

UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

CARRERA DE DERECHO

BIBLIOTECA



PROCESO DE DIGITALIZACIÓN DEL FONDO BIBLIOGRÁFICO DE LA BIBLIOTECA DE DERECHO

GESTION 2017

Nota importante para el usuario:

“Todo tipo de reproducción del presente documento siempre hacer mención de la fuente del autor y del repositorio digital para evitar cuestiones legales sobre el delito de plagio y/o piratería”.

La dirección de la Biblioteca



UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
CARRERA DE DERECHO
INSTITUTO DE INVESTIGACIONES Y SEMINARIOS



RESOLUCION CEUB 1126/2002

TESIS DE GRADO

**“MECANISMOS DE CONTROL JURISDICCIONAL DEL
ESTADO PLURINACIONAL BOLIVIANO PARA LA
PROTECCIÓN DE LOS DATOS DE LOS USUARIOS
BOLIVIANOS DE LAS REDES SOCIALES”**

TESIS PARA OPTAR AL GRADO DE LICENCIATURA EN DERECHO.

POSTULANTE : ALEJANDRO TOLIN ROJAS
TUTOR : Dr. EMERSON CALDERON GUZMAN

LA PAZ – BOLIVIA

2012

Dedicatoria

Dedicado a mis padres que siempre me impulsaron a seguir adelante y a luchar por hacer realidad mis sueños, a mis queridos abuelos que son los ejemplos más grandes de vida que he tenido, y a todas las personas que confiaron en mí.

Agradecimientos

Quiero agradecer a Dios por haberme dado conocimiento y paciencia para poder concluir este estudio.

Agradezco también a mis padres el **Lic. Florencio Tolin** la **Sra. Maruja Rojas**, a mí hermano **Lic. Williams Tolin** y a toda mi familia que con sus ejemplos ayudaron a mi formación desde muy niño.

A mi tutor el **Dr. Emerson Calderón Guzmán** por su colaboración indispensable en la culminación de la presente tesis.

A la cancillería y otros profesionales que ayudaron a esta investigación con sus opiniones y consejos permitirme cumplir con todas y cada una de mis necesidades para lograr una investigación fehaciente del presente trabajo de tesis de grado.

Otra de las personas las cuales tengo que agradecer profundamente por toda la colaboración proporcionada, la guía, y la formación para que este trabajo sea posible es al señor **Dr. Arturo Vargas**. Docente de nuestra querida Facultad de Derecho y Cs. Políticas.

Y a todas las personas que ayudaron a este estudio.

.

RESUMEN O ABSTRAC

Las redes sociales son servicios gratuitos que se ofrecen a los usuarios de internet, en estos los usuarios de los mismos colocan sus datos de manera voluntaria y a la vez son participes y generadores de contenidos en su página de perfil, sus datos son vulnerables a todo tipo de ataques ya sea realizado por terceros o sea por descuido propio, esto genera una serie de problemas y descontentos a los usuarios de las redes sociales.

Está claro que dentro de nuestro ordenamiento jurídico estatal no existen normas que puedan garantizar la seguridad de los datos de los usuarios bolivianos de las redes sociales, así como un mecanismo de control jurisdiccional que pueda encargarse de hacer cumplir estas normas, todo esto debido a la falta de orientación, desinterés de la sociedad, y a los adelantos tecnológicos que han creado en pocos años grandes avances en el mundo de la informática.

Es necesario adoptar conciencia social, profesional y sobre todo estatal para así poder poner a la prevención como principal mecanismo de protección para prevenir la comisión de los delitos informáticos de los cuales son víctimas los usuarios de las redes sociales,

MECANISMOS DE CONTROL JURISDICCIONAL DEL ESTADO PLURINACIONAL BOLIVIANO PARA LA PROTECCIÓN LOS DATOS DE LOS USURIOS BOLIVIANOS DE LAS REDES SOCIALES

ÍNDICE

DEDICATORIA	I
ADRADECIMIENTO.....	II
RESUMEN ABSTRAC	III
DISEÑO DE LA INVESTIGACIÓN	
Identificación del problema	1
Problematización.....	3
Delimitación del Tema de la Tesis	4
Delimitación Temática.....	4
Delimitación Temporal	4
Delimitación Espacial	4
Fundamentación e Importancia del Tema de la Tesis.....	5
Objetivos del Tema de la Tesis.....	5
Objetivo General	5
Objetivos Específicos.....	6
Marco Teórico	6
Hipótesis de Trabajo	6
Variables	6
Variable Independiente	6
Variable Dependiente.....	6
Métodos	7
Métodos Generales.....	7
Métodos Específicos.....	7

Técnicas a utilizar en la Tesis	7
Introducción.....	8
DESARROLLO DEL DISEÑO DE PRUEBA	
CAPÍTULO I MARCO HISTÓRICO	
Internet e historia del desarrollo de las redes sociales.....	10
CAPÍTULO II. MARCO TEÓRICO	
Teoría de las redes sociales, teoría de los seis grados y delincuencia informática.....	22
CAPÍTULO III. MARCO CONCEPTUAL	
Información conceptual sobre Derecho Internacional, Derecho Informático, Protección de datos y redes sociales.....	29
CAPÍTULO IV. MARCO JURÍDICO	
Legislación Nacional, Tratados Internacionales sobre la materia y Legislación Comparada	40
CAPITULO V. MARCO PRÁCTICO	
Vulnerabilidad de los datos de los usuarios de las redes sociales según la opinión de expertos en informática, redes sociales, Derecho Informático y Derecho Internacional Público	48
CONCLUSIONES	56
RECOMENDACIONES	58
BIBLIOGRAFIA	59
ANEXOS	60

DISEÑO DE INVESTIGACION DE LA TESIS DE GRADO

DISEÑO DE LA INVESTIGACIÓN DE LA TESIS DE GRADO

ENUNCIADO DEL TEMA DE LA TESIS.

MECANISMOS DE CONTROL JURISDICCIONAL DEL ESTADO PLURINACIONAL BOLIVIANO PARA LA PROTECCIÓN LOS DATOS DE LOS USURIOS BOLIVIANOS DE LAS REDES SOCIALES.

IDENTIFICACIÓN DEL PROBLEMA

Cuando varias computadoras están conectadas de forma en que puedan compartir datos se forman una red informática, cuando estas redes informáticas a través de internet se conectan a otras redes en todo el mundo, éstas pueden compartir toda clase de datos e información que llevan en su red informática. Del objetivo de crear una comunicación más sencilla entre amigos y familiares en todo el mundo, nacieron las redes sociales, destinadas enteramente a la socialización. Las redes sociales son una representación de los datos que los usuarios desean compartir con sus contactos, ya sea que estos esté destinado como una forma de comunicación, compartir fotos, intercambiar, crea o suprimir datos; todo eso se realiza al momento de utilizar una computadora conectada al servicio de internet.

Los usuarios de estas redes sociales pueden sufrir de diferentes tipos de riesgos al colocar sus datos pues estos pueden ser robados ya sea por descuido del usuario o por el ataque de los conocidos “hackers”; pueden llegar a ser extorsionados, ultrajados, difamados; también cabe señalar que cuando se pone algún dato y luego es suprimido o borrado, este mismo dato no desaparece de la red social en la que fue subido.

Al personalizar los datos que se muestran en una red social, el robo de los mismos no es el único peligro que se puede correr, Debido a que la red social no puede verificar de manera efectiva la identidad del usuario, éste puede crear un perfil falso con el cual puede llegar a cometer toda clase de difamaciones y ultrajes, también este usuario puede llegar a generar un movimiento de varias personas con las que pueden llegar a coincidir con su forma de pensar, llegando a expresar su descontento con algunas instituciones gubernamentales, personajes públicos, etc., jugando con la reputación de estos personajes, incluso suplantando sus identidades, creando varias revueltas impulsadas por las redes sociales.

Por ejemplo, los varios problemas generados en el Estado Federal de México, debido al uso de las redes sociales generaron que este Estado aplique como forma de control jurisdiccional uno de los fallos más importantes contra la red social denominada Facebook: “Recientemente **la justicia de la provincia de Mendoza** (Estado Federal de México) ordenó a la red social **Facebook**, el **cierre de paginas que alentaban a reteadas masivas en los colegios**, buscando que los adolescentes faltasen sin autoridad de los padres a las escuelas.

La decisión fue fundada en el **artículo 5 de la Ley 25240 de Defensa del Consumidor**, modificada por **la Ley 26361**, donde se **establece que las cosas y servicios deben ser suministrados o prestados de forma tal que no presenten peligro para la salud o integridad física de los consumidores y usuarios**. Se buscó de esta forma evitar posibles daños que podían darse con actitudes como la que fomentaban.

Se hace referencia también en dicho fallo a **la función que hoy cumplen las redes sociales**, permitiendo la libertad de expresión, derecho que no debe ejercerse en detrimento de la necesaria armonía con los demás derechos constitucionales, como ser la integridad moral y física de las personas...¹”.

¹ Problemática Legal de las Redes Sociales.2010.
file:///C:/Users/familia/Desktop/DERECHOINFORMATICO/Redes sociales problematicalegal.htm.

Otro ejemplo importante es el ocurrido en Argentina, país que protege de manera efectiva los datos de los usuarios de su país, en caso específico el de sus fotografías subidas a estos sitios. “La tutela jurídica del derecho a la propia imagen comenzó en ese país desde la sanción de la Ley de Propiedad Intelectual, específicamente el Art. 31 de la Ley 11.723 establece: *“El retrato fotográfico de una persona no puede ser puesto en el comercio sin el consentimiento expreso de la persona misma, y muerta ésta, de su cónyuge e hijos o descendientes directos de éstos, o en su defecto del padre o de la madre. Faltando el cónyuge, los hijos, el padre o la madre, o los descendientes directos de los hijos, la publicación es libre. La persona que haya dado su consentimiento puede revocarlo resarciendo daños y perjuicios. Es libre la publicación del retrato cuando se relacione con fines científicos, didácticos y en general culturales, o con hechos o acontecimientos de interés público o que se hubieran desarrollado en público.”* El derecho a la propia imagen atribuye al individuo la capacidad de ejercer un control sobre la captación, grabación, uso y difusión de su imagen entendida como representación gráfica de la figura humana, y también de su voz...”².

Actualmente, el Estado Plurinacional Boliviano carece de un mecanismo de control que pueda proteger los datos de los usuarios de las redes sociales, ya que el tema no es muy conocido por los juristas bolivianos, y genera un vacío jurídico que puede ser aprovechado por usuarios de las redes sociales con fines perjudiciales.

PROBLEMATIZACIÓN

- ¿Qué mecanismos de control jurisdiccional debe implementar el Estado Plurinacional de Bolivia para garantizar la privacidad de los datos de los usuarios bolivianos de las redes sociales?

² LOZA, Leandro. 2010. Aspectos Legales y Normativos de las Redes Sociales. file:///C:/Users/familia/Desktop/DERECHO INFORMATICO/Aspectos Legales y Normativos de las Redes Sociales _ Abogados Derecho Informático y Nuevas Tecnologías - Estudio Juridico.htm.

-¿Es posible que los datos de los usuarios bolivianos de las redes sociales sean usados de forma arbitraria e indiscriminada?

-¿Cual es la opinión de expertos en derecho informático y derecho internacional sobre la necesidad de contar con mecanismos de control jurisdiccional para garantizar la privacidad de los usuarios de las redes sociales?

-¿Qué mecanismos jurídicos existen en otros países para proteger la privacidad de los usuarios de las redes sociales?

DELIMITACIÓN

DELIMITACIÓN TEMÁTICA

El presente estudio se realiza en las ramas del Derecho Informático y Derecho Internacional Público.

DELIMITACIÓN TEMPORAL

Se realizará el estudio desde la aparición de las redes sociales al año 2012.

