



Facultad de Ciencias Jurídicas y Justicia
Licenciatura en Ciencias Jurídicas y de la Justicia

**Protección de información personal en base de datos
de bolsa de empleo y relaciones laborales**
(Tesis de Licenciatura)

Joseline Kelly Martini Ordóñez

Guatemala, junio 2022

Facultad de Ciencias Jurídicas y Justicia
Licenciatura en Ciencias Jurídicas y de la Justicia

**Protección de información personal en base de datos
de bolsa de empleo y relaciones laborales**
(Tesis de Licenciatura)

Joseline Kelly Martini Ordóñez

Guatemala, junio 2022

Para los efectos legales y en cumplimiento a lo dispuesto en el artículo 1º, literal h) del Reglamento de Colegiación del Colegio de Abogados y Notarios de Guatemala, **Joseline Kelly Martini Ordóñez**, elaboró la presente tesis, titulada **Protección de información personal en base de datos de bolsa de empleo y relaciones laborales.**

AUTORIDADES DE UNIVERSIDAD PANAMERICANA

M. Th. Mynor Augusto Herrera Lemus

Rector

Dra. Alba Aracely Rodríguez de González

Vicerrectora Académica

M. A. César Augusto Custodio Cobar

Vicerrector Administrativo

EMBA. Adolfo Noguera Bosque

Secretario General

FACULTAD DE CIENCIAS JURÍDICAS Y JUSTICIA

Dr. Enrique Fernando Sánchez Usera

Decano de la Facultad de Ciencias Jurídicas y Justicia



Guatemala, 15 de octubre de 2021

Señores Miembros
Consejo de la Facultad de Ciencias Jurídicas y Justicia
Universidad Panamericana
Presente

Estimados señores:

Tengo el agrado de dirigirme a ustedes, haciendo referencia a mi nombramiento como **tutor** de la estudiante **Joseline Kelly Martini Ordoñez, ID 000108212**. Al respecto se manifiesta que:

- a) Brindé acompañamiento al estudiante en referencia durante el proceso de elaboración de la tesis denominada **Protección de información personal en base de datos de bolsa de empleo y relaciones laborales**.
- b) Durante ese proceso le fueron sugeridas correcciones que realizó conforme los lineamientos proporcionados.
- c) Habiendo leído la versión final del documento, se establece que el mismo constituye un estudio serio en torno al tema investigado, cumpliendo con los requerimientos metodológicos establecidos por la Facultad de Ciencias Jurídicas y Justicia para esta modalidad académica.

En virtud de lo anterior, por este medio emito **DICTAMEN FAVORABLE** para que continúe con los trámites de rigor.

Atentamente,

M.A. José Luis de Jesús Samayoa Palacios

Quetzaltenango, 17 de enero de 2022


Señores miembros
Consejo de la facultad de Ciencias Jurídicas y Justicia
Universidad Panamericana
Presente

Estimados señores:

Tengo el agrado de dirigirme a ustedes, haciendo referencia a mi nombramiento como revisora metodológica de la tesis de la estudiante Joseline Kelly Martini Ordoñez, ID 000108212, titulada Protección de información personal en base de datos de bolsa de empleo y relaciones laborales. Al respecto me permito manifestarles que, la versión final de la investigación fue objeto de revisión de forma y fondo, estableciendo que la misma constituye un estudio serio que cumple con los requerimientos metodológicos establecidos por la Facultad de Ciencias Jurídicas y Justicia para esta modalidad académica.

En virtud de lo anterior, por este medio emito DICTAMEN FAVORABLE para que se continúe con los trámites de rigor.

Atentamente,



Licenciada Mónica José Ixcot Fuentes
Abogada y notaria

Licenciada
Mónica José Ixcot Fuentes
ABOGADA Y NOTARIA

En la ciudad de Guatemala, departamento de Guatemala, el día cuatro de mayo del año dos mil veintidós, siendo las nueve horas, yo, **ANNELYS PADILLA VILLATORO**, Notaria, número de colegiado veintiocho mil cuatrocientos cuarenta y cuatro (28444), me encuentro constituido en mi oficina profesional situada en la dieciocho (18) calle número veinticuatro guion sesenta y nueve (24-69) de la zona diez (10), Empresarial Zona Pradera, Torre III, Nivel Doce (12), Oficina un mil doscientos ocho (1208), soy requerida por **Joseline Kelly Martini Ordoñez**, de treinta años de edad, soltera, guatemalteca, estudiante, de este domicilio, quien se identifica con Documento Personal de Identificación (DPI) con Código Único de Identificación (CUI) dos mil ciento dieciséis, espacio cincuenta y siete mil setecientos cincuenta y uno, espacio cero ciento uno (2116 57751 0101), extendido por el Registro Nacional de las Personas de la República de Guatemala, quien requiere mis servicios profesionales con el objeto de hacer constar a través de la presente **DECLARACIÓN JURADA** lo siguiente: **PRIMERO:** La requirente, **BAJO SOLEMNE JURAMENTO DE LEY**, y enterada por la infrascrita Notaria de las penas relativas al delito de perjurio, DECLARA ser de los datos de identificación personal consignados en la presente y que se encuentra en el libre ejercicio de sus derechos civiles. **SEGUNDO:** Continúa declarando bajo juramento la requirente: i) ser autora del trabajo de tesis titulado: **“Protección de información personal en base de datos de bolsa de empleo y relaciones laborales”**; ii) haber respetado los derechos de autor de las fuentes consultadas y reconocido los créditos correspondientes; y iii) aceptar la responsabilidad como autor del contenido de la presente tesis de licenciatura. No habiendo nada más que hacer constar, finalizo el presente instrumento en el mismo lugar y fecha de inicio, cuarenta minutos después, la cual consta en una hoja de papel bond tamaño oficio, impresa en ambos



Licda. Annelys Padilla Villatoro
Abogada y Notaria

lados, que firmo y sello, a la cual le adhiero los timbres para cubrir los impuestos correspondientes que determinan las leyes respectivas: un timbre notarial del valor de diez quetzales con serie BA guion cero cero setenta y nueve mil novecientos doce (BA-0079912) y un timbre fiscal del valor de cincuenta centavos con número de registro cuatro millones novecientos noventa y un mil seiscientos quince (4991615). Leo íntegramente lo escrito a la requirente, quien enterada de su contenido, objeto, validez y demás efectos legales, la acepta, ratifica y firma con la Notaria que autoriza. **DOY FE DE TODO LO EXPUESTO.**

f) 

ANTE MÍ:



Licda. Annelys Padilla Villatoro
Abogada y Notaria



ORDEN DE IMPRESIÓN DE TESIS DE LICENCIATURA

Nombre del Estudiante: **JOSELINE KELLY MARTINI ORDOÑEZ**

Título de la tesis: **PROTECCIÓN DE INFORMACIÓN PERSONAL EN BASE DE DATOS DE BOLSA DE EMPLEO Y RELACIONES LABORALES**

El Decano de la Facultad de Ciencias Jurídicas y Justicia,

Considerando:

Primero: Que previo a otorgársele el grado académico de Licenciada en Ciencias Jurídicas y de la Justicia, así como los títulos de Abogada y Notaria, la estudiante ya mencionada, ha desarrollado el proceso de investigación y redacción de su tesis de licenciatura.

Segundo: Que tengo a la vista el dictamen favorable emitido por el tutor, M.A. José Luis de Jesús Samayoa Palacios de fecha 15 de octubre de 2021.

Tercero: Que tengo a la vista el dictamen favorable emitido por la revisora, Licenciada Mónica José Ixcot Fuentes de fecha 17 de enero de 2022.

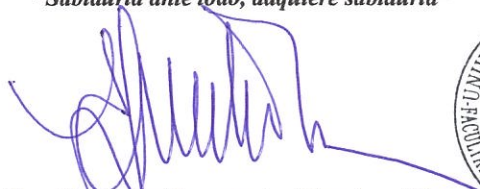
Cuarto: Que tengo a la vista el acta notarial autorizada en la ciudad de Guatemala, departamento de Guatemala, el día 04 de mayo de 2022 por la notaria Annelys Padilla Villatoro que contiene declaración jurada de la estudiante, quien manifestó bajo juramento: *ser autor del trabajo de tesis, haber respetado los derechos de autor de las fuentes consultadas y reconocido los créditos correspondientes; y aceptar la responsabilidad como autor del contenido de su tesis de licenciatura.*

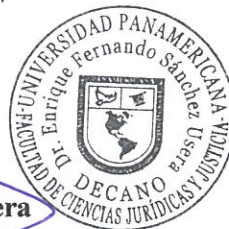
Por tanto,

Autoriza la impresión de la tesis elaborada por la estudiante ya identificada en el acápite del presente documento, como requisito previo a la graduación profesional.

Guatemala, 07 de junio de 2022.

"Sabiduría ante todo, adquiere sabiduría"


Dr. Enrique Fernando Sánchez Usera
Decano de la Facultad de Ciencias
Jurídicas y Justicia



Nota: Para efectos legales, únicamente el sustentante es responsable del contenido del presente trabajo.

Dedicatoria

A Dios:

Por darme la fortaleza e iluminación para culminar mis estudios de derecho y acompañarme a lo largo de mi vida.

A mi familia:

Alvia Josefina Ordóñez de Martini, Rodolfo Santiago Martini Herrera, Stephanie María Martini Ordóñez, por todo el apoyo que me han demostrado a lo largo de mi vida especialmente en mi carrera.

A mis amigos:

Leslie Avila Campos, Gabriel Briones Girón, Herber Giovanni Rosales Franco, por toda su ayuda y muestras de solidaridad tanto en mi vida personal como en la carrera de Derecho.

Índice

Resumen	i
Palabras clave	ii
Introducción	iii
Datos personales y su debida protección	1
Plataformas digitales	21
Resguardo de los datos personales	41
Conclusiones	66
Referencias	68

Resumen

Se pretendió determinar si la protección de datos personales en plataformas digitales, derivadas de la bolsa de empleo y relaciones laborales, cumplía con la protección adecuada a los usuarios. Es por ello que se tenía como objetivo principal precisar el concepto de datos personales y establecer si existía vulnerabilidad al momento de ingresar los mismos y de esta manera poder concluir que hoy en día en Guatemala existe una falta de protección legal para dichos datos personales los cuales incluso se convierten en bienes comerciales.

Se utilizó la modalidad del estudio monográfico de tipo comparativo, que pretendía realizar un análisis jurídico de la vulnerabilidad de los datos personales adquiridos a través de bolsas de empleo y sitios dedicados a la intermediación entre un posible trabajador y el patrono. Para ello se llevó a cabo un análisis comparativo entre las legislaciones de Argentina, México y Costa Rica. Se consideraron éstos, ya que en dichos ordenamientos ya existía una norma que ampara y protege los derechos de las personas, las cuales se utilizaron como modelo para poder determinar la necesidad que existe en Guatemala sobre la implementación de una posible legislación que regule los derechos a la intimidad e identidad de los habitantes de la República.

Se estableció que existe una necesidad actual de protección de datos, especialmente aquellos derivados de las plataformas digitales en virtud que a pesar que la Constitución Política de la República de Guatemala regula y protege la integridad, no es suficiente para poder brindar un resguardo adecuado a la información, más cuando se trata de sitios en línea en donde se pueden comercializar sin consecuencia alguna y al no existir una disposición legal se genera una vulnerabilidad social.

Palabras clave

Protección. Titulares del derecho. Datos personales. Datos sensibles. Plataformas digitales.

Introducción

El problema tendrá como características la falta de protección legal en donde el Estado garantice el debido uso de la información y sancione aquellos actos que vulneren la misma. Así como la vulnerabilidad de información de datos personales derivados de las relaciones laborales y bolsa de trabajo. También, se abarcará la exposición de datos personales en las plataformas digitales que otorgan oportunidades de empleo y por último la venta de la información por parte del personal hacia empresas dedicadas al *marketing*, publicidad o bien haciendo uso comercial (ante la compraventa de información) sin tener consecuencia alguna.

Se pretenderá a través del objetivo general determinar si la protección de datos personales en plataformas digitales logrará resguardar la información derivada de la bolsa de empleo y relaciones laborales. Como objetivos específicos se precisará el concepto de datos personales y determinará si existe vulnerabilidad al momento de ingresar los mismos en las plataformas digitales de bolsa de empleo y se analizará la regulación y uso de las plataformas digitales, como medio utilizado para adquirir información y su relevancia en el derecho de protección de datos personales. Esto con el fin de poder establecer que existirá una necesidad real de modificar la legislación actual adhiriendo disposiciones que protejan la intimidad y demás información de los usuarios.

