe entender que es lo que define en qué momento produciría efecto el acuerdo, lo cual es de suma importancia ya que debe plasmarse y cumplirse con los pagos, productos y entrega, esto nos guía a las diferentes teorías.

En la teoría de emisión se respalda la tesis de que un contrato se considera válido en el momento que el usuario acepte los términos y manifieste una declaración de voluntad. Contrario a esta teoría se puede mencionar la teoría de expedición, la cual indica que un contrato sería válido en el momento que el usuario manifieste su intención, pero a su vez, sea enviada al oferente.

La teoría de recepción indica que un contrato es válido en el momento que oferente recibe esa aceptación. Por último, la teoría de la cognición respalda que un contrato es válido hasta el momento que el oferente recibe la manifestación de la voluntad y esta es de su conocimiento.

Al tratar los casos de contratos electrónicos, se considera que todas esas premisas se cumplen casi que, al instante en la mayoría de las transacciones electrónicas, razón por la cual se respalda la tesis de que el contrato es válido y eficaz en el momento que se confirma la orden. No obstante, en la normativa costarricense se realiza un aporte de mucha importancia en el artículo 254 del Reglamento a la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor:

> Los contratos celebrados por medios electrónicos quedarán perfeccionados desde que se reciba la aceptación de la propuesta o de las condiciones con que ésta fuere modificada. La simple visita al sitio de Internet en el cual se ofrecen determinados servicios o bienes, no impone al consumidor obligación alguna.
>
> El consentimiento solo se entenderá formado si el consumidor:
>
> a) ha tenido previamente acceso a las condiciones generales del contrato, las cuales deben estar expresadas en términos claros, comprensibles e inequívocos;
>
> b) ha aceptado expresamente las condiciones del contrato; y
>
> c) ha contado con la posibilidad de almacenarlas digitalmente y/o imprimirlas.

> Los contratos regulados en el presente capítulo se tendrán por celebrados en el lugar del domicilio del consumidor. Si el consumidor que no reside permanentemente en el país celebra el contrato encontrándose en Costa Rica, podrá decidir que los eventuales diferendos sean conocidos en Costa Rica, aplicándose el Derecho costarricense. (Ley 7472, 1995, Reglamento a la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor)

Como ejemplo existe la compra de artículos en línea. El usuario selecciona los productos que necesita, los cuales se agregan a lo que se conoce comúnmente como "carrito de compras". Seguidamente, cuando está listo, procede a una sección donde se revisa el carrito y se confirma la orden. El siguiente paso es agregar un método de pago y confirmar el pago, lo cual una vez que se completa se procede a completar la orden. Una vez que se acepta el pago y se confirma la orden se está haciendo eficaz el contrato.

Los medios probatorios de este tipo de contratos funcionan muy similar a los contratos comunes. Se recurre al documento electrónico el cual normalmente contiene una firma digital por las partes. De no existir un documento con firma digital se recurriría a otros medios de prueba como conversaciones virtuales, intercambio de correos electrónicos, capturas de pantalla y recibos o facturas digitales entre varios otros.

4.2.1 Clasificación de los contratos electrónicos

La clasificación de los contratos electrónicos se puede realizar de las siguientes maneras:

En cuanto a su ejecución:

- Directo: Se ejecuta por medio de bienes virtuales, los cuales se pueden entregar de forma inmediata mediante la red al no necesitar presencia física de los contratantes ni del artículo.

Un ejemplo de este tipo de bienes puede ser un programa de computadora o una aplicación de celular donde se efectúa el pago y se procede a descargar el contenido.

- Indirecto: Al contrario del contrato directo, los bienes en este tipo son materiales y físicos, por lo cual es necesario hacer entrega de estos al contratante. Por ejemplo, para este tipo de contratos son las compras en línea de artículos para el hogar, donde el comprador debe retirar el producto o se lo hacen llegar a su domicilio.

Por emisión de las declaraciones:

- Puro: La manifestación de la voluntad se realiza mediante medios electrónicos ya sea por aplicaciones, correo electrónico o aceptación de términos y condiciones como se mencionó con anterioridad.
- Mixto: Se da una mezcla en cuanto a esta manifestación de voluntad, donde parte de la transacción sea por un medio electrónico y la otra parte por un medio físico.

Por sus sujetos:

- Consumo: Estos se dan cuando en el acuerdo existe una o más de las partes que sean consumidores.
- Mercantil: El contrato mercantil normalmente se da entre empresas y normalmente equivalen a compras en masa.

Por la forma de pago:

- Electrónico: Este consiste cuando las partes utilizan un medio electrónico para efectuar el pago del servicio o artículo. Puede incluir transferencias bancarias, tarjetas de crédito, monederos virtuales y más.

- Tradicional: Este medio de pago sería mediante efectivo y es poco común hoy en día a la hora de realizar transacciones electrónicas.

Por último, una de las cuestiones más importantes a la hora de realizar un contrato electrónico es la seguridad. Tal y como se ha mencionado en reiteradas ocasiones, a la hora de existir nuevas tecnologías, son mucho más los riesgos a la hora de enfrentar a los cibercriminales. Por este motivo las empresas deben velar por brindar esa seguridad mediante protocolos de protección de datos.

En Costa Rica se exige esa seguridad en el artículo 256 del mencionado reglamento

> Artículo 256.- Seguridad en los medios de pago. Los comerciantes deberán adoptar sistemas de seguridad efectivos, confiables y certificados, con el objeto de garantizar la seguridad, la integridad y la confidencialidad de las transacciones y de los pagos realizados por los consumidores.
>
> El comerciante deberá informar oportunamente en su sitio de Internet sobre:
>
> a) el nivel de protección que se aplica a los datos entregados por los consumidores y las posibles limitaciones de los sistemas de seguridad empleados;
>
> b) la seguridad de los medios de pago y la tecnología que se esté utilizando para proteger la transmisión, procesamiento y almacenamiento de los datos financieros; y
>
> c) el nombre de la entidad certificadora de los sistemas de seguridad. (Ley 7472, 1995, Reglamento a la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor)

El reglamento también protege los datos personales de los usuarios en su artículo 263:

> Artículo 263.- Protección de los datos personales. Los comerciantes están obligados a:
>
> a) adoptar medidas de seguridad eficaces en sus procesos para proteger la integridad, veracidad y confidencialidad de los datos personales existentes en sus bases de datos;
>
> b) informar sobre el nivel de protección que otorgan a los datos personales de los consumidores, en especial en lo relativo a la transmisión, tratamiento y almacenamiento de sus datos personales; y
>
> c) introducir en los contratos que suscriban con otros comerciantes, cláusulas que tengan por objeto proteger la confidencialidad de los datos personales de los consumidores.
>
> Lo anterior sin detrimento de las disposiciones de la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, N º 8968 del 5 de setiembre de 2011.