DELIMITACIÓN ESPACIAL

La ciudad de La Paz sede del Órgano Legislativo Plurinacional del Estado Boliviano.

FUNDAMENTACIÓN E IMPORTANCIA

El desarrollo del presente estudio pretende demostrar principalmente que los datos de los usuarios bolivianos se encuentran en peligro, debido a los adelantos

tecnológicos generados últimamente. Esta actividad, casi restringida en principio debido a que solo era accesible para unos cuantos, ahora se ha convertido en una actividad constante de los usuarios del servicio de internet, y como toda actividad del ser humano debe de ser normada.

Existe la latente necesidad que el Estado Plurinacional Boliviano proteja los datos de los usuarios bolivianos de las redes sociales, su Derecho a la Privacidad y precautelarse el Derecho a la Información de los ciudadanos bolivianos con un mecanismo efectivo que pueda resguardar estos bienes jurídicos, antes que estos delitos informáticos que se generan por el mal uso de los datos de los usuarios puedan convertirse en algo más peligroso.

El Estado Plurinacional Boliviano carece de normas específicas que puedan proteger los datos de los usuarios bolivianos de las redes sociales, debido a que este tema es discutido por los entendidos en la materia, pero no muy conocido por los usuarios bolivianos de las redes sociales; se genera no sólo un vacío en la normativa, si no un estado de desinformación de los usuarios bolivianos de las redes sociales quienes llegan a sufrir toda clase de injurias y difamaciones cuando sus datos son manipulados de mala manera, haciendo que este problema sea cada vez más constante en el ámbito nacional.

OBJETIVOS

OBJETIVO GENERAL

Establecer mecanismos de control jurisdiccional del Estado Plurinacional Boliviano para garantizar la seguridad de los datos de los usuarios bolivianos de las redes sociales.

OBJETIVOS ESPECÍFICOS

- Analizar la vulnerabilidad de los datos de los usuarios de las redes sociales.
- Conocer la opinión de expertos en Informática, redes sociales, Derecho Informático y Derecho Internacional Público.
- Realizar un estudio de Legislación Comparada.

HIPÓTESIS

Se deben establecer mecanismos de control jurisdiccional del Estado Plurinacional Boliviano para garantizar la seguridad de los datos de los usuarios bolivianos de las redes sociales.

VARIABLES

INDEPENDIENTE

Establecer mecanismos de control jurisdiccional del Estado Plurinacional Boliviano.

DEPENDIENTE

Garantizar la seguridad de los datos de los usuarios bolivianos de las redes sociales.

MÉTODOS

GENERALES

El método general será el Sintético Jurídico Empírico, cuyo objetivo es relacionar el derecho con problemas concretos de la sociedad. En este caso, se vinculará el derecho con la necesidad de incorporar mecanismos de control jurisdiccional que protejan los datos informáticos de los usuarios bolivianos de las redes sociales.

ESPECÍFICOS

El método específico será el Cuantitativo Descriptivo Empírico, el mismo que tiene por objeto el estudio del derecho en relación con problemas concretos de la realidad. Su objetivo es recoger información concreta, describirla y analizarla, sin realizar procesamientos estadísticos algunos.

TÉCNICAS

- ❖ Entrevista para expertos en Informática y Redes Sociales.
- ❖ Entrevista para expertos en Derecho informático.
- ❖ Entrevista para expertos en Derecho Internacional Público.
- ❖ Revisión Documental.

INTRODUCCION

El ser humano es un ser social, que necesita de otras personas para poder desenvolverse, actúa en sociedad desde siempre, la tecnología y su gran avance ha permitido que el internet llegue a formar parte de su vida cotidiana del ser humano, las redes sociales son un medio de comunicación masiva, que permite al individuo buscar o fortalecer nexos de amistad a través del internet, estas páginas permiten al usuario de las mismas una construcción y reconstrucción permanente de datos, gracias a la evolución del navegador Web 2.0 los contenidos son elaborados por el usuario, y estos contenidos tienen como único limite el que el usuario se proponga, permite al usuario tener una ubicación inmediata para las personas que desean buscarlo en la red social, y a la vez permite al usuario interactuar con sus contactos o aquellas personas que desea conocer.

Las redes sociales son útiles para compartir conocimientos, compartir contenidos que se encuentran en el perfil de usuario, participar y crear grupos de intereses comunes, mostrar ideologías aceptación o descontento hacia personajes públicos, para divertirse atreves de las varias aplicaciones que se tiene en la red social, realizar negocios, encontrar trabajo, ofrecer trabajo, etc.

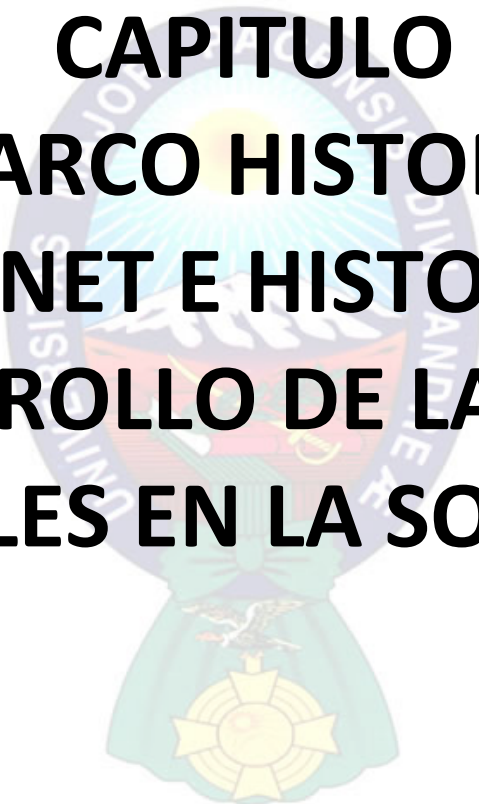
Este debe de ser considerado como un medio de comunicación masiva, como un teléfono, un buzón de correo, los usuarios de las redes sociales pueden ser víctimas de robo de datos de su perfil, que puede generar la creación de identidades falsas, montajes fotográficos, llegando a formar parte de contenidos no aptos para menores de edad, y otros delitos de carácter informático.

Existen varios países en el mundo que han visto el alcance masivo de las redes sociales y a través de sus normativas han tratado de regular esta actividad, mostrando a los usuarios de las redes sociales de sus países que sus datos están seguros de los ataques a los que pueden llegar a ser víctimas.

El presente estudio tiene como objetivo establecer mecanismos de control jurisdiccional para la protección de los datos de los usuarios de las redes sociales, analizar lo vulnerable que son estos datos, y conocer la opinión de expertos en el tema.



CAPITULO I
MARCO HISTORICO
INTERNET E HISTORIA DEL
DESARROLLO DE LAS REDES
SOCIALES EN LA SOCIEDAD.



MARCO HISTORICO

CAPÍTULO I

INTERNET E HISTORIA DEL DESARROLLO DE LAS REDES SOCIALES EN LA SOCIEDAD.

1.1. INTERNET

Internet y su rápida expansión en el mundo en el año 2011 mostro que ya existían alrededor de 2.100 millones de usuarios en el mundo, con un número que aumenta más y más.

Los diferentes servicios que presta Internet en principio solo consistía en el intercambio de información, y datos a diferentes lugares del mundo de manera casi inmediata, a lo largo de su existencia mostró la necesidad de los usuarios de una forma rápida y fácil de interacción social con sus amigos o familiares, en la actualidad al contratar el servicio de Internet, recibimos una dirección de correo-e, que consiste en la transmisión electrónica de cartas y mensajes a través del que otros usuarios de Internet en cualquier parte del mundo pueden escribirnos y enviarnos mensajes, documentos, fotos, gráficos, músicas o cualquier tipo de archivos. Permitiendo también que se pueda, escribir y enviando material a otros usuarios de la red en el mundo, también consta de servicios de chat y otras aplicaciones³, en principio este servicio fue útil a las necesidades de los usuarios, pero debido a esta necesidad constante y la personalización de los datos de los usuarios, es que diferentes sitios web ofrecieron, nuevos servicios personalizados destinados a la socialización masiva.

³ Servicios que ofrece internet, sipan.inictel.gob.pe/users/jcasachagua/ofrece.htm.

• ORÍGENES Y CARACTERÍSTICAS

En las últimas décadas, Internet se ha convertido en una herramienta indispensable para el uso del ser humano, debido a los adelantos tecnológicos de los últimos 50 años y las necesidades latentes de comunicación masiva. “Los orígenes de Internet se remontan a principios de la mitad del siglo XX, como un proyecto de investigación en redes de computación de paquetes, dentro de un ámbito militar. A finales de los años sesenta (1969), en plena guerra fría, el Departamento de Defensa Americano llegó a la conclusión de que su sistema de comunicaciones era demasiado vulnerable; estaba basado en la comunicación telefónica (Red Telefónica Conmutada, RTC), y por tanto, en una tecnología denominada de conmutación de circuitos. (Un circuito es una conexión entre llamante y llamado), que establece enlaces únicos y en número limitado entre importantes nodos o centrales, con el consiguiente riesgo de quedar aislado parte del país en caso de un ataque militar sobre esas arterias de comunicación.

Como alternativa, el citado Departamento de Defensa, a través de su Agencia de Proyectos de Investigación Avanzados (Advanced Research Projects Agency, ARPA), decidió estimular las redes de computadoras mediante becas y ayudas a departamentos de informática de numerosas universidades y algunas empresas privadas. Esta investigación condujo a una red experimental de cuatro nodos, que arrancó en Diciembre de 1969, se denominó ARPAnet. La idea central de esta red era conseguir que la información llegara a su destino aunque parte de la red estuviera destruida.”⁴ A lo largo de las décadas posteriores se unieron varias instituciones públicas y privadas a una red o malla cibernética, creando Internet como lo conocemos ahora, internet no es simplemente un red de computadoras conectadas entre sí, es una asociación de miles de redes conectadas entre sí por todo el mundo, teniendo como requisito necesario una computadora con un módem, conectado a un proveedor, que se encarga de proporcionar el acceso a la red.

⁴ Introducción al Internet,

- **SERVICIOS QUE OFRECE**

Los servicios ofrecidos a través de Internet son los siguientes: www (telaraña mundial “World Wide Web”) que son páginas con textos y gráficos. Telnet que son los accesos a sistemas remotos, FTP transferencias de ficheros entre ordenadores internet y su ordenador, Archie que es la búsqueda de ficheros FTP, E-MAIL más conocido como correo electrónico, estos como los más conocido y utilizados.

La amplia variedad de direcciones y dominios en el mundo de las redes cibernéticas permite a los usuarios individualizarse crear una dirección, identificar su nombre y su ubicación, esta dirección que puede constar de varias palabras separadas por puntos indica el nombre del sistema y de qué organización forma parte. Dominio es algunas veces uno de los siguientes: .com, normalmente una compañía u organización, .edu, que es una Institución educativa, .gob, una institución gubernamental, .net, Gateways u otros administradores de la red, u otros de nivel superior delimitando el área geográfica, .es, España, etc. ⁵

El correo electrónico permite a los usuarios transferir y recibir mensajes, “Como cualquier correo electrónico, E-MAIL es un correo que concede un buzón a cada usuario, definido como una dirección de correo Internet, desde el cual se envían y donde se reciben mensajes otros de otros usuarios de la red.”⁶

⁵ Internet, www.tiss.es, Pagina 2, Documentación elaborada por tecnologías de la Información San Sebastián

⁶Internet, www.tiss.es, Pagina 6, Documentación elaborada por tecnologías de la Información San Sebastián

1.1.1.WEB 2.0

- **DEFINICIÓN Y CARACTERÍSTICAS**

Navegador Web es aquello que nos permite navegar a través del servicio de internet. “Los navegadores son los que han dado el empuje que actualmente tiene Internet. Un navegador permite acceder a documentos hipermedia sin limitaciones, pudiendo ver las imágenes, escuchar los sonidos, o reproducir las películas que contiene mediante programas externos o internos al navegador. La forma de moverse por Internet con un navegador es muy sencilla e intuitiva, necesitando sólo un ratón y unos pocos conceptos.”⁷

Se presupone que estos navegadores Web en principio fueron evolucionando hasta la versión llamada Web. 1.0 que en principio fue de mucha ayuda para los cibernautas pero requería de muchas actualizaciones y su limitada capacidad de generar participación no satisfacía a los cibernautas pues solo ofrecía textos e imágenes estáticos, que pertenecían únicamente al administrador o autor del sitio Web que era dueño absoluto del software, A partir de la creación de Web 2.0 que es mucho más dinámico, el software y las actualizaciones son gratuitas permite el acceso a contenidos multimedia de manera rápida, generar contenidos en el sitio Web y brinda mayor participación del usuario⁸.