La evolución del mundo globalizado y el avance de la tecnología ha generado la necesidad de plantear nuevos escenarios legales que atiendan a la protección de los datos personales e información privada de los particulares. Estos datos se derivan de plataformas que pretenden ser un intermediario de comunicación entre un posible empleado con sociedades mercantiles o sociales que están interesadas en contratar. Siendo esta la razón principal que justifica el estudio su interés.

Para poder llevar a cabo el estudio, se utilizará la modalidad del estudio monográfico de tipo comparativo. Este pretenderá realizar un análisis jurídico de la vulnerabilidad de los datos personales adquiridos a través de bolsas de empleo y sitios dedicados a la intermediación laboral. Así mismo se realizará una comparativa entre las legislaciones de Argentina, México y Costa Rica, ya que en dichos ordenamientos ya existe una norma que ampara y proteger los derechos de las personas, y se utilizarán como modelo para poder determinar la necesidad que existe en Guatemala.

El documento se dividirá en tres subtítulos, con los siguientes temas de relevancia, el primero los datos personales, ya que para poder determinar si existe una necesidad de protección de la información es necesario definir y establecer qué son. También se establecerá su función, tomando en consideración sus antecedentes históricos, su naturaleza jurídica, sus elementos característicos y si realmente tiene una importancia el proteger los mismos y cuáles serían las consecuencias de no hacerlo.

En el segundo, se conocerá sobre las plataformas digitales ya que éstas son las fuentes principales de donde se extrae toda la información y para ello también es necesario tener claro cuál es el concepto, su naturaleza y características, las ventajas y desventajas del uso de las mismas. Considerando que hoy en día existe un acceso fácil y rápido. Además, establecer si existirá o no la necesidad de las plataformas como medio para adquirir empleo, ya que hoy existe un avance tecnológico significativo que aumenta el uso de dichas páginas de web ante la necesidad de conseguir un trabajo.

Finalmente, en el tercero se tratará sobre el resguardo de los datos personales en donde se determinará el valor económico que pueden llegar a tener la información ya que los mismo se consideran objeto de comercio, que se deriva también de la vulnerabilidad de la información. Posteriormente se hará una comparación con las legislaciones de otros países en donde existen normas que amparan los derechos personales de los usuarios que utilizan las plataformas como medios para adquirir empleo.

Protección de información personal en base de datos de bolsa de empleo y relaciones laborales

Datos personales y su debida protección

Antecedentes históricos

La protección de datos personales se remonta desde el año de 1890, en Estados Unidos de América. Éste es considerado el origen más claro, con su artículo *The right to privacy* cuya traducción en español sería el derecho a la privacidad, que buscaba una garantía a los habitantes respecto a su vida personal, derivada de las injerencias de los medios de comunicación como el periódico. En aquella época se comenzaba a notar cambios en la sociedad tanto desde el punto de vista económico, político y social que implicaba el reconocimiento de derechos y fue entonces cuando los autores de dicho artículo Warren y Brandels determinaron por primera vez la importancia del derecho de la privacidad y la defensa a la información personal.

Históricamente, se tienen otras referencias previas, las cuales surgen del aforismo inglés con el autor William Pitten, “*A man´s house as his castle*” (López-Torres, 2014), cuya traducción al español es la casa de cada uno es su castillo, en el año de 1763, en donde se buscaba que le otorgaran a

cada ciudadano la protección de personal, la cual se encontraba en sus propios hogares. Es decir que lo que buscaba este principio era que las personas pudieran tener una garantía que sus derechos frente al poder de la monarquía que en aquella época regía el gobierno de la sociedad inglesa. En este sentido podemos determinar que, como uno de los primeros antecedentes de la protección de información, se regulaban únicamente aquellos “datos o conocimientos precisos que resultaban referibles a la esfera de intimidad del sujeto” (Gómez, 1999) (p.3). Sin embargo, a lo largo del tiempo se determinó que también era necesaria una distinción entre la privacidad y la intimidad, y nació entonces, la obligación de regular toda información de carácter personal. Posteriormente, parafraseando al autor Recio Gayo se puede determinar que, el control de la propia información que se encuentra almacenada en bases de datos de empresas públicas y privadas. Las cuales, hoy en día ya se comienzan a considerar aquellas que se encuentra en los sitios de internet en donde existen registros, en los cuales se incluye el correo electrónico, las herramientas colaborativas, las redes sociales, los portales de servicios, los sitios de investigación, educativos o diversión, entre otros.

Asimismo, los datos personales y su protección fueron sujeto de un desarrollo normativo, comenzando con la Declaración Universal de los Derechos Humanos del 10 de diciembre e 1948 que tuvo lugar en París, la cual estipula en su artículo 12 en su parte conducente establece que “nadie

será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia (...)”, que aparece como uno de los primeros antecedentes en la protección de la información personal, ya que dicho derecho garantizaba los ataques a la información especialmente aquellos que devenían de las autoridades del Estado, sin excluir a las personas físicas o jurídicas que no eran dueñas de dichas referencias.

Parafraseando a (López-Torres, 2014) en 1960, los Tribunales de Estados Unidos de América, crearon precedente reconociendo el derecho a la protección de información, estipulando los cuatro agravios a la privacidad de la persona, derecho establecido por Warren y Brandeis y se consideró como un derecho constitucional en dicho país. Este nuevo concepto debía tener carácter de seguridad nacional, especialmente porque en este lugar se consideraba que el gobierno indagaba sobre la información de las personas, y fue entonces motivo de controversia dentro de la sociedad.

A raíz de dichos precedentes y la jurisprudencia que se generó especialmente en Estados Unidos de América (Oriano, 2005) señala que se comenzó a considerar la existencia del *Data Privacy* el cual se puede traducir como el Derecho a la Privacidad, considerado en la Primera Enmienda, que permitía proteger a cualquier persona que residiera en el país, frente a la obligación legal de revelar si se pertenecía o no a un grupo de personas u organización. Posteriormente se estableció una cuarta

enmienda en donde se salvaguardaba la información que se debía registrar de forma obligatoria ante las autoridades estatales, en donde se limitaba al abuso que pudieran hacer el gobierno de forma arbitrales. En este sentido se protegían la información en donde se incluía el domicilio, documentos y efectos personales. Luego se publicó la quinta enmienda que prohibía la incriminación y relevación de datos personales.

En 1905, se aplicó la protección de datos y su debida privacidad, desde el punto de vista jurídico a través de la Corte Suprema de Georgia, por primera vez. En dicha sentencia del caso *Pavesick & New England Life Insurance Company*, reconocieron la necesidad de proteger la imagen y la intimidad de la vida privada, reconociendo esta protección como un derecho innato que debe ser protegido por el Estado, para garantizar la seguridad de estos. Este antecedente motivó en la búsqueda de mayores y mejores protecciones para las personas. (Valencia, 2019)

Pasando un poco a los antecedentes europeos, de acuerdo con lo que estableció el autor (Alfonso, 1993), el cual se parafrasea se tiene evidencia que pensadores como Benjamín Constant De Rebecque, Jeremy Bentham, Thomas Hobbes, John Looke o Robert Price fueron los precursores de la protección en dicho continente, comenzando en Reino Unido en 1961, en donde se presentó un proyecto de ley sujeto a debate en ese mismo año, en donde se comprendía la necesidad de proteger el derecho de no invasión

de la privacidad y la conservación de la dignidad humana, este fue presentado también en Alemania, por Lord Mancroft, el cual no fue del todo aceptado.

En el mismo sentido en 1967, Alexander Lyon, intentó presentar el proyecto para la protección de datos, el cual fue rechazado, dejando una vulnerabilidad en la protección de los datos. En 1972, Younger Committee Report, se publicó lo que dio lugar a que en 1979 se introdujera el *White paper* (papel blanco) donde se logró una protección de datos y se introdujo el concepto de datos y protección de estos “Los resultados de este comité dieron lugar al *white paper* donde se introdujo en 1979 el concepto de protección de datos personales derivados del tratamiento informatizado de datos y el *lindop Report*” (Nisa Ávila, 2020).

En 1984 se aprobó *the Data Protection Act*, cuya traducción al español se entiende como la ley de protección de datos), la cual dio lugar luego de casi veintitrés años de conversatorios y discusiones al respecto, las cuales, luego de la aprobación de *the European Community*, es decir de la Comunidad Europea a través del Convenio para la Protección de las personas con respecto al Tratamiento Automatizado de Datos de carácter Personal de fecha 28 de enero de 1981.

En Alemania también se iniciaron las discusiones legales sobre la necesidad de proteger la información personal y es por ello que en el año de 1970 surge la ley de Hesse, promulgada por Land de Hesse. Su contenido se apreciaban normativas de amparo sobre el control de datos, y ya para 1977 se comunicó a nivel de federación una ley la cual sancionaba el uso ilícito o control sobre éstos. Al igual que con la legislación alemana, los países suecos también promulgaron normas desde 1973 cuyo fin fue progresivo, ya que se fue ampliando a través de las publicaciones de legislaciones en diversos países.

La necesidad de proteger el derecho a la intimidad de la persona y la inviolabilidad de sus datos se encuentra establecida en la Constitución Política desde 1985, ya que en su artículo 24 se establece que los documentos, correspondencia y libros son inviolables, y si en algún momento se requiere de una revisión o ser incautados será necesario llevar una resolución judicial debidamente firmada por la autoridad competente.

Adicional se refuerza el derecho de privacidad de la correspondencia, comunicaciones telefónicas, cablegráficas y otros productos de tecnología moderna, en este sentido el legislador dejó abierto ya que se sabe que cada día se desarrollan mayores y mejores instrumentos de comunicación, lo que permite una facilidad para las personas de poder mantener contacto de manera más ágil y efectiva con otros individuos alrededor del mundo.

Adicionalmente, la legislación también protege libros, documentos y archivos que se relacionan al tema del pago de tributos, cualquiera que sea su tipo de contribución (pueden ser tasas, arbitrios, contribuciones especiales) y también cualquier otro documento que puede ser obtenido. Es preciso considerar que hoy en día la mayoría de dicha información se encuentra en una plataforma digital, si bien es cierto existen libros, éstos ya se pueden descargar virtualmente para tener la información que se requiera.

Sin embargo, fue en 2008 cuando fue promulgada la ley de Acceso a la Información Pública, Decreto 57-2008 emitida por el Congreso de la República de Guatemala, cuando se comienza a definir los datos personales o aquellos que son sensibles, con el fin de poder garantizar a la población el acceso a la información pública, sin embargo, esta norma no evidencia la protección de dichos datos, por lo que se puede determinar que para este país aún le queda el reto de poder determinar normativas que protejan debidamente la información de sus habitantes.

Definición de datos personales

Para poder comprender un poco más, es necesario establecer una definición conceptual sobre los datos, su protección y alcance. El Decreto número 57-2008 del Congreso de la República de Guatemala, Ley de

Acceso a la Información Pública, en su artículo 9 numeral 1 define los datos personales como “lo relativo a cualquier información concerniente a personas naturales identificadas o identificables”, asimismo la norma da una definición de los datos personales sensibles en donde se incluyen las características físicas o morales de las personas o hechos de su vida privada en donde se incluye el origen racial, las ideologías, creencias religiosas, el estado de salud de la persona, incluyendo su estado psíquico, sus preferencias y cuestiones íntimas de la persona.

Asimismo, la Comisión Europea define los datos personales como “cualquier información relativa a una persona física viva identificada o identificable”, por lo que de esta definición se pueden extraer tres elementos fundamentales para que se consideren personales los datos, primero que corresponda a una persona física, que según el Código Civil Decreto Ley 106, se considera una persona humana de existencia real. Debe estar viva, lo que incluye la condición física y espiritual del ser humano, capaz de realizar actividades físicas y mentales adecuadas según la edad y como tercer elemento debe ser identificada, es decir que aquella información que se encuentra bajo seudónimos no se incluiría dentro de esta clasificación, ni aquella que sea ambigua o que se constituya como anónima.

Dentro de la definición de datos personales se pueden incluir entonces, los nombres y apellidos de la persona física, su domicilio, que se constituye de forma voluntaria por la residencia y ánimo de permanencia del sujeto, el código único de identificación personal del documento personal de identificación que el Registro Nacional de las Personas de Guatemala le emite a cada habitante del país cuando adquieren la edad suficiente para tener capacidad de adquirir derechos y obligaciones. También se incluyen los registros médicos obtenidos en hospitales o clínicas particulares, en los establecimientos académicos tanto a nivel primario, secundarios y superior.

Además, hoy en día gracias a los avances tecnológicos y evolución que se ha venido dando a lo largo de los años, la información personal extiende sus parámetros por lo que deben incluirse otros elementos como la dirección del correo electrónico indistintamente del dominio al que pertenezca, los datos de localización, que muchas veces se queda activado en los teléfonos móviles, automóviles o cualquier otro dispositivo que tenga *GPS* (por sus siglas en inglés Sistema de Posicionamiento Global) que permite determinar la ubicación o posición de cualquier objeto en el mundo, la dirección de protocolo de internet (IP), las búsquedas *http* que puedan generarse dentro de un ordenador que le pertenece a una persona.