La contratación y el comercio electrónicos son realidades que continúan en constante crecimiento y forman parte de la vida de la población actual. Es necesario contar con la debida regulación y actualización de la normativa a nivel mundial con el fin de compaginar con las naciones alrededor del mundo. Esto es solo uno de los pocos pasos que toman relevancia a la hora de hablar del Derecho Informático, razón por la cual merita se brinde la debida protección a los consumidores de servicio.

Capítulo 5 - Regulaciones nacionales e internacionales.

5.1 Protección de datos

Si bien la tecnología continúa avanzando día a día en conjunto con el envolvimiento de los usuarios y con sus respectivos usos, ya sea correctos o incorrectos, se ha determinado y analizado el avance y adaptación tanto de los usuarios como los mismos criminales. Por esta razón ha sido necesario implementar diferentes mecanismos de protección en cuanto a datos a nivel global y contar con una regulación de las tecnologías emergentes que forman parte de la vida cotidiana de los usuarios.

La protección al consumidor posee varias ramificaciones tal y como se ha desmenuzado durante el transcurso de la presente investigación, razón por la cual es importante trazar un panorama normativo el cual ha sido trascendental a la hora de alcanzar una debida protección para los consumidores de todos los servicios tecnológicos, virtuales e informáticos con los cuales se cuentan hoy en día.

A nivel internacional, en la región europea se desarrolló el 4 de mayo de 2016 el reglamento General de Protección de datos de la Unión Europea. Si bien este reglamento es aplicable a los países pertenecientes a esta unión, también se incluye a las empresas cuyas sedes radiquen en esta última.

Antes de llegar a esta normativa de amplia importancia, existieron en Europa varias generaciones las cuales fueron desarrollando el tema de protección de datos. Al considerar la primera generación se debe cubrir la protección a la libertad personal, la cual fue fundamental para delimitar los derechos que se fueron desarrollando. Estos derechos también fueron conocidos como derechos individuales, los cuales fueron forjando una delimitación del ser humano como individuo, protegiendo la intimidad.

Entre los años 1960 y 1970 empezó a tratarse con más seriedad la tutela de derechos a la intimidad y protección de la privacidad, por lo cual se considera el inicio de la segunda generación. Se crean leyes de protección de datos las cuales fueron consideradas pertenecientes a la primera generación, sin embargo, quedan fuera de esta última al formar parte del periodo histórico de consolidación normativa. Estas leyes fueron desarrolladas en Hessen, Alemania y en Suecia, esta última en 1973, dirigida principalmente a los sistemas de información donde se prevenía a las autoridades el acceso a el registro de datos personales utilizados y almacenados como tratamiento de datos automatizado.

Entrando en la década de los años 80, el 28 de enero de 1981 específicamente, se crea el Convenio sobre Datos Personales del Consejo de Europa, dando inicio a lo que se conoce como la tercera generación de protección de datos. Este último fue de suma importancia, ya que su objetivo era lograr una uniformidad a la protección extendiendo su cobertura a varios países los cuales fueron adaptando y acoplando la debida protección jurídica que se pretendía tutelar. Estos esfuerzos lograron que la protección de datos fuera considerado un derecho fundamental según el Consejo de Europa, abriendo paso a nuevas normativas y expansión de su tutela. Una de estas fue la Ley de Registros de Datos Personales de 1987, la cual fue la primer ley de este índole en Finlandia.

Una de las principales problemáticas con el mencionado convenio europeo radicaba en su obligatoriedad. Muchos de los países, a pesar de su existencia, no lo consideraban de carácter mandatorio, razón por la cual fue necesario modificar y delimitar mucho más la normativa, dando inicio a la siguiente generación. Como soporte a este crecimiento, la Unión Europea focalizó esfuerzos para intentar cubrir los vacíos legislativos, lo cual sorpresivamente fomentó el libre tránsito de los datos personales.

En 1992 se generó un proyecto rechazado por el Parlamento Europeo bajo muchas críticas y comentarios desvirtuando el esfuerzo, lo cual al ser corregido se logró, en 1995, incorporar la

Directiva sobre tratamiento de datos personales, logrando con esto un hito histórico el cual conllevaría al inicio de la cuarta generación, esta última contando con un gran apoyo por parte de la Unión Europea, la cual oficializó de carácter mandatorio el cumplimiento de las normas plasmadas en la Directiva, ayudando de esta manera a la implementación del comercio electrónico, lo cual no se cumplió tres años después, razón por la cual la Comisión inició procesos ante cinco países, incluidos Francia y Alemania. Progresivamente los países fueron implementando esta directiva en su gran mayoría.

No obstante, es la República Federal de Alemania una de las grandes impulsoras con aportes muy valiosos a la protección de datos mediante la conocida sentencia del Tribunal Constitucional Federal el 15 de Setiembre de 1983, logrando el reconocimiento en este tema por varios otros países configurando la intimidad como un derecho en relación con la autodeterminación informativa y marcando un hito mediante la Ley de Censo de Población de 1982, mencionada en capítulos anteriores.

Por otro lado, en América Latina hubo dos países pioneros en cuanto a la protección de datos y esto se debió a las amenazas y retos percibidos en cuanto a procesos informáticos. Por ejemplo, la Constitución política de Perú protege directamente el derecho a la privacidad en ámbitos informáticos y tecnológicos, brindando protección a la intimidad personal y familiar en su artículo 2 inciso 6. El segundo país en regular esta protección en su Constitución fue Venezuela en su artículo 60, donde la ley específicamente protege la intimidad limitando los usos informáticos.

Es importante recalcar que, al igual que sucedió en Europa, la implementación de esta protección fue prácticamente a ojos cerrados y sin ninguna noción del alcance que iba a tener la informática en la actualidad. Muchos otros países si tomaron en consideración la protección de datos, mas no incluyeron en su momento normativas que respaldaran un posible desarrollo informático.

5.2 Protección al consumidor

Por otro lado, Estados Unidos como una de las grandes potencias mundiales en el orbe, no se quedó atrás en cuanto a normativas de protección al consumidor contando con varias leyes que amparan a estos últimos.

Uno de los aspectos más importantes cuando se menciona la Ley de la Comisión Federal de Comercio es el hecho de que La Oficina de Protección al consumidor trabaja apegada a esta. Fue creada en 1914 para dar un soporte jurídico a la competencia injusta, sin embargo, esta comisión no trabaja con temas individuales de consumidor sino más bien ilícitos en conjunto.