“**Web 1.0:** Fue el concepto original de Internet. Consistía en páginas estáticas escasamente actualizadas. Por lo general, eran páginas de empresas que informaban sobre sus actividades. Los usuarios recurrían a ellas para obtener datos y no participaban en el contenido.

⁷ Introducción a Internet, Pagina 38.

⁸ Formacion Web 2.0, <http://scopeo.usal.es/images/documentoscopeo/scopeo.001.pdf> .

Web 2.0: Permite que los usuarios puedan producir contenido propio, añadir, cambiar y borrar información de un sitio y crear el suyo propio de una manera sencilla. Las páginas web son más “personales”: La Web 2.0 permite a los usuarios interactuar entre ellos, como sucede en los blogs y las redes sociales”⁹.

“Las característica web 2.0 es el marcado carácter colaborativo. Sin trabajo en equipo, de autores y lectores, no hay red social que valga. Vemos ejemplos: un blog sin comentarios no es más que un texto plano, un wiki mantenido por una sola persona es un esfuerzo inútil. De esta manera, lo que realmente hay que destacar de la web es su vocación para ser plataforma lecto/escritura. En la web 1.0 existía un solo autor, que recibía el título de nobiliario digital de web máster, y que decía qué contenidos debíamos leer y en qué orden. En la web colaborativa la figura de autor queda relegada a la forma a veces desvaída del editor, que mantiene una línea, porque no impone una dirección única en los contenidos. Se puede decir que esta nueva etapa en las relaciones entre autor y lector se van haciendo más estrechas y para crear comunidades de interés que se organizan en forma horizontal; el creador de contenidos web pierde su posición jerárquica para convertirse en un participante más de la vida social digital.

De todo lo anterior se puede decir que la red 2.0 borra las fronteras entre el trabajo profesional y la creación amateur. En cierto modo es así pero en el nuevo web no todo tiene el mismo valor, en cierto modo existe la meritocracia que se rige por sus propias leyes. Como es lógico, el conocimiento profundo de la materia tratada es un valor fundamental para crear contenidos, pero también lo es la capacidad para transmitirlo y convertirlo en moneda de circulación social. Es decir, aquel autor que no sólo sepa de lo que está escribiendo, sino que además sea capaz de crear una comunidad a su alrededor y de repartir juego entre sus lecto/escritores será el que encabece la iniciativa.

⁹MORDUCHOWICZ, Roxana. MARCON, Atilio. SYVESTRE, Vanina. BALLESTRINI, Florencia. Los Adolescentes y las Redes Sociales, Pagina 10. 2010. Revista del Ministerio de Educación, República Argentina.

Es lo que se llama superusuario de la web. Y los individuos ya empiezan a tener un poder que en ocasiones se puede comparar con el de las figuras mediáticas, sobre todo, como es lógico, en los Estados Unidos. Es por eso que los blogs, se están utilizando desde hace tiempo para aprovechar su efecto red y lanzar campañas de opinión o de imagen”¹⁰.



¹⁰ HERRERA Jimenez, Francisco Jose, Web 2.0 y didácticas de lenguas, Pagina2, www.francisco@lajanda.org.

1.1.2. REDES SOCIALES DE INTERNET

- **DEFINICIÓN**

Las redes sociales son grandes grupos de personas de todo el mundo, conectadas a través del servicio de Internet. El ser humano es un ser social por naturaleza, la evolución de la tecnología y el uso frecuente del servicio de Internet permite que las redes sociales beneficien a los usuarios de las mismas, no sólo como una herramienta para poder interactuar con otras personas, sino que permite una construcción y reconstrucción de datos generados por el usuario teniendo como único límite el que uno mismo se proponga dentro de las redes sociales. “Las redes sociales son utilizadas por diferentes personas para diferentes fines, tales como las relaciones interpersonales, laborales, promoción política y otras”¹¹. Al momento el servicio de internet es accesible para cualquier persona, pues no tiene restricción de edad o género, y al ser tan accesible Internet, formar parte de una red social es sencillo, pues el requisito que piden la mayoría de las redes sociales es una dirección de correo electrónico y la aceptación de un contrato estándar.

“El primer antecedente se remonta a 1995, cuando un ex estudiante universitario de los Estados Unidos creó una red social en Internet, a la que llamó classmates.com (compañeros de clase.com), justamente para mantener el contacto con sus antiguos compañeros de estudio. Pero recién dos años más tarde, en 1997, cuando aparece SixDegrees.com (seis gra-dos.com) se genera en realidad el primer sitio de redes sociales, tal y como lo conocemos hoy, que permite crear perfiles de usuarios y listas de amigos”.¹²

¹¹ FLORES CUETO, Juan Jose, Las redes sociales jflores@usmpvirtual.edu.pe/

¹² MORDUCHOWICZ, Roxana. MARCON, Atilio. SYVESTRE, Vanina. BALLESTRINI, Florencia. Los Adolescentes y las Redes Sociales, Pagina 10. 2010. Revista del Ministerio de Educación, República Argentina.

“De 1997 a 2001, AsianAvenue, Blackplanet y MiGente permitían a los usuarios crear relaciones personales y profesionales, creando perfiles que permitían a los usuarios identificar amigos en sus redes sin pedir la aprobación de esas conexiones.

Desde entonces, diversas redes se han creado unas permanecen y otras han desaparecido. Según la zona geográfica el líder puede ir cambiando, pero a la fecha los principales competidores a nivel mundial son: Hi5, MySpace, Facebook, Twitter.

Se puede afirmar que el crecimiento de las redes sociales en Internet ha sido exponencial a partir de la etapa de la Web 2.0, donde el usuario de Internet dejó de ser un simple observador y consumidor de contenidos a un verdadero generador de los mismos”¹³.

Para poder formar parte de las redes sociales, pide como requisito la cuenta en un servidor de correo electrónico, la creación de un perfil en la red social y la aceptación que se presenta en un contrato estándar al cual muchas personas ven como un simple protocolo antes de poder acceder a los servicios de estos servidores, es así que nacen las redes sociales.¹⁴

“Las redes sociales permiten que los usuarios armen en ella su propia página Web (home pa-ge). En esta página, las personas pueden contar quiénes son, hablar de sus gustos e incluir la información que quieran compartir con su lista de amigos. El sitio personal en una red social funciona como una página web y por lo general, incluye información sobre su autor. Entre otros datos suelen figurar su nombre, email, la fecha de nacimiento, género, ciudad, y sus gustos: películas, libros, deportes. El sitio puede incluir –además - fotos, textos,

¹³LOZA, Leandro. 2010. Aspectos Legales y Normativos de las redes Sociales. file:///C:/Users/familia/Desktop/DERECHO INFORMATICO/Aspectos Legales y Normativos de las Redes Sociales _ Abogados Derecho Informático y Nuevas Tecnologías Estudio Juridico.htm

¹⁴ Problemática Legal de las Redes Sociales.2010.

file:///C:/Users/familia/Desktop/DERECHOINFORMATICO/Redes sociales problematicalegal.htm.

juegos, links, comentarios, vídeo clips y música. Una diferencia importante entre los sitios personales en las redes sociales y los blogs, es que en las redes sociales, las páginas web buscan sobre todo conocer gente y tener más amigos.”¹⁵

“Las Redes son formas de interacción social definidas como un intercambio dinámico entre personas, grupos e instituciones en contextos de complejidad. Consisten en un sistema abierto y en construcción permanente que involucra a conjuntos que se identifican en las mismas necesidades y problemáticas y que se organizan para potenciar sus recursos”¹⁶.

• CARACTERÍSTICAS

Estas redes sociales permiten al usuario de las mismas crear un perfil en el cual pueden poner los datos que deseen compartir con sus contactos; estos datos sirven para una mejor ubicación de la persona, que al momento de ser parte de una red social buscará a sus amigos o familiares, y estos a el usuario. Al colocar estos datos en la red social estos se personalizan y sirven exactamente para eso, ayudar a la búsqueda de otro usuario, y ayuda al fin principal de las redes sociales, la sociabilización. “Las redes sociales son plataformas de Internet que agrupan a personas que se relacionan entre sí y comparten información e intereses comunes. Éste es su principal objetivo: entablar contactos con gente ya sea para reencontrarse con antiguos vínculos o para generar nuevas amistades. Pertenecer en una red social, le permite al usuario construir un grupo de contactos, que puede exhibir como su lista de amigos. Estos amigos pueden ser amigos personales que él conoce,. A veces también, son contactos que se conocieron en Internet”¹⁷.

¹⁵ MORDUCHOWICZ, Roxana. MARCON, Atilio. SYVESTRE, Vanina. BALLESTRINI, Florencia. Los Adolescentes y las Redes Sociales, Pagina 10. 2010. Revista del Ministerio de Educación, República Argentina.

¹⁶ Definición de Red Social. <http://michfer.wordpress.com/2008/08/07/redes-sociales-definicion/>

¹⁷ MORDUCHOWICZ, Roxana. MARCON, Atilio. SYVESTRE, Vanina. BALLESTRINI, Florencia. Los Adolescentes y las Redes Sociales, Pagina 3. 2010. Revista del Ministerio de Educación, República Argentina.

En las redes sociales la publicación de información es importante para una mejor socialización, es por eso que esta información se presentan de manera textual, indicando el nombre completo si es que el usuario ve por conveniente compartir esta información, o bien puede identificarse con un apodo o sobrenombre por el cual es más conocido, su fecha y lugar de nacimiento, los lugares donde realizó sus estudios, el lugar donde actualmente trabaja, su ideología o pensamiento político y otros que no está obligado a colocar, pero a la vez estos permiten una mejor individualización de datos para poder ser buscado de una manera más fácil; puede colocar fotos en las cuales aparece o aparecen sus contactos, puede etiquetar esas fotos para individualizar algún acontecimiento que desea compartir con sus contactos u otras personas, puede restringir su información para sólo sus amigos o puede elegir que ésta esté abierta al público en general, llegando a ser una decisión muy personal al momento de la creación o después de la misma¹⁸.

Los datos colocados son actualizados constantemente, dependiendo del usuario que puede llegar a compartir diferentes datos desde que realizó un cambio de ciudad, su estado civil hasta su estado de ánimo, si éste ve conveniente ello. Los usuarios de las redes sociales pueden comentar los datos publicados en las redes sociales a fin de generar un nexo de sociabilidad con sus amigos y familiares.