Naturaleza jurídica

Luego de haber establecido los antecedentes y definido el concepto es necesario conocer sobre la naturaleza jurídica de los datos personales y la necesidad que existe de proteger los mismos, para el efecto se considera que constituyen al derecho público, ya que debe regular las relaciones entre las personas dentro de la sociedad y deberá ser el Estado quien cumpla con una participación proteccionista, indistintamente del tipo de información de la que se trate. Además, es preciso tener en cuenta que dentro de la Carta Magna se encuentran regulados estos conceptos.

Características

Los datos tienen ciertas especificaciones características, que ayudan a determinar cuándo cierta información puede ser objeto de resguardo. Como primer punto, éstos deben considerarse como confidenciales, es decir toda aquella data, cuya revelación al público pueda causarle un peligro a una persona, por ejemplo, su dirección, sus estados financieros, su estado de Salud, su número telefónico, debe hacerse con reserva. Los datos, son de propiedad personal, los cuales al hacerse públicos puede causar un agravio al interesado, y por ende esta característica es primordial a tomarse en cuenta.

También se caracterizan los datos por ser sensibles, en donde la revelación de estos pudiera constituir un agravio para la persona, el cual al ser revelado puede incluso constituir un delito tipificado en las normas penales. Todo lo que se obtiene o se sabe de una persona, su nombre, apellido, dirección, sexo, estado civil, su nacionalidad o cualquier otro dato sensible, son únicos y pueden ser objetos a un mal uso por lo que es importante considerar y categorizar la información.

Es importante considerar que los datos personales solo aplican para personas físicas o jurídicas, es decir, únicamente se pueden proteger en este sentido, a los de los seres vivos, por lo que los datos de los fallecidos no se considerarían sujetos a protección de los datos, al igual que aquellos detalles de los bienes muebles o inmuebles per se, sin embargo, estos si pueden considerarse parte de la información de las personas. Las legislaciones brindan protección a los seres vivos, como bien lo indica la Constitución Política de la República de Guatemala, cuando establece que su deber es velar por la protección de la persona y la familia, en este caso se entiende que es al ser vivo quien debe brindarle la protección, sin embargo, se considera que, a raíz del deber de cuidar y velar también por la familia, debe resguardarse incluso después de la muerte para proteger también a quienes lo rodeaban.

Clasificación

Existe además, una clasificación determinada por la autora Marina (2020), en donde se establece que, de los datos que es relevante para la presente investigación, dentro de los que se incluyen: Los datos de carácter personal que a su vez tienen una subcategoría, dentro de la cual se constituyen como primer punto los datos ordinarios, en estos se pueden incluir todos los detalles de identificación personal como por ejemplo el nombre y lugar de residencia, información financiera, asuntos fiscales, récord crediticio, historial académico, solicitudes de empleo, hojas de vida, puesto, área de trabajo, motivos de despido, número de teléfono del trabajo y demás datos relevantes.

Como segunda subdivisión se encuentra los datos especialmente protegidos, que pertenecen a un conjunto específico de “categorías especiales” que deben tratarse con mayor seguridad. Estas categorías son: Origen étnico o cultural: Refiriéndose a la raza o etnia de las personas, en este sentido se incluyen costumbres, idiomas, creencias religiosas, entre otras. Las Opiniones políticas, religiosas y filosóficas, la orientación sexual y el género, referentes la identidad, la Afiliación sindical, también podría incluirse como parte de aquellos sobre afiliación sindical son los que indican si una persona concreta está afiliada a un sindicato.

También se tiene una categorización especial, que constituyen todos aquellos datos sobre acusaciones o condenas penales de los procesos en donde el individuo ya fue citado, oído y vencido en un juicio, se le dictó una sentencia y se hace constar en los antecedentes tanto penales como policiales dependiendo del tipo de delito o infracción a la que incurra la persona involucrada. Este tipo de información es necesario determinarla porque muchas veces es objeto de discriminación y debe ser obligación del Estado proteger a sus habitantes, incluyendo a los reformados.

Están, además, los datos genéticos y biométricos, referentes a la constitución fisiológica y de salud que resultan de la herencia biológica, hoy en día los avances tecnológicos y científicos han ayudado a conocer y desarrollar más para obtener información cromosómica, que no solo releva el origen familiar de un individuo, si no también puede mostrar el estado de salud, las posibilidades de contraer determinadas enfermedades, basados en los antecedentes familiares de cada uno. Es necesario tener en cuenta que este tipo de dato no se considera como identificable ni sensible, por lo que no se detallará más en esta investigación.

Existen principios fundamentales referentes a los datos personales que hay que tomar en cuenta, dentro de los que se incluyen, la calidad de los datos, la conservación, la transparencia y la seguridad de los datos, esto de acuerdo con el Estudio Centroamericano de Protección de Datos de

Guatemala, redactado por el Instituto Panameño de Derechos y Nuevas Tecnologías. Para ahondar un poco sobre estos principios, se establece que la calidad de datos implica llevar a cabo un procedimiento y tratamiento adecuados, indicando, asimismo, cuando los datos deben ser cancelados. Es importante la cancelación de los datos hasta cierto grado luego del fallecimiento de la persona, con los fines hereditarios que se pueda llegar a determinar.

Ya que al momento de que un individuo fallece, los bienes pasan a nombre de sus herederos, pero para poder llevar a cabo este proceso se debe tener, necesariamente acceso a dicha información y datos personales, pero para ello debe existir un respaldo legal que proteja al individuo y con ello también a sus familiares y demás personas que lo rodean y para ello debe existir un respaldo o protección por parte de las autoridades estatales que cuiden su privacidad a pesar de la muerte de este.

(Valladares, 2019) establece:

Se determina que el procedimiento y tratamiento de los datos personales deben ser adecuados, pertinentes y no excesivos al fin legítimo para el cual se recopilaron. Además, determina cuándo se deben cancelar los datos, como en caso de que. no exista consentimiento legal, sean inexactos e incompletos, ya no sean pertinentes o necesarios.
(p.4)

Para el principio de conservación y como bien lo establece el mismo autor anteriormente citado, es necesario tomar en cuenta “que los datos personales serán conservados únicamente en la manera que no permita la identificación de su titular y por un período razonable y necesario para el cual fueron registrados”. Además, determina que “En ningún caso, serán conservados los datos personales que puedan afectar de cualquier modo a su titular, una vez transcurridos diez (10) años desde la fecha de ocurrencia de los hechos registrados, salvo disposición legal en contrario”.

Respecto a la Transparencia la referida iniciativa indica el autor “las personas, que solicitan datos personales deberán informar de manera previa, expresa, precisa e inequívoca lo siguiente: la existencia del archivo, manual o automatizado, la finalidad y destinatarios. (...), deben informarle a la persona los derechos que posee”. (p.7) Esto nos da la pauta que los datos personales deben ser protegidos y en ningún momento pueden ser divulgados sin previo consentimiento de aquella quien es dueña de la información.

El mismo documento establece para el principio de seguridad de los datos que (Valladares, 2019):

Conforme los Artículos 8 y 9 de la iniciativa, los responsables de los archivos, ficheros, registros o bases de datos, públicos o privados deberán adoptar las medidas necesarias para garantizar la seguridad de los datos personales con el fin de evitar su alteración, pérdida o acceso no autorizado. Adicional, la legislación también impondría la obligación de

confidencialidad a las personas responsables del tratamiento de los datos personales, aún después de finalizar su relación con el archivo de datos". (p.7)

Importancia de la protección de los datos personales

Hoy en día, la información sobre cualquier materia, objeto y personas está al alcance de cualquier persona, esto debido a que en la red no existe una protección determinada sobre todos los datos que se ingresan, ya sea para abrir una cuenta de correo electrónico, ser parte de las redes sociales o incluso para poder aplicar para un puesto de empleo que se publica en páginas web o bien, a través de plataformas o intermediarios cuyo fin es poder conectar personas y empresas que tenga los perfiles adecuados para el puesto vacante.

(Marben, 2019) afirma:

La protección de datos es un tema muy en boga en el momento actual y que conviene tomarse muy en serio. Debemos ser conscientes de que los datos personales que manejamos no nos pertenecen y, por tanto, tenemos la responsabilidad de hacer un uso correcto de los mismos. Ello es aplicable tanto a nivel profesional como a nivel personal (amigos, conocidos, familiares, etc.). (p.1.)

Los datos y su protección deben ser considerados como un derecho personal, ya que incluyen información sensible y privada de los individuos y por ende deben estar sujetos a determinados parámetros que permitan brindar resguardo y confidencialidad, y para poder entender este aspecto, es preciso comprender los principales derechos de los ciudadanos en

materia de protección de datos, en el artículo denominado “la importancia de la protección de datos”, son los siguientes:

Como primer punto, es el derecho de la información, “Es el derecho de saber para qué serán utilizados los datos que se facilitan y el modo para poder solicitar su modificación o cancelación. Esta información debe darse de forma precisa e inequívoca” (Marben, 2019). Este derecho debe ser considerado como una garantía de suma importancia para los ciudadanos, además de ser un derecho humano, que va de la mano con el derecho de libertad de pensamiento y expresión.

Esto quiere decir que todos los ciudadanos por el hecho de ser persona tienen la protección de tener su información, ya que cada uno tiene su nombre, su estado civil, sus estados de cuenta, sus estudios primarios, secundarios, incluso universitarios, incluso en la apariencia física. Es de conocimiento general que el Estado lleva un registro de cierta información personal, el cual es una atribución para adquirir también ciertos derechos y obligaciones, pero es obligación de la entidad proteger que nadie tenga acceso a la misma.

Luego, tenemos el derecho de acceso a acceder a la propia información, que va de la mano con el punto anterior. Esto debe ser gratuito y personal, ya que no se le puede cobrar a un ciudadano por el acceso, tampoco se le

puede negar el mismo, ya que es parte del derecho humano que el Estado está obligado a proteger y, por ende, hoy en día se tienen varias instituciones como el Registro Nacional de las Personas de Guatemala, en donde se lleva un registro con la información civil de los ciudadanos, a la cual cualquiera puede acceder a ella en el momento que así lo requiera.

Asimismo, está el derecho de rectificación, ya que a raíz que el Estado lleva un registro de todos los elementos personales del ciudadano, se pueden cambiar o actualizar la misma, a través de determinados procesos (pueden ser estos notariales o judiciales o bien meramente de trámite), para corregir aquellos que se encuentren registrados de forma errónea, o que por gusto individual se desea cambiar. El ejemplo más claro es cuando se computa mal un apellido, en donde hace falta una tilde, virgulilla o bien tiene una falta ortográfica. Otro ejemplo, es cuando de forma voluntaria se realiza un cambio de nombre, una identificación de persona o una identificación de tercero, tanto en proceso judicial como notarial.

Adicional, es preciso tomar en cuenta el derecho a la cancelación, y es uno de los objetos a indagar en el presente trabajo de investigación, ya que debe ser considerado como tal la opción de que sean suprimidos cuando ya han cumplido con su función toda información cargada. Se sabe que hoy en día, cualquier puede acceder a la información en las plataformas digital, sin embargo, cuando la persona ya no desea que la misma quede

colgada en una red, en una nube digital, entonces se debe tener la opción de eliminar toda aquella documentación que quedó grabada y que ya no se desea que sea pública.

Este punto es necesario, ya que hoy en día existen plataformas en donde se ofrecen trabajo, o en la base de datos de las empresas donde se lleva un registro de todo lo referente a los posibles candidatos, incluso a los trabajadores, que no son eliminadas cuando se da de baja a un trabajador, o bien cuando ya la persona adquirió el empleo, o simplemente porque a decisión personal ya no se requiere o necesita que los datos queden al alcance de cualquier persona y lo que podría generar incluso un peligro para el individuo.

Otro derecho que hay que considerar, es el de oposición a la manera en que tratan los datos personales si así se requiere. Muchas veces, las plataformas digitales, las empresas o cualquier otra institución de forma arbitraria se convierten en los dueños de todo tipo de datos que no les corresponde, por lo que esta garantía debe velar porque en el momento que las personas busquen disponer o eliminar de dicha información puedan hacerlo sin que se les niegue o que con engaños se apropien y distribuyan la misma a terceros que puedan hacer mal uso de esta.