Esta comisión realiza denuncias a los Tribunales como última instancia, ya que primeramente negocia con los transgresores. Normalmente trabajan con denuncias en conjunto, tales como reportajes, columnas o artículos en los cuales varios consumidores expresen su malestar. Seguidamente contactan a la empresa que esté cometiendo el injusto, con el fin de negociar o llegar a un acuerdo del cese de las actividades que estén afectando a los consumidores. Si la empresa no acoge las medidas e implementa las soluciones, se envía el caso a los Tribunales quienes decidirán la acción a tomar.

Un aspecto muy importante con respecto a la Comisión Federal es el hecho de que cuentan con una serie de recomendaciones para las empresas con el fin de que eviten varios tipos de abuso a los consumidores a la hora de efectuar transacciones comunes.

Después de creada la Ley de Protección del Crédito al consumo en 1968, la Ley sobre la Verdad en los Préstamos fue creada para brindar un apoyo jurídico a los consumidores en cuanto al costo final a la hora de adquirir un crédito, obligando a los prestamistas a incluir la carga financiera y el porcentaje anual. Por medio de esta se permite no solamente la publicidad para los adquirentes si

no el derecho de poder rescindir el contrato de crédito cuando la principal garantía es su vivienda actual.

La Ley del Leasing al Consumo se convierte en una disposición añadida a la Ley Sobre la Verdad en los Préstamos buscando una debida representación de los costos en los alquileres de bienes de consumos duradero, exigiendo una descripción detallada de los contratos de leasing con el fin otorgar a los usuarios la potestad de comparar los servicios con otros oferentes.

La Ley de Igualdad de Oportunidades de Acceso al Crédito es un medio de tutela a la igualdad entre los consumidores. Con esta se tipifica la ilegalidad a la hora de que exista discriminación por parte de un prestamista en cuanto a género, religión, nacionalidad o edad.

Una normativa de suma importancia la cual brindó un respaldo a la mala utilización de las tarjetas de crédito con fines ilícitos, eximiendo de responsabilidad a los titulares posterior a la notificación de estos últimos, fue la Ley Sobre Uso Indebido de Tarjetas de Crédito. En otras palabras, si el tarjetahabiente reporta un robo o pérdida de tarjeta de crédito, cualquier transacción que se realice después de este reporte queda totalmente invalidad brindando a la entidad financiera la responsabilidad en el caso de que la tarjeta fuera utilizada.

La Ley Sobre Información Exacta del Riesgo brinda al consumidor la potestad de tener a suu disposición la información disponible a la entidad financiera. Esta ley protege también el conocimiento de dicha información con respecto a historiales crediticios y las personas que han tenido acceso a esa información en los últimos 6 meses o 24 meses en el caso de que se deba a una solicitud de empleo.

Si existiera la denegación de un crédito o préstamo, es responsabilidad del prestamista hacer saber a quién solicita el préstamo la razón de la negativa.

En situaciones donde se presenten cargos en el cobro, cuando exista algún rubro que deba revisarse o que el usuario considere que es errónea, están amparados por la Ley del Cálculo Correcto para aclarar los cobros recibidos.

Costa Rica se empezó a enfrentar a cambios y progreso en cuanto al desarrollo comercial, siendo parte de tratados de libre comercio y apertura de mercados internacionales. Por esta razón fue creada la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, la cual entró en vigencia en 1995, brindando un respaldo jurídico y normativo a la desregulación, competencia y apertura comercial.

Esta ley fue de suma importancia ya que logró que se reformara el artículo 46 de la Constitución Política, brindando un respaldo constitucional al consumidor al añadir al artículo el siguiente extracto:

> Los consumidores y usuarios tienen derecho a la protección de su salud, ambiente, seguridad e intereses económicos; a recibir información adecuada y veraz; a la libertad de elección, y a un trato equitativo. El Estado apoyará los organismos que ellos constituyan para la defensa de sus derechos. La ley regulará esas materias. (Constitución Política de la República de Costa Rica. Art. 46. 8 de noviembre de 1949)

Costa Rica se empezó a enfrentar a cambios y progreso en cuanto al desarrollo comercial, siendo parte de tratados de libre comercio y apertura de mercados internacionales. Por esta razón fue creada la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, la cual entró en vigencia en 1995, brindando un respaldo jurídico y normativo a la desregulación, competencia y apertura comercial.

5.2.1 Comercio electrónico y protección al consumidor

Con la integración y facilitación del comercio electrónico en la vida cotidiana y el desarrollo de la tecnología a nivel mundial, fue necesario empezar a regular la incursión en los nuevos panoramas tecnológicos, brindando modelos internacionales que marcaron una pauta importante.

Una de estas normativas es la Ley Modelo sobre Comercio Electrónico de la Comisión de

las Naciones Unidas para el Derecho Mercantil Internacional , aprobada en Nueva York en 1996 con el objetivo de lograr una solidez jurídica en cuanto a la relación de las estructuras tecnológicas nuevas y el Derecho Mercantil aplicado a estos medios electrónicos. Principalmente, logrando plasmar por escrito un documento regulando estas diferentes actividades comerciales.

La importancia de esta ley radica principalmente en la disponibilidad de normas que se pudieran aplicar y acoplar a los diferentes sistemas judiciales internacionalmente. Con esto se pudo disminuir las dudas o inquietudes que podían generarse con la inclusión de este nuevo término comercial referido a lo electrónico.

Asimismo, se define y abarcan alcances y definiciones, dando primeramente al término de "comercial" una amplitud al incluir actividades comerciales, contractuales o extracontractuales, añadiendo toda relación de índole comercial.

Esta Ley Modelo también se encargó de tutelar el alcance del comercio electrónico cubriendo todo tipo de transmisión de datos por medios tecnológicos de la época y algunos utilizados hoy en día, tal y como lo menciona Fernandez:

> La Ley Modelo es aplicable a toda forma de mensaje de datos, es decir, información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, que se utilice en el contexto de actividades comerciales. Entre

> los medios de comunicación recogidos en el concepto de "comercio electrónico" cabe citar las siguientes vías de transmisión basadas en el empleo de técnicas electrónicas: la comunicación por medio del EDI definida en sentido estricto como la transmisión de datos de una terminal informática a otra efectuada en formato normalizado; la transmisión de mensajes electrónicos utilizando normas patentadas o normas de libre acceso; y la transmisión por vía electrónica de textos de formato libre, por ejemplo, a través de la INTERNET. Se señaló también que, en algunos casos, la noción de "comercio electrónico" sería utilizada para referirse al empleo de técnicas como el télex y la telecopia o fax. (Fernández, 2014, p. 475)

Es importante resaltar que la Ley Modelo no cubre detalles en cuanto al comercio electrónico y es una guía para que los países que la acojan puedan definir una normativa más detallada tomando en cuenta las consideraciones que plasma dicha ley.