Queda claro resaltar que al momento de subir un dato a una red social éste ya no pertenece a la persona que lo subió, pues las cláusulas del contrato estándar que uno está obligado a aceptar si se desea ser parte de la red social indican que estos mismos datos le pertenecen a la red social, así que si suprimen datos del perfil de usuario, estos no son eliminados de la red social y pueden llegar a ser utilizados en un futuro por la red social u otra persona de manera perjudicial. "El usuario al realizar el proceso de registro en cualquier sitio web que preste este tipo

¹⁸ MORDUCHOWICZ, Roxana. MARCON, Atilio. SYVESTRE, Vanina. BALLESTRINI, Florencia. Los Adolescentes y las Redes Sociales, Pagina 6. 2010. Revista del Ministerio de Educación, República Argentina.

de servicios, tales como Facebook, Hi5, Orkut, debe obligatoriamente aceptar y prestar conformidad a los términos y condiciones del sitio y políticas de privacidad impuestas unilateralmente. En este orden, la naturaleza jurídica del contrato que rige la relación, llamados comúnmente “Términos de Uso” (Terms of Service), “Términos y condiciones”, Políticas de Privacidad (Privacy Policy), es la de un contrato por adhesión”¹⁹.

Al formar parte de una red social y tener a alguien como contacto se puede visitar su perfil y ver los datos colocados en el mismo. Las redes sociales prestan otros servicios que son variados, dependiendo de la red social de la cual se forma parte; en su mayoría ofrecen servicios de chat, mensajería, juegos y otras aplicaciones que ayudan a una mejor exploración de la red social, si bien es cierto que todas estas aplicaciones están destinadas al entretenimiento de los usuarios pueden llegar ser adictivos y una razón diferente para visitar el perfil de la red social²⁰.

• TIPOS DE REDES SOCIALES

“Esta estructura social de relaciones entre usuarios puede ser de distinto tipo, como intercambios financieros, amistad, etc. También es el medio de interacción de distintas personas, como por ejemplo juegos en línea, chats, foros, spaces, etc.”²¹.

De entre las redes sociales más importantes en toda la red se pueden nombrar a las siguientes:

Facebook. Es la red más popular en el mundo, durante el 2011 superó los 600 millones de usuarios en todo el planeta. Es utilizada por jóvenes para armar redes

¹⁹ LOZA, Leandro. 2010. Aspectos Legales y Normativos de las Redes Sociales.

file:///C:/Users/familia/Desktop/DERECHO INFORMATICO/Aspectos Legales y Normativos de las Redes Sociales _ Abogados Derecho Informático y Nuevas Tecnologías - Estudio Jurídico.htm

²⁰MORDUCHOWICZ, Roxana. MARCON, Atilio. SYVESTRE, Vanina. BALLESTRINI, Florencia. Los Adolescentes y las Redes Sociales, Pagina 6. 2010. Revista del Ministerio de Educación, República Argentina.

²¹ Las Redes Sociales, www.delfingroup.es/blog/.

de contactos entre amigos y es utilizada por empresas para comunicarse con el público.

Twitter. Ésta es una red social de Microblogg.ing, el año 2010 fue una de las redes sociales de mayor crecimiento, posee más de 200 millones de usuarios.

MySpace. Otra plataforma basada en relaciones sociales, permite compartir perfiles de usuario, amigos, fotos, etc. En 2011 posee más de 34 millones de usuarios.

LinkedIn. Ésta es la red social para profesionales es más utilizada en el ámbito corporativo; permite a las personas tejer redes de contactos laborales, cargar sus curriculum vitae en la web y disponer de ellos en formato público, posee más de 100 millones de usuarios²².

- **RIESGOS Y PELIGROS**

En la última década estos servicios han ayudado bastante a varias personas a encontrar a sus amigos y familiares en el mundo; han sido utilizados para varios fines, como las relaciones interpersonales, laborales, intercambio de información de todos los tipos, incluso llegando a fomentar varios estudios de conocimiento científico, pero también han generado una serie riesgos como:

Malware: Acrónimo en ingles de las palabras Malicious y Software, es decir código malicioso, archivos dañinos que al infectar a la computadora realizan diferentes acciones, como el robo de información, el control de sistema o el robo de contraseñas. Los virus o troyanos son variantes más conocidas en este campo.

Phishing: Consiste en el robo de información personal o financiera del usuario, a través de la falsificación de un ente de confianza. Es frecuentemente realizado

²² Las Redes Sociales www.delfingroup.es/blog/

mediante el correo electrónico y sitios web duplicados, aunque puede realizarse por otros medios²³.

Estos riesgos se dan por el uso incorrecto de las redes sociales ya sea intencional o provocado por terceros, que al futuro pueden producir una serie de delitos de una índole mayor “En el uso diario de las redes sociales, los usuarios suben a la web diversos datos de índole personal que pueden ser útiles para los atacantes. El robo de información en las redes sociales se relaciona directamente con el robo de identidad, uno de los delitos informáticos que más ha crecido en los últimos años.

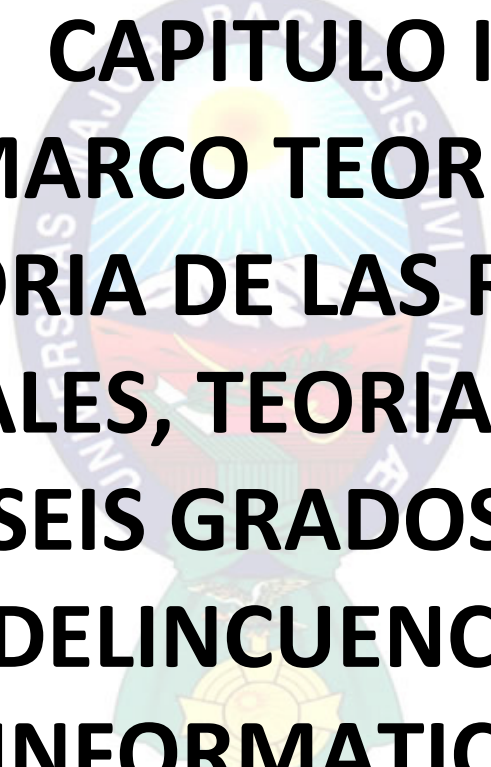
Los dos vectores de ataque más importantes para el robo de información son:

- **INGENIERÍA SOCIAL:** Se busca contacto directo con el usuario o víctima, extrayendo información a través de la comunicación, la “amistad” o cualquier comunicación que permita la red social.
- **INFORMACIÓN PÚBLICA:** una mala configuración de las redes sociales puede permitir que información de índole personal esté accesible más allá de lo que el usuario dejaría o le sería conveniente para su seguridad, por lo que las personas malintencionadas podrían acceder a dicha información²⁴.

Hechos pueden permitir difamaciones, injurias, mal uso de datos que genera malestar no solo a los usuarios de las redes sociales si no también a personajes públicos, son usurpados, obligando a los entendidos en la materia a buscar las formas de proteger a los usuarios y no usuarios de las redes social.

²³ Guia de seguridad en redes sociales, Pagina 5, 6, Internet Web Social Media Network Creativi Advertising Blog

²⁴ Guia de seguridad en redes sociales, Pagina 8, Internet Web Social Media Network Creativi Advertising Blog



**CAPITULO II
MARCO TEORICO
TEORIA DE LAS REDES
SOCIALES, TEORIA DE LOS
SEIS GRADOS Y
DELINCUENCIA
INFORMATICA.**

MARCO TEÓRICO

CAPITULO II

TEORIA DE LAS REDES SOCIALES, TEORIA DE LOS SEIS GRADOS Y DELINCUENCIA INFORMATICA.

2.1. LA TEORÍA DE LAS REDES SOCIALES

Las redes sociales se definen como un grupo de individuos delimitados, en grupos, organizaciones, comunidades, sociedades, que comparten unos con otros relaciones sociales, ya sea de parentesco, amistad, afinidad, pensamiento político, intercambio de bienes, dinero, información, etc., y al mismo tiempo sus subgrupos que tienen relación con los miembros de la red social.

“La teoría de las redes sociales es una rama de la Microeconomía que busca predecir el resultado del comportamiento agregado de un grupo de personas definido por las relaciones entre sus miembros. Su aplicación práctica es lo que llamamos análisis de redes sociales”²⁵

Esta teoría se origino en el año 1934 por J. Scott, pero el sociólogo Moreno en el año 1934 con su concepto de sociometría es considerado como fundador de esta teoría “Moreno se intereso por la estructura de los grupos de amigos aunque fuera por razones terapéuticas”²⁶, esta teoría tiene una gran influencia en teorías sociológicas como la de Durkeim en su teoría del contrato social y teorías matemáticas como la de los grafos de Cartawright y Zander, y de esta forma evoluciona por conceptos, toma como objeto el estudio del individuo y sus relaciones sociales, el análisis de las relaciones los brinda datos que son utilizados para interpretar los comportamientos sociales de las personas que

²⁵ Teoría de las redes sociales, lainsindias.net/indianopedia/Teoria_de_redes_sociales .

²⁶ LOZARES, Carlos. Teoria de redes sociales, Pagina 104,

forman parte de estas redes²⁷, esta teoría a lo largo de su evolución muestra una idea central “reside en el supuesto de que la gente siente, piensa y hace tiene su origen y se manifiesta en las pautas de las relaciones situación a la que se dan entre actores oponiéndose así a la idea de que los atributos o las características de los actores individuales están a la base o son causas de las pautas de comportamiento y, por tanto, de la estructura social. La raza, la edad, el sexo, la categoría social importan mucho menos en la teoría de las redes que las formas de relación, mantenerlas o mantenerlas. Son las relaciones, los vínculos que mantienen los actores, los que establecen las estructuras en cuyas posiciones se sitúan las unidades. Por consiguiente, la explicación de los comportamientos requiere un análisis de cómo los actores están conectados unos con otros en las diversas situaciones en las que son observados.

El análisis de redes no es más que un conjunto conceptual y sus métodos descriptivos, estructurales y productivos para conseguirlo.”²⁸ Este análisis se basa en la idea de que las relaciones entre personas son más importantes que sus características individuales.

2.2. LA TEORÍA DE LOS SEIS GRADOS

Esta teoría explica según el Psicólogo Stanley Milgram en el año 1967 aseguraba que el “mundo es un pañuelo” pues en un experimento que realizó demostró su teoría “consistió en la selección al azar de varias personas del medio oeste estadounidense para que enviara tarjetas postales a un extraño situado en Massachusetts, situado a varios miles de millas de distancia. Los remitentes conocían el nombre del destinatario, su ocupación y la localización aproximada. Se les indicó que enviaran el paquete a una persona que ellas conocieran directamente y que pensarán que tendría más probabilidades de conocer directamente el destinatario. Esta persona tendría que

²⁷ LOZARES, Carlos. Teoría de redes sociales, Página 104, 105, 106, 107.

²⁸ LOZARES, Carlos. Teoría de redes sociales, Página 110.

hacer lo mismo y así sucesivamente hasta que el paquete fuera entregado a su destinatario final.

Aunque los participantes esperaban que la cadena incluyera al menos cientos de intermediarios, la entrega de cada paquete solamente llevo como promedio entre cinco a siete intermediarios. “²⁹de allí es que nace la teoría de los seis grados que explica que si una persona conoce a cien personas y cada una de estas personas conociera a otras cien distintas en dos grados podría llegar a tener 10.000 personas y en seis grados a 9000 millones que es más que la población actual en el mundo.³⁰

De estas teorías es que las redes sociales de internet, basan su popularidad en los últimos años “Las redes sociales computacionales están permitiendo a las personas crear nuevas dinámicas de comunicación más potentes que las anteriores. Diferentes estudios han descubierto que estas redes de software permiten a las personas tanto fortalecer sus redes sociales actuales como formar nuevas redes de manera efectiva. Hoy en día podemos analizar prácticamente cualquier servicio o sistema de Internet en términos de redes sociales. Todas estas redes tecnológicas serían inútiles si no se nutrieran de la comunicación entre las personas; incluso hay quienes han expresado esto en términos matemáticos. Bob Metcalfe, uno de los inventores de Ethernet, determinó, en relación con las redes de telecomunicaciones, que la utilidad de la red crece en relación al cuadrado de la cantidad de usuarios conectados (Ley de Metcalfe). Posteriormente, David Reed descubrió que esta fórmula quedaba corta para describir Internet, ya que además de permitir comunicaciones persona a persona permite la creación de grupos. La ley de Reed postula que la utilidad de una red, en particular las redes sociales, crece en forma exponencial a la cantidad de personas que la integran.”³¹

²⁹ Redes Sociales, pensamiento sistematico, es.wikipedia.org/wiki/Red_social.