Hoy en día, muchos de estos derechos no se garantizan y las plataformas y empresas se protegen a raíz de una aceptación de condiciones que, permite disponer de todos los datos que se ingresen sin importar los deseos de los dueños de la información y al disponer de ellos sin la más mínima protección deja en un estado de vulnerabilidad a la persona. Como se ha establecido en reiteradas ocasiones, el hecho que cualquier persona tenga acceso a dicha información da lugar a que otros individuos con ánimo de perjudicar, pueda hacer mal uso de los mismos e incluso puede ser objeto de la comisión de un delito, el cual se pudo haber evitado con el simple hecho de proteger estos datos personales.

Muchos autores, señalan que, la protección de los datos debe ser una prioridad para cualquier entidad que tenga acceso a los mismos, pero especialmente para el Estado, recordemos que en la Constitución Política de la República de Guatemala, establece que su deber primordial es proteger a la persona y a la familia y debe velar por el bien común, esto lo regula el artículo primero de la Carta Magna, y da una pauta sobre las obligaciones que tiene el gobierno frente a sus ciudadanos, y parte de ello es velar porque su información tenga la protección necesaria para cada uno de sus conciudadanos.

La protección de datos personales busca garantizar la privacidad de las personas, el resguardo o protección de su intimidad, lo cual supone fundamentalmente, la posibilidad real de controlar el uso y la finalidad para la cual se destina la información relativa a los datos personales de cada individuo, y la facultad de oponerse a su utilización, de manera tal de impedir que esa información sirva a propósitos no aceptados por su titular al momento de adherirse a los contratos electrónicos que usualmente se denominan políticas y condiciones.

Plataformas digitales

Antecedentes históricos

Para poder comprender sobre las plataformas digitales, primero se debe comprender un poco más acerca de la historia del internet, sus inicios y cómo ha venido evolucionando. Es por ello que es necesario retroceder a 1947, en la época de la guerra fría, que surge al finalizar la Segunda Guerra Mundial, en donde existía una lucha por implementar un método de cambio de ideologías, que surgía por un conflicto provocado por (Martinez, 2019) “tensión entre el bloque occidental-capitalista liderado por Estados Unidos de América y el oriental-comunista liderado por la Unión Soviética”. (p.1)

En este sentido es necesario tomar en cuenta que el término de guerra fría surge, debido a que nunca se llevó a cabo un enfrentamiento físico entre los países, si no por el contrario, fue un conflicto político, económico y social en donde Estados Unidos de América buscaba contrarrestar la influencia de la Unión Soviética. Es por ello que ese país se destacó por reforzar militarmente a su población con el objetivo principal del colocarlo en una situación favorable, frente a sus adversarios.

En 1985 Gorbachov, se convirtió en Secretario General quien en conjunto con George H. W. Bush a través de reformas de reestructuración lograron ponerle fin a la Guerra Fría, posterior a ello, surge la caída de Berlín en Alemania, que también había sido fruto de los actos políticos generados por la guerra fría y luego ya queda disolución de la Unión Soviética como tal, lo cual conllevó a tener consecuencias políticas, económicas y jurídicas dentro de dichos países que al final del día afectaban también a todos los países de forma ya sea directa como indirectamente.

Entre el periodo de la guerra fría, que se sitúa en el año de 1957, (Martinez, 2019) señala que la Unión Soviética lanzó el primer satélite artificial, el cual se denominada *Sputnik 1*, creando así un desafío tecnológico entre ambos países que buscan desarrollar mejores formas de tecnología y conocimiento relacionado a dicha materia y en respuesta a ello los Estados Unidos de América se organizaron para desarrollar el

proyecto denominado en inglés como *Advanced Research Projects Agency* que se traduce al español como la Agencia de Proyectos para la Investigación Avanzada) en donde el departamento de defensa de dicho país se encontraba vinculado para poder tener respuesta a los desafíos tecnológicos y militares que se tenía por parte de aquel enemigo. Este hecho es fundamental para poder comprender el origen de las redes ya que asentó fundamentos de lo que hoy por hoy se conoce como internet.

Cinco años después de la creación de dicha agencia, en 1962, el reconocido investigador que trabaja para el gobierno de Estados Unidos de América, creó y publicó un “sistema de comunicaciones que, mediante computadoras conectadas a una red descentralizada, resultaba inmune a ataques externos”, (Rodríguez Lascano, 2016, pág. 2), lo que permitía un sistema de comunicación protegido, que permitía tener una mayor accesibilidad, ya que el mismo tenía como objetivo principal utilizar bloques, que a su vez denominó paquetes, a través de un dispositivo y que el mismo pudiera ser transmitido por una red.

En este sentido cabe mencionar que fue Leonard Kleinrock, quien en el año de 1964 publicó un libro que es la base sobre la teoría de la conmutación de paquetes, y convenció a Roberts sobre la teoría de la comunicación la cual versa específicamente sobre el supuesto en donde a través de dichos paquetes que sustituían a los circuitos que ayudó para el

desarrollo muchos años después de lo que se consideran las redes sociales, pues estos lograban que los ordenadores se comunicaran entre sí.

Este concepto se le denominó “red galáctica”, en donde para poder comprender mejor, se trataba de un conjunto de interlocutores globalmente conectados para que todo el mundo pudiera acceder a datos y programas desde un sitio, de forma más fácil y efectiva en comparación al modo de las comunicaciones que se trabajaban en dicho momento. Este tipo de programas se asemejaban mucho a lo que actualmente se le conoce como internet y se comenzó a determinar la importancia de tener una red que conectada cada día a mayores países y personas alrededor del mundo.

En 1965 se logró crear una red que permitiera establecer el acceso desde cualquier punto del mundo, que se conectaba a un ordenador en Massachusetts (En ese momento se denominó *TX2*) y que tenía un receptor en California (que le colocaron *Q-32*), lo que se realizó por medio de una red telefónica, que para aquella época tenía una velocidad relativamente baja y como era parte de los primeros indicios de la red eran limitadas. Sin embargo, los resultados para dichas pruebas fueron favorables para aquella época.

De hecho, el resultado de estos experimentos determinó la compatibilidad entre los programas que recuperaba los datos, según el equipo lo iba necesitando remotamente y para ello el autor Lascano en su escrito “Breve historia de Internet” establece lo siguiente:

(Rodríguez Lascano, 2016) indica:

El resultado de este experimento fue la constatación de que los ordenadores con tiempo compartido podían trabajar bien juntos, ejecutando programas y recuperando datos según fuese necesario en el equipo remoto, pero que el sistema telefónico de conmutación de circuitos era totalmente inadecuado para esa área. Se confirmó la convicción de Kleinrock de la necesidad de la conmutación de paquetes. (p. 7)

Se continuaron con las investigaciones a lo largo de los años y en 1969 Michel Elie, cuando ingresó a la Universidad de California que se sitúa en el estado de Los Ángeles, Estados Unidos de América, comenzó a realizar una serie de investigaciones al incorporarse al *Advanced Research Projects Agency* el cual de ahora en adelante para la presente investigación se le denominará ARPA, por sus siglas en inglés, en cuyo caso tuvo un gran avance, ya que se logró conectar una computadora que se encontraba en dicha Universidad contra otra que se situaba en el Instituto de Investigación de *Satanford* – SRI- por sus siglas en inglés, el cual se encontraba en el mismo Estado a varios kilómetros de distancia.

Con el tiempo fueron incrementando las universidades que se fueron conectando entre sí gracias a los avances y estudios tecnológicos que se desarrollaron en la agencia de proyectos avanzados y para el efecto se le cambió la denominación, quedando como ARPANET, el cual conectaba cuatro universidad y tenía como objetivo principal mantener las comunicaciones, inicialmente la idea era que se tuvieran especialmente si hubieran guerras posteriores, ya que existía una gran incertidumbre de la existencia de una y con ello llegaba el temor. A raíz de este nuevo descubrimiento también surgía la necesidad de buscar la protección de dichas redes, ya que la que se tenía podía ser sujeto de bloqueos, en caso de un conflicto.

El desarrollo de las redes siguió creciendo con el paso de los años, y con ellos nuevas plataformas que permitían un mejor acceso a comunicaciones entre personas o instituciones, y es entonces cuando surge una figura que hoy en día se le conoce como correo electrónico. Este hecho sucedió en el año de 1970, cuando Ray Tomlinson determinó las bases creadas a raíz una necesidad del mecanismo de coordinación que podrían ser el fundamento para la protección de los datos, especialmente de la red.

Es importante considerar, que en 1972 el país de Estados Unidos de Amé reforzó las investigaciones sobre las redes, ahora ya no eran parte de la milicia si no que pertenecían a las universidades y proyectos de defensa

del país. Cada día más y más científicos comenzaron a utilizar y desarrollar colaboraciones para poder comprender mejor el tema de la tecnología, de tal manera que se buscaron compartir opiniones y colaboraciones de trabajo, para no solo tener resultados más eficientes sino también certeros.

Poco a poco se fueron integrando más casas de estudios hasta lograr tener cincuenta, cuyos centros de investigación se dedicaron a las investigaciones tecnológicas. Un año después de dichas mejoras en los trabajos, en el año de 1973, el ARPANET consiguió obtener conexiones fuera del país y comunión con otros estados como lo fueron Inglaterra y Noruega, para el efecto la obra denominada Historia de Internet: cómo nació y cuál fue su evolución establece lo siguiente: (Bahilio, 2021) “En 1972 ya integraba 50 universidades y centros de investigación que estaban distribuidos por Estados Unidos de América. Un año después, ARPANET ya estableció conexiones con otros países como Inglaterra y Noruega” (p.1).

Con el paso del tiempo y según fueron avanzando las investigaciones se comenzó a desarrollar el comercio de computadoras ya que cada día más ordenadores conectados a las redes fueron aumentando y fue a partir de los años ochenta, que comenzaron a aparecer otras redes que variaban de formato según las necesidades que permitía una conexión más estable, los

cuales fueron unificados y consolidados, que hoy en día se conoce el nacimiento del internet propiamente dicho.

Históricamente fue el año 1983 el que marcó la era del internet ya que como indica Martínez en la obra ya mencionada en los párrafos anteriores, fue “el año que nació internet”, y por lo tanto el Departamento de Defensa de los Estados Unidos de América, que decidió usar un nuevo protocolo en su red para ARPANET, y se establecieron protocolos de transferencias de hipertextos que daría lugar a la primera web, utilizando los recursos del *HTML*, *http* y el web browser o bien un buscador de red, a raíz de esto también comenzaron a desarrollar nuevos programas hasta llegar al *World Wide Web*, que hoy en día se utiliza para el ingreso de las plataformas de modo de poder no solo adquirir información si no, poder tener mejores y mayores métodos de comunicación alrededor del mundo.

A raíz del *World Wide Web*, se comenzaron a expandir las plataformas digitales que permiten crear y generar páginas las cuales funcionan no solo para mantener comunicaciones entre personas si no han sido fuentes de trabajo para muchas empresas, quienes la utilizan para llevar a cabo determinadas tareas, al igual que investigaciones y actualmente se adquieren información de personas y empresas las cuales están interesadas en contratar personal y de igual manera para aquellos que tienen deseo de adquirir un trabajo, (Bahilio, 2021). “Año tras año se incrementa de forma

exponencial el número de usuarios de internet, en el mundo, una cifra ha visto impulsada por la gran penetración que han tenido los dispositivos móviles”

Con la llegada de Internet se produce un importante abaratamiento de los costos de desarrollo de programas, por lo que resulta más sencilla la creación de materiales cuyo objetivo es ser utilizados en línea. Sin embargo, según (Martinez, 2019) se siguen necesitando conocimientos avanzados de programación para crear un curso o un módulo didáctico, y por tanto estos cursos no son accesibles a todo el mundo. Desde mediados de los años 90 empiezan a surgir plataformas didácticas que permiten la creación y la gestión de cursos completos para la web sin que sean necesarios conocimientos profundos de programación o de diseño gráfico.

Definición de plataformas digitales

A lo largo de la historia se fueron desarrollando tecnologías que permitían tener mayores acercamientos entre personas a través de las vías digitales que facilitan la comunicación e incluso lograron sustituir operaciones que anteriormente se hacían manualmente, tal es el caso que se incluso que muchas empresas no necesiten una oficina física para que sus colaboradores laboren, si no que ellos lo pueden hacer desde la comodidad de su casa,

que de alguna manera facilita y mejora la efectividad de los trabajadores hacia las labores diarias.

Del mismo modo sucede con la búsqueda de trabajo, que hace varios años, se hacía a través de publicaciones físicas en periódicos locales o revistas en donde se hacían los comunicados, sin embargo, hoy en día existen nuevas fuentes las cuales se definirán en los párrafos que anteceden que permiten una mayor facilidad en la comunicación pero que el mal uso o la falta de regulación puede incluso provocar una violación a los derechos de privacidad de las personas y es por ello que en este trabajo de investigación surge la necesidad de buscar una definición de las plataformas digitales.