Otra pilar en cuanto al comercio electrónico es la Directiva Europea sobre Comercio Electrónico, en la cual principalmente se buscaba definir una regulación en este tema a nivel focalizado en Europa.

Esta Directiva se encarga en dar un foco a las regulaciones existentes y concatenar cuidadosamente los aspectos más importantes a cubrir, dejando de lado aspectos que resultaran confusos o dispares tanto normativos como jurisprudenciales, sin dejar de lado la inclusión de todos los servicios actuales referente a las empresas. Cabe resaltar que se hacía enfoque a los servicios en línea aplicados por prestadores de servicios ubicados solamente en la Unión Europea.

En la directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 se introducen 10 cambios de suma importancia reforzando el cuerpo jurídico que apoya a los

consumidores a la hora de realizar compras en línea. Esta directiva es de extrema importancia ya que estos 10 cambios sirven como base no solamente para la creación de cuerpos normativos a nivel mundial, si no como una protección con una amplia visión a los cambios de la actualidad y sobrevinientes.

En primera instancia se protege a los consumidores ante posibles engaños en cuanto al precio final de un producto eliminando cualquier monto oculto tal y como publicidad engañosa o páginas donde ofrecen un servicio gratuito el cual al final terminan cobrando, haciendo necesario que los usuarios confirmen y acepten el precio que están pagando, confirmando el costo involucrado.

De la mano con el rubro anterior se exige al comerciante incluir en el monto final todos los cobros involucrados a la transacción. Con esto se refiere a que no pueden incluirse cobros complementarios si no han sido informados antes de que el usuario realice una confirmación de su compra.

Algunos sitios web solían marcar ciertas casillas de términos y condiciones de manera predeterminada, incurriendo en un engaño a los consumidores. Estas casillas podían incluir desde servicios adicionales, con su debido costo incluido, hasta aceptación de acuerdos no informados al usuario. Esta directiva realiza una prohibición ante estas casillas marcadas por defecto, sin embargo, hay muchos sitios que aún las utilizan.

Anteriormente se brindaba al consumidor 7 días para desistir de una compra, amparando a estos a devolver el artículo comprado ante un cambio de opinión, descontento o insatisfacción. Mediante esta directiva se amplía ese término a 14 días contados a partir del momento en que el consumidor recibe la mercancía.

De la mano con el derecho al desistimiento se desarrolla el derecho al reembolso, haciendo responsable al comerciante a cubrir cualquier defecto en el artículo, así como daño en el transcurso de la entrega, cubriendo todos estos rubros en el caso de que el comprador quisiera un rembolso.

Ante el desistimiento también se pone a mano de los consumidores un formulario aplicable a toda la Unión Europea, facilitando el proceso sin importar el lugar donde se haya celebrado el contrato.

Existió un tiempo donde los comerciantes cobraban un monto extra o porcentaje cuando se realizaba una compra por tarjeta de crédito como medio de pago. Este rubro fue prohibido, obligando al vendedor a cobrar un monto equitativo sin importar el método de pago que fuese utilizado.

Ante una eventual devolución del producto, es necesario que el comerciante plasme los términos y los ponga a disposición y conocimiento del cliente. Estos montos deben ser brindados por adelantado como un estimado máximo, asumiendo, de lo contrario, los costos en su totalidad el mismo.

De los puntos más importantes tratados en esta directiva es la protección a los consumidores frente a los productos digitales. Actualmente los servicios digitales son cada día más populares, habilitando cada día más plataformas para acceder a este contenido. Hoy en día los videojuegos, películas, programas de computadora y aplicaciones han engrandecido un mercado digital de manera impactante. Mediante la directiva se establece una estructuración para obligar a los vendedores a ser claros con la información que contiene esa compra digital tal y como requisitos técnicos, detalles del contenido y posibles limitaciones entre muchas otras. Para comprar un videojuego en línea, la plataforma incluye el sistema operativo, capacidad de almacenamiento, memoria requerida y capacidad de gráficos requeridos a la mano del consumidor para que este

pueda contar con la información necesaria para determinar si es posible la compra. Un aspecto importante con respecto a este punto es el hecho de que el desistimiento estará limitado al momento en que el usuario empieza a descargar el contenido.

Finalmente, dentro de los 10 cambios estipulados se citaban las normas comunes que facilitaban la venta de productos en Europa. Entre estas se encuentran las normas que regulan las transacciones a distancia tales como correo electrónico o internet entre otras ya no tan utilizadas como las ventas por teléfono. Se regula la competencia equitativa dentro de la Unión Europea y se da la implementación de formularios para facilitar las transacciones en cuanto al desistimiento.

El 9 de diciembre de 1999 se aprobaron las Directrices para la Protección al Consumidor, aplicable al comercio electrónico entre proveedores y consumidores solamente. Dentro de estas recomendaciones se rescata el reforzamiento de la honestidad a la hora de realizar el mercadeo y publicidad de los productos, evitar cláusulas abusivas en los contratos, protección nivelada de los consumidores con la de transacciones realizadas en otras áreas de comercio, la habilitación de la disponibilidad de la información real de las partes involucradas en el negocio así como el deber de identificar correctamente el bien con sus respectivos detalles y facilidad de acceso a estos. También se propone la regulación de todos la información referente a la transacción como los costos, tiempo de entrega, instrucciones, descripción, garantía del producto e impuestos.

Otras recomendaciones fueron brindar la posibilidad la posibilidad al consumidor de cancelar una orden o corregir posibles errores efectuados durante la transacción, así como brindar a estos métodos de pago sencillos y contando con los métodos de seguridad pertinentes para proteger su información.