³⁰ Teoría de las redes sociales, lainsindias.net/indianopedia/Teoria_de_redes_sociales .

³¹ Redes Sociales, pagina 116.

2.3. TEORÍA DEL DELITO INFORMÁTICO

Existen diferentes términos para definir este tipo de delitos entre los que podemos destacar:

2.3.1.DELINCUENCIA INFORMÁTICA

Es definido como conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos. “Los delincuentes informáticos con frecuencia usan Ingeniería Social (disciplina que ataca el factor más vulnerable de un sistema informático y para el cual no hay solución tecnológica LAS PERSONAS) En esencia la Ingeniería Social se basa en engañar a las personas, le hacen creer a los usuarios que su Banco le está solicitando su clave de acceso a sus cuentas y cuando las personas la entregan hacen transferencias de sus cuentas (Robo) .”³²

2.3.2.CRIMINALIDAD INFORMÁTICA

Se define la criminalidad informática como la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (en éste caso lo informático es finalidad).

³² Delincuencia Informática, www.scribd.com/doc/16302561/DELINCUENCIA-INFORMATICA.

Tiedemann considera que con la expresión criminalidad mediante computadoras, se alude a todos los actos, antijurídicos según la ley penal vigente realizados con el empleo de un equipo automático de procesamiento de datos.

Romeo Casabona se refiere a la definición propuesta por el Departamento de Justicia Norteamericana, según la cual Delito Informático es cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución.

Para Davara Rodríguez no parece adecuado hablar de delito informático ya que, como tal, no existe, si atendemos a la necesidad de una tipificación en la legislación penal para que pueda existir un delito. Si bien admite la expresión por conveniencia, para referirse a determinadas acciones y omisiones dolosas o imprudentes, penadas por la Ley, en las que ha tenido algún tipo de relación en su comisión, directa o indirecta, un bien o servicio informático. Define el Delito informático como, la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.

Determinados enfoques doctrinales subrayarán que el delito informático, más que una forma específica de delito, supone una pluralidad de modalidades delictivas vinculadas, de algún modo con los ordenadores.

2.3.3. COMPUTER CRIMEN

En el ámbito anglosajón se ha popularizado la denominación de "Computer Crime" y en el germano la expresión "Computerkriminalität"

2.3.4. DELINCUENCIA DE CUELLO BLANCO

La doctrina, casi unánimemente, la considera inscribible en la criminalidad "de cuello blanco", para Sutherland la delincuencia de cuello blanco es la violación de la ley penal por una persona de alto nivel socio-económico en el desarrollo de su actividad profesional. "Al llamado delito "de cuello blanco" se lo ha etiquetado también como delito "económico" o "financiero, o delito institucionalizado", etc. y consecuentemente se admiten las variantes de delincuencia "de cuello blanco", "económica" o "financiera", o delincuencia "institucionalizada".

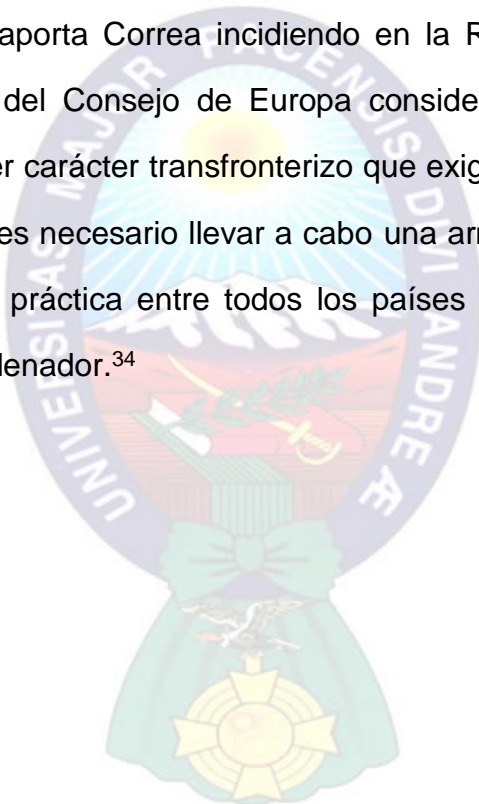
A no dudarlo la sociedad actual se encuentra librando una gran batalla contra la criminalidad, que para mí es más que un desafío. La solución en esta dura confrontación es más compleja que buscar un incremento en el monto de las penas, porque si fuere la gran cura social, aquellos países en los que está implantada la pena de muerte no tendrían delitos, delincuentes, ni delincuencia. Ya FERRI habló sobre las leyes del desarrollo de la criminalidad que pasaba desde las formas violentas o musculares a las intelectuales o astutas del robo a la estafa que viene a ser un fenómeno no ya agudo, sino crónico.”³³

³³ ZAMBRANO Pasquel, Alfonso, **Delincuencia de cuello blanco**, www.alfonsozambrano.com/doctrina.../delitocuelloblanco_azp.pdf

2.3.5. ABUSO INFORMÁTICO

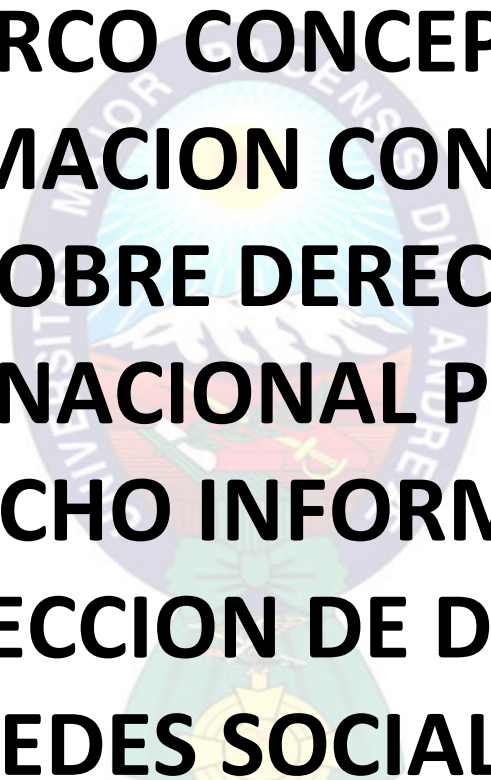
Ruiz Vadillo recoge la definición que adopta el mercado de la OCDE en la Recomendación número R (81) 12 del Consejo de Europa indicando que abuso informático es todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos.

La misma definición aporta Correa incidiendo en la Recomendación (89) 9, del Comité de Ministros del Consejo de Europa considerando que la delincuencia informática suele tener carácter transfronterizo que exige una respuesta adecuada y rápida y, por tanto, es necesario llevar a cabo una armonización más intensa de la legislación y de la práctica entre todos los países respecto a la delincuencia relacionada con el ordenador.³⁴



³⁴ CUERVO, José. Delitos Informaticos- Teoria, <http://mansiondelainformacion.blogspot.com/2007/08/delitos-informaticos.html>.

CAPITULO III
MARCO CONCEPTUAL
INFORMACION CONCEPTUAL
SOBRE DERECHO
INTERNACIONAL PÚBLICO,
DERECHO INFORMATICO
PROTECCION DE DATOS, Y
REDES SOCIALES.



MARCO CONCEPTUAL

CAPITULO III

INFORMACION CONCEPTUAL SOBRE DERECHO INTERNACIONAL PÚBLICO, DERECHO INFORMATICO PROTECCION DE DATOS, Y REDES SOCIALES.

3.1. DERECHO INTERNACIONAL PÚBLICO

3.1.1. TRATADOS Y CONVENIOS INTERNACIONALES

El Derecho Internacional Público es la rama del Derecho que se encarga de estudiar las relaciones entre Estados, y la relación de los Estados con los Organismos Internacionales. “De un modo general, el DIP (Derecho Internacional Público) es el conjunto sistematizado de normas jurídicas que regula las relaciones tanto de Estados como de los organismos u organizaciones bilaterales o multilaterales. Varios autores opinan que, en este sentido, los Estados son las personas de Derecho Internacional, esa opinión pudo ser aceptada antes de la aparición de los organismos internacionales, que han sido ya incorporados al campo del Derecho Internacional Público”³⁵.

“Los Organismos Internacionales son sujetos indiscutibles; tienen características propias que los singularizan de los otros sujetos: son creados por medio de un tratado internacional; pueden participar en la creación de una nueva organización internacional. Una vez creada se diferencia de los demás Estados que le dieron origen, esto es, tiene voluntad propia, independiente; su ámbito de competencia no es territorial sino funcional, su competencia se refiere a ciertas materias (económicas, culturales, políticas, etcétera) poseen un derecho interno propio,

³⁵TREDINICK, Felipe. 1997. Derecho Internacional Público y Relaciones Internacionales, Página 2. Editorial “Los Amigos del Libro”, La Paz- Cochabamba.

regula el funcionamiento de sus órganos internos y su personal; en su actividad exterior están regulados por el derecho internacional”³⁶ .

La fuente más importante del Derecho Internacional Público son los tratados y convenios internacionales. “A través de la negociación diplomática realizada por los Estados en reuniones o asambleas multilaterales o bilaterales cuyo resultado es generalmente la conclusión de tratados, el Derecho Internacional se enriquece y nace cuando las disposiciones allí contenidas sean realmente nuevas.

Por consiguiente, el tratado, para que sea fuente del Derecho, necesita que en él se encuentren disposiciones realmente nuevas, por aquel instrumento internacional que se limite a repetir normas o principios ya consagrados no puede considerarse como tal”³⁷.

El Dr. Felipe Tredinnick indica que los Estados asumen compromisos entre sí por medio de estos “acuerdos de voluntades, de carácter expreso que solo obligan jurídicamente a las partes contratantes”, estas obligaciones son cumplidas por los Estados que son los sujetos por excelencia del Derecho Internacional³⁸.

“Los tratados que crean derechos son, por lo general, los acuerdos multilaterales que tienen por objeto el ordenamiento fundamental de ámbitos en particular de la vida común entre los Estados (por ejemplo, los tratados sobre derechos humanos sobre el orden comercial mundial). Los acuerdos contractuales se limitan por el contrario, a la reglamentación de obligaciones bilaterales, como los que caracterizan los acuerdos de derecho privado. La clasificación de un tratado en uno de estos dos tipos puede ser significativa para la interpretación.”³⁹

³⁶ BECERRA Ramirez, Manuel.1991. Derecho Internacional, Página 21. Editorial Impresos Chavez S.A. de C.V. Primera Edición Ciudad de México D.F.

³⁷ GUERRA, Inñiguez, Ramiro. 1963. Derecho Internacional Público, Pagina 36. Editorial Talleres Profesionales Salecianos.

³⁸ TREDINICK, Felipe. 1997. Derecho Internacional Público y Relaciones Internacionales, Página 13. Editorial “Los Amigos del Libro”, La Paz- Cochabamba.

³⁹ HERDEGEN, Mathias. 2005. Derecho Internacional Público, Pagina 118. Editorial Circuito de Maestría Marco de la Cueva. Primera Edición Ciudad de México D.F.