Las plataformas digitales se pueden definir entonces como aquellos canales de comunicación más importante tanto para las instituciones, empresas como personas individuales que permite el ingreso de usuarios de forma ilimitado, agilizando las búsquedas de información obteniendo una respuesta inmediata y extensa, dependiendo de la solicitud del usuario final, en donde se maximizan los recursos de la red, para poder cumplir con el fin primordial que es el acceso a la información de cualquier materia, de forma ágil y efectiva.

Adicional, y siguiendo la finalidad del presente trabajo de investigación, se puede agregar a la definición que dichos canales de información también adquieren relevancia para las empresas, ya que estas plataformas digitales permiten que las instituciones puedan acceder a información de manera ilimitada y que tengan la posibilidad de llegar a los usuarios de forma más rápida, y un tiempo de respuesta menor, así como maximizar la productividad de los recursos humanos. Estas plataformas permiten además tener un mayor alcance, incluso alrededor del mundo.

(Monahan Sánchez J. J., 2012), establece lo siguiente:

Las plataformas digitales son todos aquellos sitios de internet que almacenan información de una empresa y a través de la cual los usuarios pueden acceder a cuentas personales y detalles sobre la empresa. Las plataformas digitales son ejecutadas por programas o aplicaciones cuyo contenido es ejecutable en determinados sistemas operativos, ya sean contenidos visuales, de texto, audios, videos, simulaciones. Éstas se han convertido en el canal de comunicación más importante de las empresas e instituciones ya que les permite llegar a una cantidad ilimitada de usuarios al mismo tiempo, agilizando los tiempos de respuesta, modernizando los procesos a fin de hacerlos más cómodos para el usuario y maximizando la productividad de sus recursos humanos. (p. 25)

Adicional a esto, se puede determinar que, las plataformas digitales también sirven para proporcionar a los usuarios información que se está buscando y facilitar la ejecución de tareas varias, en simultáneo con miles de personas alrededor del mundo. Se entiende, además, que las mismas no tienen una nacionalidad específica, ni tampoco tendrá un dueño, ya que una vez los datos recaen en la web (o red), quedan sujetos al alcance de

cualquier persona, lo que implica una globalización de información que puede incurrir en una vulnerabilidad o riesgo para todos aquellos que ponen la confianza en las mismas.

Hoy en día muchas empresas utilizan la plataformas como medio de trabajo que permite utilizar y optimizar los recursos, adicional que al automatizar determinadas actividades, reducen también el trabajo humano, o incluso lo perfecciona, reduciendo de tal manera el rango de error que se generaba a raíz de los errores provocados por las personas, sin embargo, no se está tomando en consideración el riesgo, ya que no se puede comparar un programa que está diseñado para realizar determinadas tareas contra una persona quien adicional a las indicaciones incluye un criterio y lógica que permite tener un mayor resguardo o protección de toda aquella información que se maneja, especialmente aquella que se considera confidencial.

Clasificación de las plataformas digitales

Existen varios tipos de plataformas las cuales tienen determinadas funciones dependiendo de las necesidades que los usuarios finales vayan teniendo, adicional es necesario tener en cuenta que dicha clasificación no es la única, ya que día a día van surgiendo nuevas ideas y desarrollos que invitan a los programadores y personas expertas a crear nuevas que puedan

cumplir con los requerimientos que se vayan determinando y adicional, se han creado de la mano legislaciones, normas, políticas para proteger en ocasiones el trabajo y la información que se van desarrollando.

Dentro de la clasificación se encuentran las plataformas digitales educativas, las cuales proporcionan información catalogada como útil para investigaciones y herramientas de estudio y análisis. Adicional se encuentran las sociales, que también se conocen actualmente como redes sociales, cuyo objetivo principal es facilitar las comunicaciones entre las personas indistintamente de donde se ubiquen. Asimismo, están las audiovisuales, en donde el contenido se basa en multimedia como videos y audios de determinadas categorías, según la creatividad del usuario. Las plataformas de comercio electrónico también son consideradas como parte de la categorización, en donde existen tiendas virtuales o las conocidas como *e-commerce*, que permite acceder a la compra y venta de productos dependiendo el gusto y necesidad de las personas de manera libre y voluntaria.

Otra de las categorías es la de plataformas bursátiles o *brokers*, que se utilizan como intermediarios entre inversionistas y bolsas de valores, que se usan para realizar negociaciones, las plataformas bancarias, que también se les conoce como banca en línea, que permite hacer transferencias, solicitar estados de cuenta, realizar pagos de servicios y

productos de forma más rápida, evitando apersonarse a una oficina bancaria para la realización de dichos trámites que permite que los clientes tengan mayor accesibilidad y eficacia.

Existen también las Plataformas especializadas las cuales son plataformas que satisfacen una necesidad particular de un sector de la población, por ejemplo, las que sirven para administrar contenido web, páginas de edición de videos o imágenes, plataformas de marketing digital, traducción de idiomas. Otras son las Plataformas de pago que funcionan como administradores económicos a través de los cuales se puede enviar y recibir dinero. Adicionalmente, encontramos las plataformas de noticias que incluyen páginas especializadas en ofrecer noticias de actualidad, como los diarios impresos. Las Plataformas de juego para aquellas personas o mejor conocidas como *gamers online* que su traducción en español sería jugadores en línea, que pueden jugar en solitario o en multiplataforma con otros usuarios. Por último, las Plataformas de localización que ayudan a obtener direcciones de cualquier parte del mundo.

Naturaleza jurídica de las plataformas digitales

Los modelos de las plataformas digitales fueron creados con el objetivo de brindar un servicio de información a todas aquellas personas que tuvieran acceso a la misma. En tal caso se puede determinar que, al ser considerado un servicio el cual debe estar sujeto también a un contrato, y por ende podría establecerse que su naturaleza deviene de un contrato de mediación entre las partes, entre un sujeto que concreta la prestación a cambio de una comisión. En este sentido (Aibar, 2019) en su escrito el trabajo en las plataformas digitales establece que los modelos más simples de plataformas, en los que se establece la interacción de la oferta y la demanda a través de la mera publicación de la información en la plataforma, tienen naturaleza de servicio de la sociedad de la información.

En este sentido, la titularidad de la relación jurídica corresponde a los creadores de las plataformas, así como a los dueños que a través de diversos contratos pueden obtener accesos a ello. Adicional como se ha establecido anteriormente, al momento que los individuos ingresan sus datos personales para poder acceder a alguna plataforma y se sujetan a las condiciones que de ella se derivan, se está teniendo un contrato entre ambas partes, en donde una de ellas (el contratante) se obliga frente al contratado para brindar un servicio.

Ventajas y desventajas de las plataformas digitales

El uso de las herramientas digitales ha cambiado el mundo, otorgándole ciertas facilidades que años atrás no se tenían, sin embargo, existen también ciertos riesgos que se deben considerar que van enfocados mayormente a la vulnerabilidad de la información de las personas al momento de utilizar los mismos. Es por ello que para los efectos del presente trabajo de investigación se considera necesario hacer alusión sobre algunas de las ventajas y desventajas de las plataformas descritas.

En este sentido, se puede determinar que las herramientas permiten crear y gestionar investigaciones de manera sencilla, en la cual se pueden realizar seguimientos exhaustivos sobre cualquier información al instante, lo que aplica para cualquier ámbito, puede ser político, económico, educativo, social. Un ejemplo claro se establece al momento de acceder a los datos de determinadas empresas, las cuales los interesados muchas veces debían apersonarse al lugar para poder solicitar personalmente lo que se requería, sin embargo, hoy en día la mayoría de las sociedades ya cuentan con una plataforma digital en donde se puede acceder y extraer información relevante de la cooperación.

En el ámbito educativo, las plataformas, han sido de gran apoyo para poder tener nuevos métodos de enseñanza, tanto a nivel primario, secundario e incluso a universitario. De hecho, con las nuevas tecnologías se pueden

incluir gran variedad de actividades que pueden tomarse por los estudiantes a cualquier día y hora, según se acomode a sus necesidades o bien permite facilitar el acceso a estudiantes que no pueden salir de sus hogares, o tienen alguna dificultad para poder apersonarse a los centros educativos.

También se puede ver en el sentido social, en donde las plataformas han logrado crear un mayor acercamiento y con ello mejorar las comunicaciones con personas incluso aquellas que se encuentran separadas por países y por zonas horarias. Estas herramientas permiten realizar llamadas en tiempo real, redactar correo o conversaciones instantáneas, así como la creación de foros y los conocidos *Webinar* o conferencias generales sobre temas de interés fomentando el debate y discusión de temas relevantes para los individuos.

Ahora bien, en el ámbito laboral se tienen varias ventajas a considerar respecto a este tema en virtud que facilitan la comunicación entre una persona que se encuentra interesada en adquirir un empleo, frente a un empleador que requiere de alguien para que realice actividades laborales dentro de su sociedad. Si bien es cierto, hace unos años las empresas utilizaban los medios impresos, como los diarios o periódicos locales para poder publicar ofertas de empleo, usando como referencia números telefónicos como medios de comunicación a los cuales los interesados

acudían sin tener la certeza de que se tratara de una compañía formal que realmente se encontraba interesada en encontrar a un empleado. Hoy en día las plataformas se utilizan como un medio que pueden usar las sociedades o bien otros emprendimientos que se constituyen como intermediarios para poder asociar a un futuro empleado con su empleador.

Sin embargo, existen también ciertas situaciones en las cuales colocan al usuario en desventaja al usar este tipo de herramientas, uno de ellos es la falta de seguridad de la información que está utilizando. Es preciso tener en cuenta que muchas veces los datos se almacenan en una nube, de la cual no se tiene control sobre lo que se encuentra, y al ser “subida” a dicha red se convierte en pública, de tal forma que los dueños de estas pueden tener acceso en cualquier momento a la información confidencial de las personas.

Adherirse a un contrato, el cual deja una vulnerabilidad en la protección de los datos, y permite que las empresas se adueñen de todo aquello que se sube a la red, en donde se puede tener acceso de los datos sensibles de las personas como lo son los nombres, dirección de domicilio, estado civil e incluso a los estados de cuenta, lo que deja en un estado de indefensión a las personas quienes utilizan las mismas, indistintamente si se ingresan los datos para adquirir una aplicación de recreación o si buscan un empleo.

Existe también una falta de regulación para proteger los datos de las personas que se someten a este tipo de contratos, permitiendo que los mismos se puedan estructurar de manera arbitraria y sin buscar la protección del cliente. Esto que provoca que la información del cliente quede en estado de vulnerabilidad. Adicional se considera que para tener resultados de protección se requiere de una sanción y en este caso al no tenerlo, no habrá modificaciones y se continuará violando el derecho de privacidad de los usuarios que hacen el uso de las plataformas digitales propiamente.

Necesidad del uso de plataformas digitales como medio para adquirir empleo

En este escenario, se puede establecer que actualmente la mayoría de las personas interesadas en adquirir un empleo buscan a través de la web, ingresar a páginas que permitan tener comunicación con empresas quienes publican ofertas de trabajo según las necesidades profesionales que tengan, en dichas solicitudes se colocan los requisitos que deben cumplir para poder ser parte de la bolsa de empleo y en base a ello las personas aplican para que se inicie con el proceso de selección propiamente dicho.

Adicional a ello, existen también ciertas empresas cuya razón social es ser intermediarios entre los empleados y empleadores, las cuales pueden acercarse a través de plataformas digitales, como lo son Computrabajo, Jobmas, aplicaciones como LinkedIn o incluso ciertos programas como Valentina, que buscan conectar a las personas, considerando sus características, cualidades, oportunidades y fortalezas y aquellas aptitudes que las empresas, asociaciones o cualquier tipo de cooperación requiera.

Muchos autores mencionan que las plataformas digitales son parte de la evolución en el mercado laboral, en el entendido que prometen nuevos medios de comunicación entre las empresas y los posibles candidatos a una plaza. Además, existen plataformas que le dan la oportunidad a las personas de obtener un entrenamiento previo de cómo llevar a cabo entrevistas de trabajo, llenar formularios para la aplicación, o incluso cómo deben verse sus hojas de vida. Sin embargo, para que puedan acceder a este tipo de capacitaciones también deben suscribirse a páginas web que solicitan datos personales los cuales, al momento que el usuario desea salirse o dejar de pertenecer a la misma, no existe garantía que su información sea protegida, por el contrario, éstas se convierten en públicas y se encuentra vulnerables.

Es preciso tomar en cuenta, que muchas veces son personas jóvenes quienes con el afán de conseguir un empleo ingresan sus datos, quienes, por tener una mayor facilidad en el desarrollo de habilidades digitales, buscan aumentar sus posibilidades de ser tomados en cuenta para ofertas de trabajo y no se interesan con lo que pasa con todos aquellos datos que ingresan para poder aplicar o ser parte de las mismas. Muchas veces, las mismas páginas web, generan correos automáticos para los usuarios, donde no solo ofrecen trabajo, si no, además, envían publicidad de ventas de productos u otros servicios, por el simple hecho de tener la facilidad, con lo que se enriquecen.