Dentro de la legislación costarricense se cuenta con una amplia ley protectora a los consumidores la cual ha regido desde 1995. El objetivo de ley es claro en su artículo 1:

> El objetivo de la presente Ley es proteger, efectivamente, los derechos y los intereses legítimos del consumidor, la tutela y la promoción del proceso de competencia y libre concurrencia, mediante la prevención, la prohibición de monopolios, las prácticas monopolísticas y otras restricciones al funcionamiento eficiente del mercado y la eliminación de las regulaciones innecesarias para las actividades económicas. (Ley 7472, 1995, Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor)

La ley es bastante eficaz y a su vez lo suficientemente amplia para cubrir parámetros necesarios en cuanto a la protección y regulación que brinda, acaparando un aspecto global del consumidor en términos generales. Aún y cuando en los últimos años se haya brindado ese soporte jurídico y haya funcionado de manera eficiente, la mencionada globalización tecnológica y la inclusión del desarrollo de las tecnologías informáticas es un tema que debe ir tomándose en cuenta antes de que este absorba la realidad actual del país.

En su artículo segundo, la misma ley aclara los derechos del consumidor tutelados:

> (…) son derechos fundamentales e irrenunciables del consumidor, los siguientes:
>
> a) La protección contra los riesgos que puedan afectar su salud, su seguridad y el medio ambiente.
>
> b) La protección de sus legítimos intereses económicos y sociales.

> c) El acceso a una información, veraz y oportuna, sobre los diferentes bienes y servicios, con especificación correcta de cantidad, características, composición, calidad y precio.
>
> d) La educación y la divulgación sobre el consumo adecuado de bienes o servicios, que aseguren la libertad de escogencia y la igualdad en la contratación.
>
> e) La protección administrativa y judicial contra la publicidad engañosa, las prácticas y las cláusulas abusivas, así como los métodos comerciales desleales o que restrinjan la libre elección.
>
> f) Mecanismos efectivos de acceso para la tutela administrativa y judicial de sus derechos e intereses legítimos, que conduzcan a prevenir adecuadamente, sancionar y reparar con prontitud la lesión de estos, según corresponda.
>
> g) Recibir el apoyo del Estado para formar grupos y organizaciones de consumidores y la oportunidad de que sus opiniones sean escuchadas en los procesos de decisión que les afecten. (Ley 7472, 1995, Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor)

Nótese que, aún y cuando la ley lleva varios años en vigencia, se cubren aspectos muy importantes aplicables al desarrollo electrónico tales y como los mencionados en cuanto a la protección de información veraz, publicidad engañosa y clausulas abusivas entre otros. El único problema es que, al no mencionar directamente las transacciones virtuales, podría prestarse para malentendidos o vacíos legales en un futuro. Un ejemplo es la regulación de los contratos de click-wrap agreements o point-and-click agreements cubiertos previamente en la presente investigación.

La ley costarricense de igual manera exige a los comerciantes a cumplir ciertas pautas cubiertas en su artículo 34 donde se cubre principalmente la información veraz, clara y actualizada, así como los detalles del producto, plazos (en los casos que el pago sea a crédito o a tractos), intereses y otros cargos así como los saldos, instrucciones de los artículos, si la mercadería vendida es usada o nueva y el otorgamiento de factura en todas las compras.

Esta protege ámbitos detallados tales y como la aplicación de promociones, ofertas y regulación de estas y un artículo muy importante es el 17, donde se regula la competencia desleal:

> Entre los agentes económicos, se prohíben los actos de competencia contrarios a las normas de corrección y buenos usos mercantiles, generalmente aceptados en el sistema de mercado, que causen un daño efectivo o amenaza de daño comprobados. Esos actos son prohibidos cuando:
>
> a) Generen confusión, por cualquier medio, respecto del establecimiento comercial, los productos o la actividad económica de uno o varios competidores.
>
> b) Se realicen aseveraciones falsas para desacreditar el establecimiento comercial, los productos, la actividad o la identidad de un competidor.
>
> c) Se utilicen medios que inciten a suponer la existencia de premios o galardones concedidos al bien o servicio, pero con base en alguna información falsa o que para promover la venta generen expectativas exageradas en comparación con lo exiguo del beneficio.
>
> d) Se acuda al uso, la imitación, la reproducción, la sustitución o la enajenación indebidos de marcas, nombres comerciales, denominaciones de origen, expresiones

> de propaganda, inscripciones, envolturas, etiquetas, envases o cualquier otro medio de identificación, correspondiente a bienes o servicios propiedad de terceros.
>
> También son prohibidos cualesquiera otros actos o comportamientos de competencia desleal, de naturaleza análoga a los mencionados, que distorsionen la transparencia del mercado en perjuicio del consumidor o los competidores.
>
> Los agentes económicos que se consideren afectados por las conductas aludidas en este artículo solo podrán hacer valer sus derechos en la vía judicial por el proceso ordinario. Lo anterior, sin perjuicio de los procedimientos administrativos y judiciales, que se realicen para proteger al consumidor por los efectos reflejos de los actos de competencia desleal, en los términos del inciso b) del artículo 53 de esta ley. (Ley 7472, 1995, Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor)

La ley también cubre un aspecto especial digno de recalcar el cual se refiere a la educación a los consumidores, atribuyendo al Poder Ejecutivo la potestad de formular programas los cuales ayuden al consumidor a protegerse a sí mismo ante irregularidades a la hora de efectuar transacciones. A opinión, es de suma importancia que estas capacitaciones incluyan información acerca del consumo virtual, tomando en consideración la cantidad de estafas aplicadas por delincuentes gracias a las facilidades de comunicación con las cuales se cuentan en la actualidad y teniendo presente que estas se pueden evitar en su gran mayoría con un consumidor preparado e informado.

Por otro lado, al hablar del Comercio electrónico, aún y cuando la población costarricense se amparaba bajo la Ley de protección al consumidor, Código Civil y Código de Comercio, la transformación jurídica tomó un paso muy importante con la creación del Reglamento a la Ley de

Promoción de la Competencia y Defensa Efectiva del Consumidor, integrando en el año 2017 un capítulo exclusivo a la tutela del Comercio Electrónico cuyos artículos se han mencionado previamente en la presente investigación.

5.3 Regulación a la protección de datos en Costa Rica

Normalmente en nuestro país, el tema de la protección de datos y los derechos relacionados a esta se entiende como una extensión del Derecho a la Intimidad, el cual es regulado en la Constitución Política mediante el artículo 24 y haciendo alusión internacionalmente a la Declaración Universal de Derechos Humanos en su artículo 12 y Convención Americana de Derechos Humanos en el artículo 11.

En la normativa nacional se desarrolló desde el año 2011 la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales para asegurar la protección de Derechos Humanos, autodeterminación informativa e información privada de carácter personal. Esta ley ha dejado por fuera regulaciones importantes como el Hábeas Data per se y varias pauta en cuanto a la protección de datos electrónicos por fuera, los cuales, aún y cuando se puedan incluir en la regulación actual, dadas las circunstancias de sus cambios, podría ocasionar vacíos legales en algún momento.