Los tratados internacionales son clasificados principalmente:

- **Por el número de partes:** Se clasifican en tratados bilaterales y multilaterales.
- **Por el procedimiento de celebración:** Se clasifican en tratados formales y tratados en forma simple o sin formalidades. Puede hablarse de una tercera categoría, la de tratados mixtos, cuando para una de las partes el procedimiento es formal y para la otra sin formalidades.
- **Por el contenido de las normas:** Se clasifican en tratados-ley y tratados-contrato. A esta división hace referencia el inciso a) del párrafo 1° del artículo 38 del Estatuto de la Corte Internacional de Justicia cuando habla de convenciones internacionales generales o particulares. Los tratados-ley contienen normas abstractas; los tratados-contrato se refieren a una obligación concreta.
- **Por las características de las partes:** se dividen en tres clases:
 - Los tratados entre Estados.
 - Los tratados entre Estados y organizaciones internacionales (gubernamentales).
 - Los tratados entre organizaciones internacionales.
- **Por la posibilidad de ampliar el número de partes:** se clasifican en tratados cerrados o abiertos; los primeros son aquellos en los que los

Estados contratantes originarios no admiten que otros Estados lleguen a ser partes en él, y los segundos son aquellos en que sí lo admiten. ⁴⁰

Según el citado Dr. Felipe Tredinnick, un convenio internacional se denomina como: “palabra generalmente utilizada en la práctica internacional para regular asuntos de transporte de todo tipo o asuntos culturales de dos o más países”⁴¹.

3.2. DERECHO INFORMÁTICO

3.2.1. DEFINICIÓN

El Derecho Informático es la rama del Derecho que tiene como objeto de estudio los fenómenos que genera el ser humano a través del uso de la informática.

José Alfredo Arce Jofre afirma que el Derecho Informático se constituye en el conjunto de normas, aplicaciones, procesos, relaciones jurídicas que surgen como consecuencia de la aplicación y desarrollo de la informática. Es decir que la informática en general, desde ese punto de vista, es objeto regulado por el derecho⁴².

Como lo explica Jorge Téllez, en su libro de Derecho Informático, “la informática es uno de los fenómenos más significativos de los últimos tiempos, llega su incontenible uso en todas las aéreas del conocimiento humano (ciencias del ser y del deber ser), dentro de las cuales el Derecho no puede ser la excepción dando lugar a una nueva disciplina como el Derecho Informático.

Aunque es muy difícil de confeccionar por el variado número de peculiaridades y muy a pesar de los puntos de vista que pudiera provocar, se puede decir que el

⁴⁰ HERNANDEZ, Joel. Tratados y Derecho Informático, Pagina 3.

⁴¹ TREDINICK, Felipe. 1997. Derecho Internacional Público y Relaciones Internacionales, Página 16. Editorial “Los Amigos del Libro”, La Paz- Cochabamba Bolivia.

⁴² ARCE, Jofre, José Alfredo. 2005. Informática y Derecho. Pagina 28. Editorial- Bolivia dos mil, La Paz- Bolivia.

derecho informático es la rama de las ciencias jurídicas que contempla a la informática como conocimiento (informática jurídica) y como objeto de estudio (derecho a la información)”⁴³.

3.3. INFORMÁTICA JURÍDICA, DERECHO A LA INFORMACIÓN Y LIBERTAD DE EXPRESIÓN

La informática jurídica hace referencia al hecho de poder acceder a archivos documentales referentes a derecho de una manera rápida y eficaz sin generar distorsión y generando un apoyo importante a las personas relacionadas con este campo.

“La Informática jurídica estudia la utilización de aparatos o elementos físicos, electrónicos, como la computadora, en el derecho; es decir, la ayuda que este uso presta al desarrollo y aplicación del derecho. En otras palabras, es ver el aspecto instrumental dado a raíz de la informática en el derecho”⁴⁴.

“Desde hace años la informática jurídica ha permitido un mejor uso de los fenómenos jurídicos, por lo que muchos juristas, anteriormente escépticos y indiferentes, han encontrado en la computadora un instrumento eficaz para el mejor desarrollo de sus actividades.

De esta forma merced a la información en el campo del derecho, se han constituido diferentes tipos de archivo (legislativo, de jurisprudencia, doctrinales , bibliográficos, etcétera), los cuales representan un potencial informático insospechado, además de que constituyen un apoyo rápido y eficaz en la realización de actividades de gestión, así como ayuda en la toma de decisiones, y

⁴³ TELLÉZ, Jorge. Derecho Informático, Página 13. Editorial, Impresos Chávez S.A. de C.V. Primera Edición Ciudad de México D. F.

⁴⁴ ARCE, Jofre, José Alfredo. 2005. Informática y Derecho. Pagina 34. Editorial- Bolivia dos mil, La Paz- Bolivia.

en la educación e investigación, por mencionar solo unos campos, lo cual representa un hecho sin precedente dentro del ámbito jurídico”⁴⁵.

El derecho a la información es una cualidad del ser humano para poder acceder a todo tipo de información generando una corriente a través de el mismo participando como informados y receptor “El concepto de Derecho a la información comprende un conjunto de tres facultades vinculadas entre sí como lo son: difundir, investigar y recibir información; todas ellas, agrupadas en dos vertientes importantes como son el derecho a informar y ser informado”⁴⁶.

El derecho a la información y libertad de expresión son elementos esenciales de los estados democráticos. Según José Alfredo Arce Jofré, la libertad de expresión a través de internet debe entenderse como la posibilidad que tienen los usuarios de comunicarse entre sí, así como la de hacer circular y tener acceso a información e ideas difundidas por otros usuarios⁴⁷.

3.4. PROTECCIÓN DE DATOS

Para poder definir qué es protección de datos para el derecho informático que es dato. “El Ser humano, para representar lo que le interesa transmitir en un mensaje, utiliza un código común preestablecido entre el emisor y receptor del mismo. Generalmente, el código mas usualmente utilizado es la palabra, tanto en forma escrita como oral. El dato es una representación de la realidad expresada en términos que forman parte de un código preestablecido de manera que pueda ser interpretada, y que sea destinado a dar información a un receptor (de allí el origen de la palabra “datum”, que en latin significa “dato”, participio del verbo “dar”). Podemos clasificar los datos en base a las siguientes situaciones concretas.

⁴⁵ TELLÉZ, Julio.1987. Derecho Informático, Página 15.Editorial, Impresos Chávez S.A. de C.V. Primera Edición Ciudad de México D. F.

⁴⁶ TELLÉZ, Jorge. Derecho Informático, Página 47. Editorial, Impresos Chávez S.A. de C.V. Primera Edición Ciudad de México D. F.

⁴⁷ ARCE, Jofre, José Alfredo. 2005. Informática y Derecho. Pagina 22. Editorial- Bolivia dos mil, La Paz- Bolivia.

- **DATOS PÚBLICOS:** Aquellos que tienen menor importancia y que son de fácil obtención, es decir que se encuentran casi a disposición de todos. Por ejemplo: nombre, domicilio, número de teléfono, número de documentos de identidad, número de registro único de contribuyentes, etc.

- **DATOS PRIVADOS O RESERVADOS:** Aquellos que constituyen lo que se ha dado en denominar “información sensible”. Esto es lo que se refiere a cuestiones íntimas del individuo: raciales, religiosas, costumbres sexuales, opiniones, estado de salud, etc., y cuyo conocimiento puede provocar discriminación al titular de los datos son los que requieren por ello mayor protección⁴⁸.

Debido a que la relación del ser humano con la informática, la protección de los datos que se utilizan en las computadoras y sus diferentes fines de los mismos son el objeto de estudio para esta rama del derecho. “Como se ha dejado asentado, la informática no es un fenómeno exclusivamente tecnológico con implicaciones exclusivamente positivas. Las computadoras, al permitir un manejo rápido y eficaz de grandes volúmenes de información, facilitan la concentración de datos referidos a las personas, constituyendo así, un verdadero factor de poder⁴⁹.”

Los datos de los usuarios de medios magnéticos, computadoras y otros llegan a ser utilizados de varias formas permitidas por los dueños de estos datos, así también pueden ser utilizados de mala manera por terceros. Entonces, se entiende según el Miguel Ángel Davara Rodríguez, “la protección de datos personales entre los que deben encuadrar aquellos que, unidos al individuo, se pueden considerar como características que definen a la persona y a su entorno- y que se encuentra reconocida, en las modernas legislaciones, mediante el derecho a la intimidad.

⁴⁸ ARCE, Jofre, José Alfredo. 2005. Informática y Derecho. Pagina 45. Editorial- Bolivia dos mil, La Paz- Bolivia.

⁴⁹ TELLÉZ, Jorge. Derecho Informático, Página 50. Editorial, Impresos Chávez S.A. de C.V. Primera Edición Ciudad de México D. F.

Es al surgir la informática y su simbiosis a las comunicaciones llamada telemática-, cuando aparece la nueva relación entre datos y personas, que necesita ser protegida más allá de las normas referentes a la intimidad.

Entonces se entiende por protección de datos “el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada de sus datos personales susceptibles de tratamiento autorizado, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorna personal, social o profesional, en los límites de su intimidad.

Esta protección de datos se centra, desde el punto de vista normativo en el ordenamiento jurídico en una norma básica”⁵⁰.

Los datos de los usuarios de medios electrónicos así como los de usuarios de los medios de comunicación como el internet, es encuentran a merced de varios ataques no solo a la intimidad y la privacidad, si no también generan toda clase de difamación e injuria, “la protección se realiza sobre el dato, para que éste no pueda ser tratado o elaborado, y convertido en información, nada más que para aquellos fines y para aquellas personas autorizadas para ello. Esta necesaria protección es un límite a la utilización de la informática ante el temor de que se pueda agredir la intimidad de los ciudadanos, personal o familiarmente, y que pueda coartar el ejercicio de sus derechos”⁵¹.

3.5. REDES SOCIALES

“Son comunidades virtuales en las que los usuarios arman un sitio personalizado, definen su perfil, para entrar en contacto con amigos que conocen o con amigos de sus amigos, con quienes tienen intereses particulares”⁵².

⁵⁰ DAVARA Rodríguez, Miguel Ángel. 2008. Guía Práctica de Protección de Datos para Abogados, Pagina 21. Editorial Da Fa Ma. Primera Edición, Madrid España.

⁵¹ DAVARA Rodríguez, Miguel Ángel. 2008. Guía Práctica de Protección de Datos para Abogados, Pagina 22. Editorial Da Fa Ma. Primera Edición, Madrid España.

⁵² MORDUCHOWICZ, Roxana. MARCON, Atilio. SYVESTRE, Vanina. BALLESTRINI, Florencia. Los Adolescentes y las Redes Sociales, Pagina 10. Septiembre 2010. Revista del Ministerio de Educación, República Argentina.

Grupos de personas unidas por varias redes informáticas conectadas al servicio de Internet, ingresan a la página web o servidor que ofrece este servicio, pueden contactarse con sus familiares o amigos que desea encontrar, puede utilizar los servicios de chat, administración de sus contactos, mensajería, subir fotos, escribir comentarios, etc.

Además de formar parte de la red social se someten a lo indicado en el contrato estándar que la misma red social obliga a aceptar, para ser parte de la misma, este contrato autoriza a la red social a poder utilizar los datos que se suben a la red social, aun si el usuario no está de acuerdo.

3.6. CONTROL JURISDICCIONAL

El control jurisdiccional deviene del poder judicial “El Estado en la actualidad asume para sí el monopolio de la fuerza a través del ejercicio de diferentes funciones: mediante la función legislativa, sanciona normas jurídicas para que los particulares y el mismo Estado se sometan en su actuación; luego, por medio de la actividad administrativa se realizan los actos necesarios para cumplir los servicios públicos. Por último, por medio de la función jurisdiccional, se dirimen conflictos a través del Poder Judicial”⁵³.