Resguardo de los datos personales

Análisis de los términos y condiciones, así como políticas de privacidad de los sitios de bolsas de empleo

Existen muchas plataformas que buscan ser mediadores entre empresas como posibles contratantes y personas cuyo perfil académico, personal y profesional pueden ser considerados como candidatos para obtener la plaza laboral que se publican, en donde a través de un *click* pueden generar contratos, en donde se establecen las políticas y condiciones del uso de las mismas, así como los derechos que tienen las páginas sobre los datos que se van ingresando de acuerdo al interés del usuario.

Para el efecto del presente trabajo de investigación se considera importante, llevar a cabo un análisis sobre las disposiciones que se tienen, en las que el usuario acepta con facilidad, con el fin de poder acceder y ser tomado en cuenta al momento que se publique una plaza. Este tipo de acuerdo al ser creado por medio de una sola parte (en este caso los creadores de la plataforma) podría considerarse como un contrato de adhesión, el cual se define como aquel acuerdo en el cual una de las partes (usualmente una sociedad mercantil) impone sus condiciones a quienes desean contratar con ella, sin posibilidad que exista una negociación sobre los términos y condiciones que puedan surgir.

Usualmente, este tipo de contratos van de la mano de un formulario, que facilita el tráfico mercantil en masa, en este caso al no ser un escrito físico y como se ha determinado anteriormente, a través de una casilla o un *click*, la persona incluso sin necesidad de leer el contenido puede adherirse a las condiciones que sin ellas no podrían acceder a la plataforma ni tener el beneficio que las mismas ofrecen. Es necesario tomar en cuenta, que es un derecho de las personas (empresarios) de crear las disposiciones, y permitir que el usuario decida si desea o no ser parte de la misma, ya que están en todo su derecho. Y legalmente, es una facultad que tienen de poder establecer contratos, los cuales son públicos y opcionales.

El problema surge, a raíz que estos contratos muchas veces, otorgan los derechos de propiedad de la información de todos los usuarios, durante el plazo de su suscripción o incluso cuando se prorrogan sin el consentimiento de la persona. En estos también se establece la facultad de poder disponer de los datos de los usuarios con el fin de realizar estudios estadísticos sin necesidad de notificarle al posible trabajador, sobre los mismos, o bien los resultados que de ellos se pueden derivar.

Adicional, en vista que los datos están a disposición de terceros, se establece la posibilidad de compartirlos con las autoridades estatales, siempre que se tenga algún motivo u orden judicial para poder entregarlos. Esto también se considera una vulnerabilidad de la información de las personas, ya que ésta debería de ser estrictamente personal y no sujeta a investigaciones, ya que para ello existen los registros públicos los cuales están avalados por la ley y conllevan procedimientos específicos para que puedan ser sujetos de investigaciones o indagaciones policiales o legales.

Este tipo de plataformas también permiten que se genere una búsqueda en otras páginas o buscadores, por ejemplo en *google*, en donde cualquier otra persona puede ingresar el nombre y apellido de aquel individuo de quien se desea tener información para que despliegue todas aquellas páginas web en donde la persona está suscrita, incluso se puede también tener acceso a fotografías, nombres completos (donde se incluya el

nombre de pila y apellido), números telefónicos o incluso direcciones personales en donde pueden ser ubicados con facilidad, lo que genera una vulnerabilidad de las personas quienes están suscritas a las mismas.

Se permite también, el envío de mensajería instantánea, en donde no solo se mandan correos de la plataforma, para notificaciones de nuevas ofertas de empleo, sino también para publicidad de terceros quienes no tienen injerencia directa en el contrato principal al cual el usuario se adhirió. Esto muestra que existe un comercio no autorizado de los datos, lo que muestra nuevamente que, al no existir directamente una legislación con sus respectivas sanciones, se continúa generando el mal uso de las mismas.

Las plataformas se guían dentro de un acuerdo, que el usuario al colocar el botón acepto, se adhieren a las disposiciones, las cuales, en su mayoría de veces, son contratos muchas veces abusivos, ya que a sabiendas que los usuarios no leen completamente su contenido, acto el cual es responsabilidad del cliente, se aprovechan y crean clausulas en donde se puede disponer completamente de la información, la pueden compartir o vender dependiendo las necesidades y disposiciones que de ella devengan.

Muestra de lo anteriormente expuesto, se puede mostrar dentro del contrato de confidencialidad de las plataformas que ofrecen empelo lo siguiente: (Computrabajo, 2019) agregada que no te identifica para fines

analíticos y estadísticos, que nos da un mejor conocimiento de los usuarios de nuestra web en su conjunto y nos ayuda a ofrecerles un mejor servicio”

Dentro de los acuerdos también se establecen plazos los cuales muchas veces son indefinidos, lo que abre una ventana para que, sin importar el año, el usuario ya no sea dueño de su propia información. Al tener un acuerdo o contrato tan arbitrario, las plataformas, abusan de su contenido y por ende en la mayoría son plazos indefinidos o se coloca como cláusula que serán (Computrabajo, 2019) “Conservados mientras la cuenta en el portal web siga activa o en la medida en que sea necesario para proporcionar los servicios, hasta que se solicite la supresión, así como el tiempo necesario para cumplir las obligaciones legales”

Es necesario tomar en cuenta, que la *web* es una red que conecta más de una plataforma, especialmente aquellas que buscan generar empleos, y por lo tanto en sus políticas también se incluyen disposiciones en las que de forma indirecta establecen el derecho de poder adquirir información de un tercero. En dado caso, el usuario acepta a través de un *click*, que otras páginas o sitios web puedan brindarle información registrada, la cual puede incluso ser considerada sensible sin perjuicio que la misma conlleve una consecuencia jurídica o económica a los creadores de las mismas. Dando lugar a un comercio de información incontrolable.

La tecnología ha llegado a tal nivel, que incluso dentro de las políticas o contratos digitales el usuario acepta otorgar su ubicación, lo cual pueden acceder desde un dispositivo móvil y controlar los lugares que se frecuenta o bien simplemente tener acceso a su dirección *IP*, lo que se entiende como el conjunto de números de forma lógica y jerárquica a una interfaz en la red de un dispositivo, el cual puede ser una computadora o cualquier otro aparato, servidor proxy (Entendido como los puentes de origen o intermediario entre conexiones, clientes y servidores de destino) , sistema operativo, navegador *web* y complementos que le corresponde al computador en donde se tiene acceso a las páginas, lo que deja también desprotegida a la personas quien tenga interés en encontrar un empleo a través de las mismas.

Es importante tomar en cuenta que, muchos de los oferentes de empleos, proporcionan información a través de la interconexión sociedades y posibles candidatos, sin embargo, no existe un política o la obligación de crear una, que investigue sobre la legalidad de las empresas que están solicitando personas que cumplan el perfil para determinados puestos de trabajo, y dentro del acuerdo, se autoriza al posible contratante a acceder a los datos y hojas de vida que los usuarios cargan, lo que deja en un estado de vulnerabilidad al solicitante, en virtud que en dichos documentos y perfiles se encuentran datos como el nombre, la dirección, estado civil,

números de teléfonos con contactos de familiares y conocidos, en donde quedan totalmente sin protección al momento de publicarse.

Otro aspecto a tomar en cuenta, es que producto de la venta de la información entre plataformas o la simple adquisición por medio de acuerdo por ella, los usuarios muchas veces se suscriben y aceptan que les envíen publicidad de comercios, encuestas, boletines y según el acuerdo de confidencialidad de la plataforma de (Computrabajo, 2019) se establece en ese sentido que “Envío de comunicaciones comerciales, encuestas, boletines, invitaciones a *webinars* (entendidas como conferencias impartidas por profesionales o expertos en una materia, las cuales se realizan a través de plataformas digitales), para informarte de nuestros productos, servicios y eventos, siempre que contemos con tu consentimiento para ello”.

Existen, además, ficheros donde se almacenan toda la información los cuales son automatizados, el cual, según el acuerdo de las diferentes páginas web, no existe protección sobre todo lo que se guarda allí, únicamente se menciona la existencia de los mismos, lo deja en un estado de vulnerabilidad a las personas nuevamente. Se considera importante tomar en cuenta que, a pesar que hoy en día, una vez cierta información se suba a redes, plataformas, sitios web, se consideran públicas, el Estado debe velar porque las mismas cumplan con determinados requisitos que

garanticen la protección de la información y no dejen en estado de indefensión a los ciudadanos, quienes dadas las necesidades de laborar, acceden e ingresan datos personales, los cuales son archivados en un sitio web o fichero electrónico, del cual nadie puede asegurar su resguardo. A efecto de evidenciar lo anteriormente expuesto en la política de seguridad de la página.

(Jobmas, 2021) se establece lo siguiente:

Se propone ceder los Datos Personales a los Oferentes de Empleo, con la finalidad de permitirles estudiar y seleccionar posibles candidatos para puestos laborales vacantes en la compañía del Oferente de Empleo. En ciertos casos, además, JOBOMAS se propone ceder los Datos Personales a terceros.

Al analizar las disposiciones establecidas dentro de los acuerdos, se puede determinar que sí existe una vulnerabilidad en la información, en donde no se garantiza que la misma no pueda ser comercializada entre más usuarios, con empresas o con otras páginas *web*, las cuales generan una red de compra-venta de información la cual hoy en día es algo muy común. Adicional, a pesar que los contratos establezcan que el almacenamiento de los datos será hasta que la persona o usuario final desea, no se ve la intención de resguardo, incluso después de la cancelación de suscripciones. Lo que deja una laguna y desprotección a los clientes que por estar en la web el Estado tampoco busca proteger.

Es obligación del Estado, especialmente el de Guatemala, reconocer y proteger el derecho a la privacidad, según lo establece la Constitución Política de la República de Guatemala, sin embargo, al momento que las personas acceden a las plataformas y se suscriben a las páginas para adquirir empleo, no se ve ninguna intención de regular o garantizar que la información no sea objeto de comercialización, divulgación, traslado o incluso contrabando de terceros quienes con diferentes fines disponen de ella sin tener consecuencia alguna sobre los mismos.

El riesgo de la vulnerabilidad de la información de los datos personales

Todos los días más y más información es procesada por los medios o redes en donde millones de personas acceden, se suscriben, ingresan para poder obtener información, buscar empleo, leer sobre noticias, entre otras, lo que ha generado hoy en día una red cuya protección va más allá de lo que se puede controlar. Al efecto Valentina Hernández en su escrito denominado La vulnerabilidad de nuestra información personal, ¿un mal incurable? se pronuncia con la frase (Hernández, 2016) “La falta de estándares técnicos de seguridad de información sensible puede significar que nuestros datos queden expuestos. La falta de herramientas legales para asegurar esos estándares puede resultar en fuertes afectaciones a los derechos fundamentales de sus titulares”. (p.1)

Indistintamente del comercio que existe entre las plataformas, los usuarios también corren el riesgo de ser objeto de cibercriminales, o personas que se dedican al *hacking* o hackeo de sistemas con el fin de adquirir de forma ilegal la información o datos que los usuarios suben a la web. Hoy en día existen legislaciones extranjeras que protegen la información y con ello castigan a los “ladrones cibernéticos”, sin embargo, sucede mayormente cuando la información proviene del Estado, sin embargo, no existe una protección formal para los pequeños navegadores quienes son objeto del estudio del presente trabajo de investigación.

En las empresas, también se puede ver reflejado este riesgo, ya que muchas de ellas llevan registros electrónicos de su personal, a quienes ya se les armó un expediente laboral, se tiene un registro en una nube, la cual puede ser objeto de robo si no cuentan con los programas o medidas necesarias para poder resguardar la información. Es necesario tomar en cuenta que dichos softwares que ayudan con el cuidado, son costosos y por ende no todas las compañías tienen la facilidad de acceder a uno de ellos, lo deja una ventana y vulnera la protección de los datos de sus trabajadores.

El valor económico de los datos personales

Los datos personales se pueden considerar como un activo intangible ya que son considerados fuentes de información de donde se puede extraer información relevante de los usuarios como sus gustos, aficiones, el lugar donde se encuentran situados, incluso las propias cuentas bancarias o cualquier otro tipo de información sensible relevante que pueden ser encontrados con facilidad, especialmente en las diferentes plataformas digitales en donde el usuario se somete a diversas políticas y acepta la distribución y comercialización de los datos, de tal manera que los mismos pueden ser objetos de comercialización por parte de las empresas que tienen ánimo de lucro.