Actualmente no existe ninguna ley que se refiera al Hábeas Data aún y cuando se haga mención en algunos recursos jurisprudenciales pertenecientes a la Sala Constitucional, otorgando una noción escasa y desactualizada de este medio y generando una necesidad imperante de protección de los datos personales y utilización de estos.

Un punto lamentable que contribuye a la falta de regulación ha sido el tiempo tan largo que ha tomado su inclusión por parte de la Asamblea Legislativa debido a la tardanza en el sistema de aprobación de leyes.

Tal es el caso que en el año 1996 se presentó el proyecto de ley mediante la tramitación del expediente n 12.827 en la Asamblea Legislativa.- El proyecto de "Adición de un nuevo Capítulo IV, titulado 'Del recurso de hábeas data', al Título III de la Ley de la Jurisdicción Constitucional, ley N 7185 del 19 de octubre de 1989."

Este proyecto se refería puntualmente a el tránsito de información mediante la red y la cantidad de datos personales que son transmitidos a diario enfocándose en el peligro en cuanto a discriminaciones, acceso a la intimidad, perjuicios económicos y laborales y violación de derechos de personalidad, imagen y honor, relacionando estos con la autodeterminación informativa.

El proyecto se respaldaba de la siguiente manera:

> Con los avances de la tecnología se hace más difícil llevar a cabo este control. En materia de datos personales, al ponerse en peligro distintos derechos de la personalidad, se dificulta la determinación de cual información está siendo recolectada, para qué fines, en qué forma y quiénes pueden acceder a ella.
>
> Es por ello que los legisladores ordinarios y constituyentes de nuestro tiempo deben buscar fórmulas jurídicas que permitan limitar o controlar el uso del poder informático. En Costa Rica, no queriendo permanecer al margen de esta problemática tan actual y haciéndose eco de las Recomendaciones emitidas en las anteriores Conferencias de Ministros de Justicia de los Países Iberoamericanos, en sentido de adoptar medidas legislativas encaminadas a proteger eficazmente los derechos de las personas afectadas por el uso de ordenadores tanto a nivel gubernamental como privado, recientemente ha impulsado en el seno de la Asamblea Legislativa un proyecto de ley (el número 12827) tendiente a garantizar

> el derecho a la autodeterminación informativa mediante el instrumento procesal conocido como HABEAS DATA, el cual ha sido reconocido por la doctrina, la jurisprudencia y las legislaciones avanzadas como garante de aquél derecho fundamental. (Proyecto de Ley No. 12.827, 1998)

El proyecto se basa en un estudio internacional el cual se adapta a la realidad que enfrentaba Costa Rica en ese entonces, por lo cual se puede medir el grado de magnitud que ha adquirido tomando en consideración que fue creado hace más de 20 años.

Entre los principales cambios, imperan la inclusión del objeto del recurso Hábeas Data refiriéndose principalmente a la autodeterminación informativa y libertad informática con relación a los datos personales. En su artículo 81 también pretende actualizar ciertas definiciones utilizables únicamente al momento de referirse al recurso como tal.

> Datos Personales: cualquier información concerniente a personas físicas o jurídicas identificadas o identificables.
>
> Tratamiento de datos: son las operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recolección, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
>
> Responsable del Fichero: Persona física o jurídica, de naturaleza pública o privada y órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento. Afectado: Persona física o jurídica titular de los datos que sean objeto del tratamiento automatizado o manual (Proyecto de Ley No. 12.827, 1998).

Otro de los principales cambios se refieren a diferentes principios a respetar a la hora de tratar con datos personales tales como la calidad de los datos, mantener los fines para los cuales se recogieron, actualización y mantenimiento de datos reales y precisos, almacenamiento de datos personales con un fin específico solamente, disponibilidad de los datos al usuario dueño de estos, prohibición de recolección de datos fraudulentos o con fines ilícitos, actualización al usuario con respecto al uso de sus datos y consentimiento del interesado para tratar con estos datos personales.

El proyecto también incluye los casos en que pueda plantearse el recurso de Hábeas Data en el artículo 72, principalmente protegiendo a las personas físicas o jurídicas con ánimo de conocer información personal que se mantenga en registros, finalidad de los datos, rectificación, actualización, inclusión, confidencialidad o cancelación. También regula la solicitud de información declarada secreto de Estado y la aplicación del recurso mediante actos administrativos.

Actualmente se cuenta con el Recurso de Amparo como defensa de derechos fundamentales, y la Sala ha manejado este tipo de recursos con énfasis en Hábeas Data haciendo referencia al concepto integrado en el Derecho Internacional sin embargo alegar que con este recurso se cubren las necesidades de la población en cuanto a la tutela de sus derechos no es correcto ni suficiente, aspecto que se respalda en la sentencia:

> A pesar de que en principio el hábeas data fue concedido en la protección del derecho a la información, el registro de datos considerados sensibles, como los relativos a las inclinaciones políticas, religiosas, al color de piel, a las inclinaciones sexuales, a la salud de la persona interesada o a las afiliaciones sindicales o políticas, si se realizan de manera nugatoria de la autodeterminación informativa podría fomentar tratos discriminatorios, por lo que este instrumento procesal debió

> ser ampliado como un mecanismo de control efectivo sobre la información que ya ha sido consignada en bancos de datos electrónicos y manuales. La existencia de datos sensibles y la posibilidad de que se manifiesten conductas discriminatorias con su manejo, entendiendo por discriminación el darle un trato a alguien no teniendo en cuenta su situación objetiva sino en función de sus rasgos como el sexo, situación familiar, color de piel, pertenencia o no a una determinada raza, etnia o religión, opinión política o gremial, ideología, origen nacional o social, posición económica, estado civil, condición física, enfermedad, elección sexual o procedimientos judiciales pendientes o finiquitados, ha marcado también un punto importante en la evolución de este instituto. (Sala Constitucional, 05802 - 1999, 1999)

A esto se le agrega un ejemplo de la utilización de los recursos de amparo en vez de un hábeas data debido a la falta de normativa:

> En la especie, el gestionante utiliza la vía sumaria del recurso de amparo a fin de hacer valer su derecho de autodeterminación informativa. No estando previsto en el ordenamiento jurídico costarricense el recurso de "hábeas data" u otro mecanismo procesal específico para la protección de este derecho, la Sala considera que se está ante uno de los supuestos genéricos previstos por los artículos 48 de la Constitución Política y 29 de la Ley de la Jurisdicción Constitucional. El amparo es por ende la vía idónea para discutir la constitucionalidad de este tipo de actuaciones, donde están de por medio la intimidad, el resguardo de datos sensibles -entendidos éstos como aquellos datos que tienen una particular capacidad de afectar la privacidad del individuo o de incidir en conductas discriminatorias- y la