Debemos establecer que el control judicial es aquel que es llevado por los tribunales judiciales y los tribunales ordinarios, este control se da exactamente al momento en que la máxima autoridad de un tribunal judicial, el juez, para poder dirimir un conflicto que se le es presentado debida y formalmente emite un fallo conocido como sentencia, la sentencia tiene carácter de cosa juzgada, es decir

⁵³VILLAROEL Ferrer, Jaime Carlos.2007. Derecho Procesal Orgánico y Ley de Organización Judicial, Pagina 56. Editorial “El Original- San José”. Cuarta Edición Ciudad de El Alto, La Paz Bolivia.

que ésta no se puede apelar, este tipo de control es encomendado al órgano judicial del Estado.

“La jurisdicción como función es la actividad pública realizada por los órganos competentes nacionales o internacionales, con las formas requeridas por la ley, en virtud de la cual por acto de juicio, se aplica el orden jurídico establecido, para dirimir conflictos mediante decisiones susceptibles de adquirir autoridad de cosa juzgada eventualmente factibles de ejecución”⁵⁴. El control jurisdiccional es una función del poder judicial que hace una gran diferenciación por razón de materia, cuantía y territorio la Jurisdicción de carácter civil que es aquella en la cual los intereses de los particulares se encuentran en conflicto, la jurisdicción penal encargada de sancionar los delitos de orden público buscando una sanción para los infractores, la jurisdicción laboral encargada de los asuntos laborales juzgando los conflictos que puedan presentarse como consecuencia de las relaciones laborales de los trabajadores, cuidando de manera igualitaria tanto al empleador como para el trabajador sus derechos y obligaciones, y la jurisdicción administrativa que puede presentarse de manera pública como órganos del Estado y su forma de expresión, los actos administrativos, esta jurisdicción se encarga de juzgar los actos administrativos⁵⁵. “La función de dirimir conflictos y decidir controversias se ha convertido en uno de los fines primarios del Estado. No es posible concebir al Estado sin esa actividad... El Estado por medio de la jurisdicción declara el derecho ante cualquier violación al régimen normativo”⁵⁶.

⁵⁴VILLAROEL Ferrer, Jaime Carlos.2007. Derecho Procesal Orgánico y Ley de Organización Judicial, Pagina 58. Editorial “El Original- San José”. Cuarta Edición Ciudad de El Alto, La Paz Bolivia.

⁵⁵JINESTA Ernesto.1997. Control Jurisdiccional de la Administración Pública. <http://www.ernestojinesta.com/ernestojinesta/curriculuartrev/control.PDF>. Revista Judicial Costa Rica Año XX, N°63.

⁵⁶ VILLAROEL Ferrer, Jaime Carlos.2007. Derecho Procesal Orgánico y Ley de Organización Judicial, Pagina 56. Editorial “El Original- San José”. Cuarta Edición Ciudad de El Alto, La Paz Bolivia.

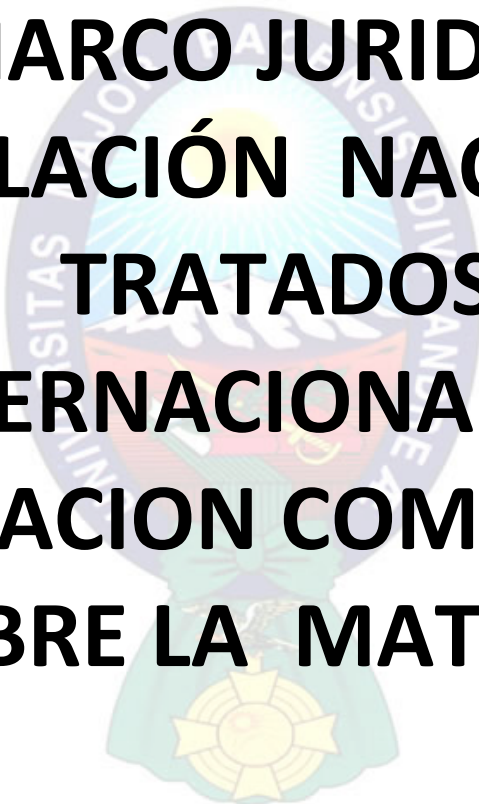
3.7. DATOS EN LAS REDES SOCIALES

Desde el punto de vista informático el dato es el antecedente para el conocimiento de una cosa. “Para la informática, los datos son expresiones generales que describen características de las entidades sobre las que operan los algoritmos. Estas expresiones deben presentarse de una cierta manera para que puedan ser tratadas por una computadora. En este casos, los datos por sí solos tampoco constituyen información, sino que ésta surge del adecuado procesamiento de los datos”⁵⁷. También definido como el elemento básico para producir información, tomando esta definición como referente podemos indicar que los datos en las redes sociales son aquella información que deseamos compartir en las redes sociales ya sea esta información textual o imágenes. “Las Redes Sociales permiten que los usuarios armen en ella su propia página Web (home page). En esta página las personas pueden contar quiénes son, hablar de sus gustos, incluir la información que desean compartir con su lista de amigos. El sitio personal en una red social funciona como una página web y por lo general, incluye información sobre su autor. Entre los datos suelen figurar su nombre, email, fecha de nacimiento genero, y sus gustos: películas, libros, deportes, juegos, links, comentarios, video clips y música”⁵⁸

⁵⁷ Definición de Datos. <http://definicion.de/datos/>

⁵⁸MORDUCHOWICZ, Roxana. MARCON, Atilio. SYVESTRE, Vanina. BALLESTRINI, Florencia. Los Adolescentes y las Redes Sociales, Pagina 6. Septiembre 2010. Revista del Ministerio de Educación, República Argentina.

CAPITULO IV
MARCO JURIDICO
LEGISLACIÓN NACIONAL,
TRATADOS
INTERNACIONALES, Y
LEGISLACION COMPARADA
SOBRE LA MATERIA.



MARCO JURIDICO

CAPITULO IV

LEGISLACIÓN NACIONAL, TRATADOS INTERNACIONALES SOBRE LA MATERIA Y LEGISLACION COMPARADA.

4.1. CONSTITUCIÓN POLÍTICA DEL ESTADO.

Artículo 106. I. El Estado garantiza el derecho a la comunicación y el derecho a la información.

II. El Estado garantiza a las bolivianas y bolivianos el derecho a la libertad de expresión, de opinión y de información, a la rectificación y la réplica, y el derecho a emitir libremente las ideas por cualquier medio de difusión, sin censura previa.

Artículo 130. I. Toda persona individual o colectiva que crea estar indebidamente o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico o electrónico, magnético o informático, en archivos o bancos de datos públicos o privados o que afecten a su derecho fundamental a la intimidad o privacidad personal o familiar, o a su propia imagen u honra y reputación, podrá interponer la Acción de Protección de la Privacidad.

Artículo 131. I. La Acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto por la acción de Amparo Constitucional.

II. Si el tribunal o juez competente declara procedente la acción ordenara la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado.

III. La decisión se elevara, de oficio, en revisión ante el Tribunal Constitucional Plurinacional en el plazo de veinticuatro horas siguientes a la emisión del fallo, sin que por ello se suspenda la ejecución.

IV. La decisión final que conceda la Acción de Protección de Privacidad será ejecutada inmediatamente y sin observaciones. En caso de resistencia se procederá de acuerdo con lo señalado en la Acción de Libertad. La autoridad judicial que no proceda conforme con lo dispuesto por este artículo quedara sujeta a las sanciones previstas por ley.

4.2. TRATADOS Y CONVENIOS INTERNACIONALES

La protección de los datos personales utilizados en medios electrónicos es algo que no está protegido por un tratado o convenio internacional, en ciertos Estados la tendencia es proteger los mismos expresamente en las constituciones y legislaciones internas de cada Estado.

La declaración de derechos humanos de 10 de diciembre de 1945, es sin duda la primera fuente que nos explica respecto de la protección de la intimidad, disponiendo que: “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia , su domicilio o su correspondencia, ni ataques a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra tales injurias o ataques.”

En el año de 1951 fue creado por la UNESCO la Oficina Intergubernamental para la Informática I.B.I (Intergovernmental Bureau for Informatics), tenía como principal objetivo asistir a los países miembros en el campo de la informática, ayudando a comprender mejor los fenómenos y cambios que se producían en sus países debido a la creciente utilización de medios magnéticos electrónicos, formulando estrategias y políticas para el desarrollo del área. Este organismo internacional ofreció a sus países miembros becas de capacitación, conferencias referentes al

problema informático, así publicó varios estudios sobre derecho informático, participando y colaborando en varios congresos. Ante la salida de países como Francia, España, considerados por aquel entonces como los países miembro más desarrollados, la UNESCO redujo a la mitad el presupuesto de dicho organismo, desaparecido en 1987. En su mejor momento, el I.B.I. tenía a los siguientes países como miembros: Argelia, Argentina, Benín, Bolivia, Brasil, Burkina Faso, Camerún, Colombia, Congo, Costa de marfil, Costa Rica, Cuba, Chile ,Ecuador Egipto, Emiratos Árabes Unidos, España, Francia, Gabón Ghana Guinea, Haití, Irak, Italia, Jordania, Líbano , Liberia, Madagascar, Mali, Marruecos, México, Nicaragua, Nigeria, Níger, Nicaragua, Panamá, Sao Tome e Príncipe, Senegal, Siria, Swazilandia, Togo Túnez, Venezuela, Zaire.

El Estado Boliviano fue parte del I.B.I. como es visto en los acuerdos con este Organismo ya desaparecido:

- ❖ Acuerdo Sede entre el Gobierno de la República de Italia y el Centro Internacional de Cálculo, Oficina Intergubernamental para la Informática, firmado en Roma el 22 de marzo de 1974.
- ❖ Convenio de “Creación del Fondo de Becas”, entre el Gobierno de Bolivia y la Oficina Intergubernamental para la Informática, suscrito en La Paz, el 27 de mayo de 1978.
- ❖ Convenio sobre la “Creación del Fondo Conjunto de Becas”, firmado en Santiago de Chile 25 de noviembre de 1980.
- ❖ Programa de Intenciones entre el Gobierno de Bolivia y la Oficina Intergubernamental para la Informática (IBI), suscrito en La Paz el 27 de enero de 1982.

- ❖ Convenio entre el Gobierno de Bolivia y la Oficina Intergubernamental para la Informática (IBI), suscrito en La Paz el 29 de noviembre de 1983.

4.3. CÓDIGO PENAL.

Artículo 363 bis.- (MANIPULACIÓN INFORMÁTICA).- El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procedimiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de un tercero, será sancionado con reclusión de uno a cinco años y con multa de setenta a doscientos diez.

Art. 363 ter.- (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS).- El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.

4.4. LEY DE TELECOMUNICACIONES

Art. 37.- Los servicios de telecomunicaciones son declarados de utilización pública. Salvo disposición judicial competente, queda terminantemente prohibido interceptar, obstruir, alterar, desviar, publicar o divulgar el contenido de las telecomunicaciones.

LEGISLACION COMPARADA

ESPAÑA

CODIGO PENAL

ARTÍCULO 197 DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS:

- I. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

ARTÍCULO 264 DAÑOS INFORMÁTICOS O SABOTAJE:

- II. La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

CALUMNIA: ARTÍCULOS 205 Y 206

INJURIA: ARTÍCULO 208 Y 209 Es posible llevar a cabo estos delitos a través del correo electrónico o incluso a través de terminales móviles.

CALUMNIAS E INJURIAS HECHAS CON PUBLICIDAD, ARTÍCULO

211 En este supuesto cabe perfectamente la difusión de mensajes injuriosos o calumniosos a través de Internet.

ARGENTINA

CODIGO PENAL

VIOLACIÓN DE SECRETOS Y DE LA PRIVACIDAD.

ARTÍCULO 153.- Será reprimido con prisión de quince días a seis meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o capture comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un mes a un año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

ARTÍCULO 153 BIS.- Será reprimido con prisión de quince días a seis meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un mes a un año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

ARTÍCULO 157.- Será reprimido con prisión de un mes a dos años e inhabilitación especial de uno a cuatro años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

ARTÍCULO 157 BIS.- Será reprimido con la pena de prisión de un mes a dos años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.
3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años.