Pero muchas veces las personas se preguntan ¿Cuál es el valor de los datos? ¿Por qué el interés de las personas de poder adquirir información sobre un determinado grupo de personas? Y parte de la presente investigación es poder determinar y resolver estas inquietudes. Comenzando por esclarecer que, la mayoría de la información objeto del comercio se utiliza mayormente para poder llevar a cabo estudios, estadísticas y también la utilizan para enviar anuncios promociones a sus cuentas electrónicas, números de teléfonos, redes sociales o cualquier otro medio basado en los gustos y características personales que se pueden

determinar derivados de toda aquella información que se puede extraer de las plataformas digitales.

Para las sociedades mercantiles que se dedican al comercio de los datos personales de las personas que se adquieren de las diversas plataformas digitales, la venden debido a que la información tiene relevancia para poder tener acceso a las preferencias de los usuarios, para prestar facilitar la propuesta de productos, mejorar la oferta y demanda en determinados productos, determinación de riesgos en los casos de los seguros de salud o vida de las personas, ya que al tener este tipo de conocimientos incluso pueden establecer los riesgos que pueden incurrir y por ende podrían aumentar el precio de las pólizas o negarles el servicios, toda esta data es relevante ya que se convierte en un factor comercial que cada día adquiere más poder en el mercado.

Existe para muchos una oportunidad económica que representa el uso de datos personales, según el artículo denominado *The economic value of Data- Discussion Paper* publicado en el año 2018, ponen de manifiesto algunos elementos relevantes relacionados a la información extraída, que parten de la oportunidad económica, del uso y explotación a través de mecanismos y técnicas tales como la inteligencia artificial, que permiten se adopten estrategias de para mejorar las estrategias de venta, ya que al no existir una regulación o política que protejan los datos de las personas,

la misma se pueden adquirir de forma gratuita, sin mayor limitación, especialmente de aquellos derivados de las plataformas que ofrecen ser una outsourcing de conexión laboral entre posible empleado y empleador.

(Bonina, 2014) indica:

Con relación al valor monetario de los datos abiertos, la empresa consultora McKinsey, publicó en 2013 el informe *Open data: Unlocking innovation and performance with liquid information*, en el que aborda su capacidad para generar información con un valor monetario; analizando cómo los datos abiertos crean valor económico en términos de ingresos, disminución de gastos y ahorro de tiempo.

De acuerdo con lo establecido en el párrafo anterior, se puede determinar que efectivamente existen estudios especializados en el valor de los datos, especialmente porque existe una alta disponibilidad de información, por ende, se determina que existe una capacidad para establecer el valor en término de costos de venta de los datos, que hacen los mismos sean considerados objetos de comercialización. (Bonina, 2014) “El estudio estima un valor monetario anual de los datos abiertos en más de tres billones de dólares; sin considerar el valor que supondría para los consumidores y empresas el intercambio de datos, aumento de la productividad, transparencia de precios (...)”

Parte de lo que le da valor a los datos según el análisis de McKinsye del 2018, se basa en los siguientes aspectos: Primero la accesibilidad, ya que se existen hoy en día incontables páginas de internet de donde se pueden

adquirir la información, así como las que son objeto de la presente investigación que se dedican a recolectar datos personales de personas que buscan un empleo; segundo la legibilidad que va derivado de la automatización de la carga y descarga de información que se puede llevar a cabo por cualquier persona con conocimiento técnico, por la falta de regulación y políticas de protección que existe actualmente. Como tercer punto se tiene el costo, ya que derivado de la premisa anterior sobre la falta de regulación y debido a que se trata de millones de datos, basado en las leyes del mercado, el costo es mínimo y finalmente los derechos, que son mínimos y por ende los datos que se adquieren son abiertos y están expuestos a casi todos.

Existe además, un potencial económico que alcanza un valor de billones de dólares y cada día va aumentando ya que se están generando nuevas oportunidades de negocio en donde los consumidores están empezando a obtener ventajas de los datos abiertos, que ayudan a mejorar la productividad empresarial y la creación de nuevos productos y servicios basados en el análisis de datos derivados de las preferencias de los usuarios, especialmente aquellos derivados de las hojas de vida, cartas de presentación o solicitudes de empleo, en donde además se suscriben sin intención, a programas en donde se manejan, estudian y distribuyen los datos.

Adicionalmente se realizó otro estudio (OECD, 2013) el cual se le llamó *Exploring the Economics of Personal Data a survey of methodologies for measuring monetary value* el cual se traduce al español como: Explorando la Economía de los Datos Personales una encuesta de metodologías para medir el valor monetario (la traducción es propia), en donde se aprecia que, efectivamente existen maneras de poder medir el valor de los datos, a pesar que estos sean valores intangibles y que incluso se pueden tener alcance en cualquier momento, en muchos sitios y que devengan de diferentes fuentes de información. Para el efecto existen metodologías que ocupan una metodología económica, sin embargo, no existe un modelo actualmente, que sea homogéneo ya que cada interesado puede determinar el valor dependiendo de las necesidades que se tengan y los modelos de negocio de las empresas.

Es por ello que, para determinar el valor de los datos se pueden generar estrategias estructuras, que tengan como objetivo principal potencializar los beneficios del procesamiento de los datos personales, para poder generar escalas que maximicen el uso, midiendo los beneficios sociales y económicos, que vayan derivando de la información, lo que genera entonces, una necesidad de poder explorar nuevas estrategias para poder darle valía a los datos, identificando modelos de aplicación basando en los datos personales, en donde se tome en consideración el trabajo de análisis,

los riesgos, y sobre todo velando porque en ningún momento se viole el derecho de protección de la información de las personas.

Regulación extranjera de plataformas digitales y protección de datos

Los datos personales y su debida protección han sido objeto de regulación en diversos países, sin embargo, para los efectos del presente estudio se tomarán en cuenta los países de México, Argentina y Costa Rica por ser influyentes dentro de la legislación de Guatemala, en términos generales para poder determinar si lo que se incluye en la normativa pudiera ser aplicado tanto de forma general como puntualmente para aquella información que se deriva de las plataformas digitales que buscan ser un intermediario entre los posibles empleadores, es decir empresas que buscan contratar al personal dependiendo de las necesidades del puesto y las aptitudes del usuario y el posible trabajador que utiliza y se somete a las políticas y condiciones ante la necesidad de conseguir un laboro, haciendo efectivo su derecho humano al trabajo.

En México, existe actualmente una ley de protección de datos personales, derivada de la necesidad que surge a raíz del incremento del uso del internet y de toda la información que se gestiona diariamente, en donde ante el riesgo de la vulnerabilidad de información México decide proteger constitucionalmente la privacidad de sus habitantes y además, promulgó

y sancionó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares o bien Ley de Protección de Datos en cuyo contenido, se regula el respeto de los derechos de los dueños de la data, en donde además se crea un Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), el cual creó guías y documentos de relevancia sobre los modelos y estatutos a tomarse en cuenta al momento de utilizar los datos de los usuarios.

La norma mexicana, va dirigida mayormente a todas las empresas del sector privado que, de alguna manera, obtengan, usen, almacenen y/o transfieran datos personales como parte de sus actividades que también se le denomina “tratamiento de datos personales”, en donde existen dos sujetos, (Salesforce, S, 2013) “el responsable y el encargado, siendo el primero la persona del sector privado que toma las decisiones sobre tratamiento de las personas y el segundo la persona ajena al responsable que trata los datos por cuenta del responsable y de acuerdo con las instrucciones”.

La norma indica además algunos principios cuyo cumplimiento debe velar, esto de acuerdo a los artículos del 6 al 21 de la mencionada ley, en donde se incluye, la licitud, ya que adquisición de datos debe haberse obtenido sin engaños ni intenciones fraudulentas si no por el contrario, debe apegarse a la norma, el consentimiento pues, el usuario debe dar su

aprobación de forma expresa sobre la disposición de su información, sin embargo en este supuesto también existen determinados supuestos de excepciones en donde no será necesario su aprobación cuando la información devenga de sitios considerados públicos, los que se sometan a un procedimiento previo de disociación, los que se derivan de la relación jurídica de los sujetos antes mencionados, y los que sean pertinentes para diagnósticos médicos que adquieran relevancia en la salud del paciente, por lo demás se necesita de su autorización para poder ser utilizados.

También se considera como principio la calidad de los datos ya que éstos deben ser exactos, precisos, completos, correctos y sobre todo actualizados, lo que da una protección a las empresas que se dedican a comercializar la información quienes de forma lícita desean adquirirlos. La finalidad es otros de los principios a tomar en cuenta, el cual es muy importante ya que indica que el uso de los datos debe de apegarse a lo que estableció en el acuerdo el cual el usuario daba su aprobación, no puede salirse más allá de lo que indica la norma. Respecto a la proporcionalidad que se menciona va de la mano con la responsabilidad en donde la empresa debe responder por el uso que se le dé a los datos personales el cual deberá ser adecuada y relevante.

Dentro de la norma se establecen las obligaciones y responsabilidades que deben tener las empresas para el manejo de datos, en donde se incluyen otorgar a los titulares los detalles del destino de sus datos personales, de manera de poder ser lo más transparentes y apegadas a derecho y velar que no se violente en ningún momento su derecho a la intimidad. Ante esto existe en la ley una serie de recomendaciones a considerarse, tales como: Dar aviso de privacidad informando a los usuarios la existencia y características del tratamiento de la información, tener el consentimiento expreso de la voluntad por escrito, a menos que exista un aviso o publicidad que haga evidente el motivo de la suscripción y el uso que se le darán a los datos.

El usuario además, tendrá el derecho de rectificar la información, cancelar todo tipo de suscripción y oposición del titular, además de ejercer el derecho de acceso, y al conjunto de estos derechos se les denomina, de acuerdo con la ley, Derechos ARCO, estos derechos los deben otorgar las empresas y aquellas que no han implementado las medidas para garantizar el cumplimiento de dichos derechos, deberán ajustarse para poder cumplir con lo que establecen las normas y cumplir los requisitos pertinentes sobre el manejo de los datos.

En Argentina, también existe una regulación Ley de Protección de los Datos Personales, promulgada en octubre del año 2000, que busca proteger los datos personales, especialmente aquellos relativos con la intimidad y honor de las personas, sean éstos públicos o privados, y para el efecto es necesario mencionar que, la norma da varios conceptos relevantes para comprender cuál es el objeto de la ley al igual que su contenido y hace una clasificación de los datos, en donde se destacan los datos informatizados, los cuales son sometidos al tratamiento o procesamiento electrónico o automatizado, y a pesar que no hace una especificación de las plataformas que se utilizan como medios de adquirir empleo, al generalizarlo también está protegiendo a todos los sujetos que se suscriben a ellos.

Al igual que en la legislación mexicana, la de Argentina, hace mención a los principios de licitud, calidad de los datos, el consentimiento, la información, la categoría de datos, pero en esta se incluyen también los referentes a la salud, en donde le da la facultad a toda institución sanitaria sea pública o privada a recolectar y tratar datos de pacientes como objeto de estudio con la salvedad que se debe respetar el secreto profesional.

Adicional es necesario tomar en cuenta que la norma hace una salvedad sobre la cesión de los datos personales, en donde puede existir una cesión de derechos, pero no puede ser utilizado más allá de lo que se había

pactado inicialmente y siempre se debe respetar el derecho humano de la intimidad de las personas.

Un factor importante, es que los datos no pueden ser comercializados con otros Estados, que no cumplan con los lineamientos de resguardo, o que tengan los niveles de protección adecuados, existen excepciones al supuesto, como para efectos de procedimientos judiciales en donde sea necesaria para esclarecer un acto que se considere delictivo, es decir para poder determinar la culpabilidad o inocencia de un sindicado, para los temas de las investigaciones médicas, como en el caso de las epidemias o pandemias en cuyo el uso de la misma puede apoyar para salvar una vida, o algún otro tipo de cooperación internacional necesario. De lo contrario no se podrá violar el derecho de los usuarios.

El titular de los datos, tiene el derecho de conocer hacia dónde va su información cuando así lo requiera en cuyo caso, se tiene un plazo de diez días para que quien los tenga se pronuncie y le indiquen el uso, la calidad y demás cuestiones relevantes que puedan ser de su interés. Ésta la deben suministrar de forma clara y si en algún momento se utilizan términos ambiguos o específicos de determinada materia, como por ejemplo informáticos, deben ir acompañado de una explicación. Si la información tiene algún error se tiene el derecho de rectificación, supresión o actualización cuando así lo sea requerido.

Respecto a los datos informatizados, es necesario que sean utilizados para el fin que se establece dentro de las disposiciones a las que se sujetan los titulares, no puede tener un objetivo diferente, ni pueden existir cláusulas ambiguas u obscuras que pretendan engañar sobre el manejo de los datos, tampoco se pueden ceder a terceros que no sean parte o no figuren dentro del acuerdo, ya que esto lo contempla también la legislación. Al momento que se concluya la prestación contractual, la información debe ser eliminada o resguardada por un periodo máximo de diez años.