> no lesividad de su uso; es decir, resguardando el derecho a la autodeterminación informativa. (Sala Constitucional, 01435 - 2003, 2003)

Entonces, es claro que la tutela de los derechos a la protección de datos calza dentro de los derechos fundamentales y , aunque existan mecanismos de defensa, es imperante que la legislación de nuestro país cubra con detalle los cambios constantes que conlleva la evolución jurídica. Es claro que es un derecho de la población de contar con los debidos recursos jurídicos para su debida protección mediante el principio constitucional de “tutela judicial efectiva” y “justicia pronta y cumplida” localizados en el artículo 41 de nuestra Constitución Política por lo cual contar con una riqueza normativa permite proporcionar el mejor respaldo a los usuarios y población en general.

Conclusiones

Se ha determinado la importancia de la inclusión y evolución tecnológica en los tiempos actuales tanto en materia social como en materia legal. Siendo el objetivo principal del Derecho conformar normas y principios para regular y fomentar la armonía a nivel mundial, se ha establecido y demostrado la importancia que hay en su debida adaptación y actualización.

La población ha confiado en el sistema jurídico a través de los años, el cual ha brindado la protección y seguridad a las personas siempre incurriendo en cambios y basándose en la realidad social y demográfica.

Mencionada la importancia del Derecho y la adaptación de este a la realidad actual, se llega a una serie de conclusiones, basadas en el estudio de aspectos históricos, actuales, normativos y jurisprudenciales, los cualescuales, concatenados, brindan un entendimiento amplio del Derecho Informático y sus ramas, logrando establecer una base sólida de los aspectos regulados y los aspectos que se necesitan mejorar.

Mediante el estudio de la normativa internacional y el Derecho Comparado se permite enriquecer la perspectiva y la situación actual del globo, manteniendo el enfoque del estudio en varias potencias mundiales las cuales cuentan con un sistema jurídico amplio y bastante avanzado.

Se consideró necesario el entendimiento del impacto del Derecho Informático y sus generalidades, así como los diferentes delitos cibernéticos relacionados, al tener en consideración que los consumidores no son solamente las personas que adquieren un producto físico o virtual si no que son todos aquellos que tienen contacto con la red y consumen los servicios de internet.

Al conceptualizar y profundizar en la procedencia e importancia del Derecho Informático en la sociedad actual, se logra brindar una concientización de la necesidad de ampliar esta rama del

Derecho la cual aún se considera en pleno desarrollo, adquiriendo cada día más importancia a nivel nacional cuando pretendemos un marco jurídico amplio y que proteja la mayor parte de retos presentes en el día a día.

Dentro del estudio se realizó un amplio análisis de los diferentes ilícitos que han evolucionado con la creación de los medios tecnológicos, los cuales brindan una inseguridad a los usuarios y consumidores de servicios a través de la red así como su debida protección a nivel nacional.

Al analizar la protección al consumidor en zonas como Europa, Estados Unidos y países cercanos de Latinoamérica, se logró brindar una comparación con nuestro sistema jurídico, ayudando a verificar las áreas de mejora y reforzando la protección actual utilizando el Derecho Comparado e Internacional.

El aspecto histórico estudiado permitió engrandecer los procesos evolutivos en cuanto a la inclusión de los temas tecnológicos y a su vez dar una noción realista de la protección que se ha brindado desde hace varios años atrás en cuanto a estos mismo. El estudio de esta historia también brindó una guía de los esfuerzos que han tomado los legisladores, tanto internacional como nacionalmente, para desarrollar una base jurídica que proteja el involucramiento del aspecto electrónico y virtual en las regulaciones actuales.

Con el estudio del origen de la privacidad y el progreso en cuanto a datos personales, antes incluso de la globalización de la red, fue posible entender la importancia de estos como derechos fundamentales y el impulso que se ha tenido con respecto al valor de su protección. Al tener esa comprensión, se desarrolla un estudio amplio en cuanto al involucramiento de las bases de datos y sistemas tecnológicos de almacenamiento, los cuales se han ido regulando en los cuerpos normativos con el transcurso de los años. Se mencionan mecanismos de protección de gran calibre

como lo son la autodeterminación informativa, el hábeas data y diferentes estatutos internacionales que se han encargado de acuerpar las diferentes legislaciones y su debida inclusión en el derecho costarricense, reafirmando lo importante de su inclusión e impulso para poder contar con una protección jurídica actual, basada en los principios constitucionales de "justicia pronta y cumplida" y "tutela judicial efectiva".

Por último, la inclusión y respaldo de las sentencias nacionales permiten un análisis jurisprudencial enriqueciendo los conceptos estudiados. Por otro lado, existe una relación estrecha con los cuerpos normativos existentes, logrando brindar un punto de vista en cuanto a mejoras necesarias y vacíos legales que puedan mejorar para brindar mayor solidez a la protección jurídica nacional.

Si bien hace muchos años se veía distante la inclusión de las ciencias tecnológicas en materias de derecho, en la actualidad se ha convertido en una realidad cambiante y necesaria. El estudio del Derecho Informático es una necesidad imperante la cual no solo debe actualizarse con la situación social actual, si no con las situaciones venideras. No solo se trata de tener normas que cubran el ámbito presente, si no intentar prever y prepararse para los cambios a futuro, tomando en cuenta los pasos agigantados que ha tomado esta evolución tecnológica.