En Costa Rica, también existe una normativa que ampara los derechos del personal, la cual es la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, ley número 8968, la cual fue promulgada en septiembre del año 2011, en la cual se hace una interesante alusión al concepto de autodeterminación informativa, que se entiende como el derecho de poder controlar el flujo de la información que concierne a cada persona, lo que se deriva del derecho de privacidad.

En esta norma al igual que en los otros países se hace alusión al consentimiento que como en cualquier contrato es un elemento fundamental para que se pueda comercializar los datos o disponer de ellos, esta autorización debe hacerse por escrito el cual puede ser por medio de documento electrónico, que para el efecto de la presente investigación sería el medio idóneo para llevarse a cabo, el cual puede ser revocado.

También en la norma se establecen los principios que se deben apegar como el de la veracidad, en donde se deben omitir aquellos que falten a la verdad, el de exactitud y deben tener fines explícitos y específicos, para que el titular esté anuente del uso que se le dará a los mismos.

También se regulan los derechos de los usuarios dueños de la data, en donde garantizan el libre acceso a sus datos, además de proporcionar la opción de rectificarlos o suprimirlos en el momento que así lo deseen o bien que tengan alguna sospecha que no están siendo utilizado para los fines que se les habían indicado al momento de suscribirse o brindar su consentimiento para su libre uso. Al igual que en las legislaciones anteriormente citadas se establecen excepciones sobre la protección, donde se incluyen los casos específicos de la seguridad del Estado, la seguridad pública, prevención o sanción de sujetos que se encuentran en algún proceso penal o relacionado a la comisión de un delito, entre otros, de lo contrario la norma le exige al responsable de la base de datos, adoptar las medidas técnicas y organizacionales que garantiza la seguridad y el respaldo para los casos de pérdidas de los mismos.

En Guatemala por su parte, no existe una ley específica que proteja los datos personales de los titulares, únicamente se pueden encontrar supuestos en donde se resguarda la privacidad e intimidad de las personas, como lo que aparece en la Constitución Política de la República de

Guatemala, que, al ser un derecho humano, también aparece en Convenios Internacionales a los cuales Guatemala está adscrita, pero estas leyes lo regulan teniendo un carácter general cuando debiera de ser específico.

Al efecto la Corte de Constitucionalidad se ha pronunciado dentro del expediente 863-2011 en donde se pronuncia indicando los avances de la tecnología dificultan la protección a la intimidad y privacidad de las personas, y se propone reconocer el derecho de la autodeterminación que también lo protege la legislación de Costa Rica como un derecho para garantizar la tutela de la persona ante el uso indebido por terceras personas especialmente para el comercio de la información que puede ser vulnerable.

Es por ello que en Guatemala fuera de los Convenios que ya se han ratificado, debe existir una nueva normativa que proteja a los usuarios sus datos a los cuales están suscritos, para que puedan rectificar, modificar o suprimir en el momento que así lo soliciten y que no permitan que las plataformas y empresas que se dedican al comercio, establezcan de forma arbitraria las políticas y condiciones a las que deben sujetarse sin derecho alguno a tener una garantía sobre el destino de los mismos.

Adicional, se deben regular los principios tomando a ejemplo las legislaciones extranjeras citadas en el presente trabajo de investigación, como el de licitud, para que los usuarios puedan utilizar las plataformas con la garantía de que están siendo objeto de engaños ni existe una mala fe por parte de los dueños de las empresas que se dedican al comercio. También considerar regular los procedimientos referentes a las sanciones en casos de incumplimiento de las disposiciones normativas, establecer la creación de organizaciones u asociaciones que puedan apoyar con la protección de los datos sensibles de las personas.

Tomar en cuenta además el principio de claridad de los datos, en donde se establezca claramente el destino para lo que van a ser utilizados, es decir que la información que se utilizará en las plataformas digitales derivadas de las bolsas de empleo tengan únicamente esa finalidad, es decir que solo las puedan compartir con las empresas interesadas en emplearlos y no ser producto de compraventa con otras que se dedican al análisis de datos, distribución ilegal de los mismos u otra actividad que pueda dejar en estado de indefensión a las personas.

Conclusiones

Con relación al objetivo general que se refiere a determinar si la protección de datos personales en plataformas digitales logra resguardar la información derivada de la bolsa de empleo y relaciones laborales, se concluye que, no existe un resguardo adecuado a la información personal cuando ésta se deriva de las plataformas digitales que se dedican a encontrar posibles empleados y conectarlos con los posibles empleadores o empresas, teniendo la calidad de bolsas de empleo, ya que dentro de sus políticas no se incluyen disposiciones a favor de la protección de la información, por lo que tampoco se garantiza la certeza jurídica sobre destino y uso de todos los datos recopilados.

El primer objetivo específico que consiste en, precisar el concepto de datos personales y determinar si existe vulnerabilidad al momento de ingresar los mismos en las plataformas digitales de bolsas de empleo, al realizar el presente trabajo de investigación, se arribó a la siguiente conclusión en donde se establece que, existe una vulnerabilidad de la información por la falta de una regulación específica en Guatemala que pretenda proteger los datos personales y profesionales de los usuarios que se suscriben con la intención de hacer valer su derecho humano al trabajo, a las múltiples plataformas que son una conexión entre un posible trabajador y un patrono en búsqueda de servicios profesionales, pero que además se dedican a

ofrecer la información como objeto de comercio, tanto dentro como fuera del país.

Con relación al segundo objetivo específico que consiste en analizar la regulación y uso de las plataformas digitales como medio utilizado para adquirir información personal y su relevancia en el derecho de protección de datos personales, se concluye que, en países como Argentina, México y Costa Rica si existe una legislación que protege el manejo de los datos y les otorga derechos a los titulares de rectificar, modificar o incluso retirar la información que se obtienen como consecuencia de la suscripción a páginas u cualquier otro sitio, sin embargo, Guatemala aún no cuenta con una normativa, por lo que se concluye que existe una necesidad actual que proteja toda la información sensible y personal de los usuarios con el objetivo de conseguir un empleo.

Referencias

Libros

Aibar, J. (2019). *El trabajo en las plataformas digitales. El Trabajo En Las Plataformas Digitales*, 33, 1–26.

Cahuec, L. E. (2015). *Negociación indebida y debida de datos personales*. Guatemala: Universidad Panamericana.

Gómez, L. O. (1999). *El derecho a la intimidad, la vision iusinformatica*. España: Universidad de lleida.

Monahan Sánchez, J. J. (2012). *Protección de datos personales e información privada de los particulares*. (Tesis de pregrado) Guatemala: Universidad Panamerica.

Oriano, P. (2005). *La Mediación Figurativa como Historia del Habitar, Público y Privado*. Argentina: l Nobuko.

Ovalle de la Vega, I. E. (2012). *La incidencia de la comercialización de datos personales* (Tesis de pregrado) Guatemala: Univesidad Panamericana.

Recio Gayo, J. P. (2016). *Protección de datos personales e innovación: ¿(in)compatibles?* (1.aed.). España: Reus.

Nisa Ávila, J. A. (2020). *Origen jurídico histórico de la protección de datos: de la evolución de las diferentes teorías jurídicas que la han protegido.*

Legislación nacional

Asamblea Nacional Constituyente. (1986). *Constitución Política de la República de Guatemala.*

Congreso de la República de Guatemala. (2008) *Decreto 57-2008, Ley de Acceso a la Información Pública.* Publicado en el Diario de Centroamérica, No. 45, del 23 de octubre de 2008. Guatemala

Jefe de Gobierno de la República (1963). *Decreto Ley 106, Código Civil.*

Legislación internacional

Asamblea General de las Naciones Unidas (1948) *Declaración Universal de Derechos Humanos.* París

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso (2000), *Ley 25.326 Ley de Protección de Datos Personales*, del 4 de octubre de 2000. Argentina.

Asamblea Legislativa de la República de Costa Rica, (2011) *Ley Número 8968, Ley de Protección de Datos. Publicada en la Gaceta Número 170*, del 5 de septiembre de 2011. Costa Rica.

Presidencia de la República (2010), *Ley Federal de protección de datos personales en posesión de los particulares*. Publicada en el Diario Oficial, del 27 de abril de 2010. Estados Unidos Mexicanos

Artículos obtenidos de internet

Castro Rojas, S. R., Luna, R., Servidía, F., Gallego, F., Demains, J., Britez, M. R., Re, M. Rodriguez, J. (2012). *Redes digitales y comunicación: historia de las plataformas y nuevos vínculos sociales*. Universidad Nacional de Rosario. <https://rehip.unr.edu.ar/handle/2133/3742>

Bahilo, L. (2021). *Historia de Internet: cómo nació y cuál fue su evolución. Marketing and Commerce*. <https://marketing4ecommerce.net/historia-de-internet/>

Bonina, C. (2014). *El valor de los datos abiertos en América Latina: oportunidades y desafíos para la innovación en ciudades abiertas*. Obtenido de <https://idatosabiertos.org/el-valor-de-los-datos-abiertos-en-america-latina-oportunidades-y-desafios-para-la-innovacion-en-ciudades-abiertas/>

Computrabajo (2021). *Computrabajo* <https://www.computrabajo.com.co>

De Mata, D. (2021). *La privacidad de datos en Guatemala y los derechos fundamentales que se derivan de la misma según la jurisprudencia de la Corte de Constitucionalidad*. Recuperado de: <https://consortiumlegal.com/la-privacidad-de-datos-en-guatemala-y-los-derechos-fundamentales-que-se-derivan-de-la-misma-segun-la-jurisprudencia-de-la-corte-de-constitucionalidad/>

Deloitte (2019) *Entendiendo el Reglamento General de Protección de Datos (GDPR) Un breve recorrido por los aspectos clave*. Recuperado de: <https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Entendiendo%20el%20Reglamento%20General%20de%20Protección%20de%20Datos%20.pdf>

Leiner, B. M., Cerf, V. G., Clark, D. D., Robert, L. E., Lynch, D. C.,

Postel, J., & Wolff, S. (1997). *Breve historia del internet. Internet Society.*

Recuperado de: <https://www.internetsociety.org/es/internet/history-internet/brief-history-internet/>

Forero, T. (2019) *Conoce la historia del Internet desde su nacimiento hasta lo que es hoy.* Recuperado de:

<https://rockcontent.com/es/blog/historia-del-internet/>

Jobmas. (2021). *Jobmas* Obtenido de <https://gt.jobomas.com>

Hernández, V. (2016). *La vulnerabilidad de nuestra información personal, ¿un mal incurable?* Obtenido de

<https://www.derechosdigitales.org/9794/la-vulnerabilidad-de-nuestra-informacion-personal-un-mal-incurable/>

López-Torres, J. (2014, November 25). *Antecedentes internacionales en materia de privacidad y protección de datos personales International backgr. International Background on Privacy and Personal Data Protection.* Recuperado de: <https://publicaciones.eafit.edu.co/index.php/ejil/article/download/2849/2626?inline=1>

Marben, A. (2019). *La importancia de la protección de datos.* Marben Abogados. <https://www.marbenabogados.com/la-importancia-de-la-proteccion-de-datos/>

Martínez, M. (2019) *Internet: así nació y así creció*. Recuperado de:
<https://blog.orange.es/red/historia-de-internet/>

OECD. (2013). *The economic value of data: discussion paper. Exploring the Economics of Personal Data*. https://www.oecd-ilibrary.org/science-and-technology/exploring-the-.....economics-of-personal-data_5k486qtxldmq-en

Olivares, R. (2011). *¿Qué es la transformación de datos? ASPECTOS LEGALES DE LA TRANSFORMACIÓN DIGITAL DE MI NEGOCIO*. Recuperado de: <https://latinalliance.co/wp-content/uploads/2020/08/Proteccion-de-Datos-Guatemala.pdf>

Rodríguez Lascano, F. S. (2016). *Servicio isp de banda ancha utilizando la red eléctrica para la EESA*. Obtenido de <https://dspace.uniandes.edu.ec/handle/123456789/5265?mode=full>

Salesforce, S. (2013). *Exploring the Economics of Personal Data. A Survey of Methodologies for Measuring Monetary Value*. https://www.oecd-ilibrary.org/science-and-.....technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en

Valencia, C. (2019). *¿Cuándo nació internet? Historia y evolución. Historia de Internet.* Recuperado de:
<https://www.mastermarketing-valencia.com/marketing-digital/blog/internet-.....historia-evolucion/>

Valladares, I. (2019). *Estudio Centroamericano de Protección de Datos. IPANDETEC, 1, 5.*https://www.ipandetec.org/wp-content/uploads/2019/01/EDP_Guatemala.pdf