Bibliografía

- Acurio Del Pino, S. (s.f.). *Delitos informáticos: generalidades*. Recuperado de: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
- Ahón, E.I. (2005). *Estado situacional y perspectivas del derecho informático en América Latina y el Caribe*. Recuperado de: https://www.cepal.org/sites/default/files/publication/files/31919/S2005728_es.pdf
- Bauzá Reilly, M. (1996). *Responsabilidad civil en materia informática.* Informática y derecho: Revista iberoamericana de derecho informático. https://doi.org/10.26439/iusetpraxis1996.n026.3547
- Bazán, Víctor (2005). *El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado*. Estudios Constitucionales, 3(2),85-139. ISSN: 0718-0195. Recuperado de: https://www.redalyc.org/articulo.oa?id=82030204
- Bru Cuadrada, Elisenda (2007). *La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad*. IDP. Revista de Internet, Derecho y Política, (5),78-92. ISSN: 1699-8154. Recuperado de: https://www.redalyc.org/articulo.oa?id=78812861008
- Cerda Silva, A. (2003). *Autodeterminación informativa y leyes sobre protección de datos.* Revista Chilena de Derecho Informático, (3), 47-75. doi:10.5354/0717-9162.2011.10661
- *Código Penal de Costa Rica*. Ley 4573 , 1970. 4 de mayo de 1970.
- Comunicado página presidencial de Costa Rica. (2 de marzo, 2020). *Trabajo a partir de la ciencia de datos ha sido en beneficio de la mayoría de las personas*. Presidencia. https://www.presidencia.go.cr/comunicados/2020/03/trabajo-a-partir-de-la-ciencia-de-datos-ha-sido-en-beneficio-de-la-mayoria-de-las-personas/

- *Constitución Política de Costa Rica* [Const]. Art. 46. 8 de noviembre de 1949 (Costa Rica).
- Díaz Gómez, A. *El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest* , REDUR 8, diciembre 2010, págs. 169-203. ISSN 1695-078X
- Fernández Delpech, H. *Manual de Derecho Informático*. - 1a ed. - Ciudad Autónoma de Buenos Aires: Abeledo Perrot, 2014.
- Gamba, Jacopo, 2010. *Panorama del derecho informático en América Latina y el Caribe*. Documentos de Proyectos 302, Naciones Unidas Comisión Económica para América Latina y el Caribe (CEPAL). Recuperado de: https://repositorio.cepal.org/bitstream/handle/11362/3744/S2009865_es.pdf?sequence=1&isAllowed=y
- Garcia Gonzalez, Aristeo. *La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado*. Bol. Mex. Der. Comp. [online]. 2007, vol.40, n.120, pp.743-778. ISSN 2448-4873.
- Guillén Mora. I. 2012. *La protección de los consumidores contra el engaño y la falta de información*. Revista El Foro, 12.32-45. Recuperado de: https://www.yumpu.com/es/document/read/11152737/colegio-de-abogados-y-abogadas-de-costa-rica
- Instituto Federal de Acceso a la Información Pública. *LINEAMIENTOS Generales para la clasificación y desclasificación de la información de las dependencias yentidades de la Administración Pública Federal.* Agosto, 2003. Recuperado de: https://sre.gob.mx/images/stories/marconormativodo c/linea02.pdf

- Ley 7472 (1995). *Reglamento a la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor*. 19 de enero de 1995. La Gaceta N° 14.
- Ley 8968 (2011). *Ley de protección de la persona frente al tratamiento de sus datos personales*. 5 de septiembre de 2011. La Gaceta No. 170.
- Ley 9048 de 2012. *Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal, 6 de noviembre de 2012*. La Gaceta, Alcance Digital 172 No. 214.
- *Ley modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional* (1996). CNUDMI, 12 de junio de 1996. Recuperado de: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453_s_ebook.pdf
- López Bulla, R. *La Seguridad De La Información, Responsabilidad De Todos*. #ashtag, n.º 3, Nov. 2013, pp. 25-27
- Organización de los Estados Americanos (OEA), *Convención Americana sobre Derechos Humanos "Pacto de San José de Costa Rica"*, 22 Noviembre 1969, recuperada de: https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm
- Organización de las Naciones Unidas (ONU): *Asamblea General, Declaración Universal de Derechos Humanos*, 10 Diciembre 1948, 217 A (III), Recuperado de: https://www.un.org/es/about-us/universal-declaration-of-human-rights
- Organización de las Naciones Unidas (ONU): *Asamblea General, Pacto Internacional de Derechos Civiles y Políticos*. Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966, 16 diciembre

1966, Naciones Unidas, Serie de Tratados, vol. 999, p. 171, Recuperado de: https://www.ohchr.org/sp/professionalinterest/pages/ccpr.aspx

- Peña Valenzuela, D. 2003. *Lex electrónica: ¿mito o realidad? Perspectiva desde la contratación por medios electrónicos.* Revista La Propiedad Inmaterial. 7 (diciembre, 2003), 103-116.
- Proyecto de Ley No. 12.827 (1998). *Ley Tipo sobre Protección de datos personales automatizados*
- Rogers, D. (2020). *Documento*. Enciclopedia Jurídica. http://www.enciclopedia-juridica.com/d/documento/documento.htm
- Saarenpaa, A. (2003). *Europa y la protección de los datos personales.* Revista Chilena de Derecho Informático, (3). doi:10.5354/0717-9162.2011.10659
- Sala Constitucional. Sentencia 01435 - 2003, 2003
- Sala Constitucional. Sentencia 05802 - 1999, 1999
- Sala Constitucional. Sentencia 11-000724-0007-CO, 2011
- Sala Tercera de la Corte. Sentencia 02-003942-0647-PE, 2009
- Sánchez, M.P. (Sin fecha). *La protección al consumidor en USA: el A.P.R.*. Esteban Sánchez Sánchez notario. https://www.essnotario.com/la-proteccion-al-consumidor-en-usa-el-a-p-r/
- Sanz Barreda, M. (2018). *Protección de consumidores y usuarios. prevención de fraudes informáticos a personas mayores*
  (Trabajo final de Grado). Universitat Jaume. Recuperado de: http://repositori.uji.es/xmlui/bitstream/handle/10234/177083/TFG_2018_Sanz+Barreda_Maria.pdf?sequence=1

- Téllez Valdés, J. (2008). *Derecho Informático Cuarta Edición.* México: Interamericana Mac Graw Hill.
- Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José. Sentencia 08-016097-0042-PE, 2015
- Tribunal de Apelación de Sentencia Penal III Circuito Judicial de Alajuela San Ramón. Sentencia 00188 - 2016, 2016
- Tribunal de Casación Penal de Cartago. Sentencia 06-200097-0454-PE, 2011
- Proyecto de Ley No. 12.827 (1998). *Ley Tipo sobre Protección de datos personales automatizados*
- Vera, J. y Mayer, L. (2020). *El delito de espionaje informático: Concepto y delimitación.* Revista Chilena de Derecho y Tecnología. doi: 10.5354/0719-2584.2020.59236
- Zuñiga, M. (6 de agosto, 2019). *La legalidad del Derecho informático y su relación con los ingenieros en TIC's*. CPIC. https://www.cpic.or.cr/Posts/Details/La%20legalidad%20del%20Derecho%20inform%C3%A1tico%20y%20su%20relaci%C3%B3n%20con%20los%20ingenieros%20en%20TIC%E2%80%99s#