PERU

CODIGO PENAL

ART. 207-A.- El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas.

Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas".

ART. 207-B.- El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días-multa.

ART. 207-C.- En los casos de los Artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando:

1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.
2. El agente pone en peligro la seguridad nacional.

CAPITULO V
MARCO PRÁCTICO
VULNERABILIDAD DE LOS
DATOS DE LOS USUARIOS DE
LAS REDES SOCIALES SEGÚN
LA OPINION EXPERTOS EN
INFORMATICA, REDES
SOCILAES, DERECHO
INFORMATICO Y DERECHO
INTERNACIONAL PUBLICO.

MARCO PRÁCTICO

CAPITULO V

VULNERABILIDAD DE LOS DATOS DE LOS USUARIOS DE LAS REDES SOCIALES SEGÚN LA OPINION DE EXPERTOS EN INFORMATICA, REDES SOCIALES, DERECHO INFORMATICO Y DERECHO INTERNACIONAL PUBLICO.

Los datos de los usuarios de las redes sociales se encuentran en peligro constante, a través de la técnica de la entrevista trataremos de demostrar si es que es fácil violar la seguridad de estos sitios web, como prevenir esta vulneración, que acciones debe de tomar el Estado.

Conociendo la opinión de expertos en informática y redes sociales, derecho informático, y derecho internacional público, podremos analizar lo vulnerables que son los datos que son subidos a las redes sociales, y trataremos de dar una solución a este problema, analizando las diferentes opiniones, y finalmente propondremos mecanismos de control jurisdiccional para poder proteger los datos de los usuarios de las redes sociales en Bolivia.

ENTREVISTA A EXPERTOS EN INFORMATICA Y REDES SOCIALES

Lic. Msc. Edwin Alberto Fernández Camargo experto en informática.

La vulnerabilidad en estos sitios se da a nivel de base de datos. A este tipo de vulnerabilidad solo tenemos acceso a un documento virtual que lo aceptamos y comprometemos a cumplirlo, al momento de crear una cuenta (tanto en Facebook, Twitter y otros).

Lo recomendable es leer estos compromisos para conocer qué tipo de derechos tenemos al colocar nuestra información en un servidor de las redes sociales para conocer en primera instancia a que nos exponemos.

La vulnerabilidad a nivel de usuarios se da principalmente por que los usuarios son responsables de la información que levantan para mostrar en su perfil, a ese nivel debemos tener en cuenta la educación electrónica que tiene cada persona.

Para poder evitar este tipo de vulnerabilidad son necesarios dos aspectos, primeramente leer estos documentos virtuales al momento de crear una cuenta y analizar qué derechos tenemos y principalmente la educación electrónica de las personas.

Se debería poder legalizar la firma digital, de esta manera, al firmar un documento virtual (caso de redes sociales), el estado boliviano tendría todos los derechos de demandar (si corresponde) y/o defender a un boliviano si es que se vulnera su confidencialidad de datos personales y/o demandar resarcición de daños y perjuicios.

Lic. en Informática Jesús Reynaldo Pérez experto en informática.

Los datos subidos a estos sitios de plataforma web, son fáciles de Hackear, en el mundo de la informática existen demasiados programas que son subidos a la red que son fáciles de obtener y descargar, las redes sociales y su simple tipo de ingeniería informática, es fácil de romperla seguridad de estos sitios a través de estos programas, no puede comprarse con el tipo de seguridad que tiene por ejemplo un banco o alguna institución gubernamental nacional o extranjera, pues para poder mellar la seguridad de estos sitios se necesita de crear o encontrar programas ... , una persona común y corriente puede utilizar los mismos para robar información que es subida a estos sitios y utilizarlos de manera perjudicial, tomando en cuenta que los diferentes tipos de redes sociales que existen en la actualidad los datos de los usuarios están a la vista de todo aquel que desea verlos, las redes sociales que son tan populares en la actualidad no enseñan a sus usuarios que en el mismo sitio web, la información que es subida puede

restringirse según lo desea el usuarios, esta puede ser visible para sus amigos o para todo el mundo que desea conocerlos, de una u otra forma si una persona con un conocimiento básico de computación puede llegar a hacer estragos en estos sitios.

Este tipo de vulnerabilidad es prevenible si el usuario de las redes sociales, primeramente cambia su contraseña de usuario cada quince días como mínimo, esta contraseña de usuario debe de contener al menos quince o dieciocho caracteres intercalados como entre letras mayúsculas, minúsculas y números no debe de olvidar que utilizando datos como su nombre y fecha de nacimiento en su contraseña se expone a que su perfil de usuario sea vulnerado por descuido propio, el usuarios de las redes sociales debe de ponerle un límite al tipo de información que se sube a estos sitios pues mucha información hace más vulnerable al usuario. No olvidemos que un cualquier buscador de la web la fotos y otros datos son los primeros en aparecer cuando buscamos a alguna persona y estas fotos y datos son los que ponemos en las redes sociales, otra forma sencilla de prevenir que los datos de los usuarios de las redes sociales sean vulnerados es conectarse en un solo sitio en específico de preferencia el hogar del usuario o el negocio de café internet de algún conocido.

El Estado puede tomar como primera acción la concientización primeramente en las escuelas colegios y universidades mostrando a estos sitios como algo que no es un juego o un pasatiempo pues tiene grandes beneficios al momento de crear una mejor relación del individuo y de sus contactos, si fuera posible crear una normativa específica que pueda sancionar a las personas que causan perjuicio al robar o manipular los datos de sus contactos u otras personas.

Lic. en Informática Andrés Albino experto en informática y redes sociales.

Los datos que son subidos a las redes sociales son los básicos, nombre, edad, sexo, correo electrónico, pero también estos pueden ser específicos que ayudan bastante a la individualización como el número de teléfono fijo, celular, intereses, pensamiento político, creencias, empresa en la que trabaja, etc., estos mientras más y más variados son los que exponen a los dueños de los mismo, se puede llegar a violar las redes sociales y el protocolo de seguridad de estos sitios, aprovechando la información pública que es subida a las redes sociales, un delincuente puede hacer un trabajo de ingeniería social planteándose una serie de estrategias para poder vulnerar la seguridad, y así poder conseguir la información que desea, el delincuente informático sabe que el eslabón más débil de las redes sociales es el usuario de las mismas así que no necesita realizar un trabajo directamente con la red social sino con el usuario, puede utilizar el “phising” que a través de promesas falsas de premios y otros puede llegar a obtener la información que desea, con los diferentes programas que puede tener a la mano puede infectar maliciosamente un correo electrónico que con solo abrirlo infecta y transfiere datos que puede ser utilizado por el delincuente informático, o si bien este pudo romper la seguridad de la red sociales puede a través de las aplicaciones de la red social obtener los datos que necesita ya sea para suplantar la identidad del usuario perjudicado u otro fin que se haya propuesto.

Esta vulnerabilidad puede ser prevenida primeramente a través de la educación, el usuario de las redes sociales debe de estar consciente que la información que sube a estos sitios es visible si él lo desea, entonces antes de formar parte de una red social debe de conocer las distintas políticas de protección que existen en las redes sociales, analizar y conocer bien la red social de la que forma parte saber los alcances de la misma y si está de acuerdo con los protocolos de seguridad poder crear un perfil de usuario, todo lo demás ya viene por añadidura a su forma de desenvolverse en la red social.

Ya que en el Estado Plurinacional de Bolivia, no existe una legislación ni leyes que puedan diferenciar los diferentes delitos informáticos varios delitos de este tipo no

pueden ser descubiertos ni penados, un ejemplo conocido por las personas relacionadas con la informática fue el de una persona que a través de un gran trabajo de ingeniería social pudo clonar las páginas del banco Visa, cuando fue descubierta no tuvo la pena que ameritaba un delito de esa envergadura, si bien existe una policía informática en Bolivia, esta no puede actuar de manera eficiente debido a que los delitos informáticos no están regulados de manera específica, y si no se puede limitar el uso de la informática, menos se pueden proteger los datos de los usuarios de las redes sociales en específico.

No hay leyes que puedan normar las transacciones en línea el comercio electrónico, la firma electrónica no está regulada y todas esas cosas en materia informática impiden el desarrollo de la informática en Bolivia.

ENTREVISTA A EXPERTOS EN DERECHO INFORMÁTICO

Dra. Karina Medinaceli experta en Derecho Informático.

Existen diferentes tipos de redes sociales y dependiendo de la utilización que el usuario les dé a las mismas, ya sea que están destinadas para el ocio como es Facebook o LinkedIn que permite desenvolverse a través del ámbito laboral, primeramente se debe de crear un perfil de usuario y necesariamente esto es voluntario, lo realiza una persona física que es el titular del dato, coloca información personal como su nombre, lugar de ubicación, fecha de nacimiento, fotografías de diferente tipo, coloca y comparte videos, vierte opiniones, y todo de forma voluntaria, la problemática se da en el desconocimiento de los usuarios al aceptar el contrato electrónico tipo estándar que está obligado a aceptar si quiere formar parte de la red social, al leer este contrato nos muestran las diferentes condiciones de privacidad, e indica que toda la información subida a la red social, comentada, compartida, y aun así la suprimida, le pertenece a la red social, no especifica que es lo que hará con estos datos en un futuro, no se sabe si esta información puede ser vendida compartida, etc., es una clara desventaja para el

titular de los datos, nadie nos obliga a abrir una cuenta en una red social pero debemos de aceptar estas condiciones si queremos ser parte de una red social, este hecho es positivo para poder marcar presencia en la red y no ser víctima de usurpación de identidad, incluso solo abrir un perfil que este mantenido en blanco, hace que se marque presencia y el nombre del titular de los datos no sea usurpado, las redes sociales tienen una serie de mecanismos como la denuncia en caso de que alguien este usurpando datos que no le corresponden o este mostrando temas no aptos para menores de edad, habría que socializar estos términos en la población vulnerable como adolescentes y niños, pese a que en estas páginas no se permite el uso a menores de 18 años aun así es que los adolescentes y niños tiene perfiles de usuarios, es necesario un monitoreo a través de los padres para poder saber qué es lo que hacen sus hijos en la red.

En una red social es necesario diferenciar el grado de participación que se tiene, pues los datos subidos pueden ser expuestos a tus amigos, amigos de tus amigos y al público en general creando así una posibilidad infinita de vulnerabilidad de datos, debe de haber una conciencia de la información que se sube, en entornos demasiado íntimos, se han dado caso que personas empleadoras de varias instituciones gubernamentales y privadas han revisado los perfiles de las personas que van a contratar, y han descubierto parte de la vida de estas personas que no va con la imagen de la institución que desea contratarlas debido al fácil acceso de estos datos y por que los mismos están abiertos sin restricción al público, colocamos información innecesaria en las redes sociales.

Los mecanismos de denuncia son una forma de prevenir la vulnerabilidad de los datos de los usuarios de las redes sociales, en el contrato tipo estándar indica que si subimos información con apta para menores, que promueva la xenofobia, temas de discriminación, etc., nuestro perfil de usuario puede ser cerrado, el perfil es gratuito pero diríamos que estamos pagando con nuestra información, al momento de subir información comentarla eliminarla esta pasa inmediatamente a dominio de la red social, una opción que se brindan las redes sociales es poder escoger el

tipo de fotos en las que uno desea aparecer, tomando en cuenta que no toda la información es subida a estos sitios de manera voluntaria, puede llegar a ser que otra persona allegada nuestra, la suba y nos comprometa directamente en aspectos de naturaleza mas intima, la jurisdicción y competencia pertenecen netamente al lugar de procedencia de las redes sociales y en caso de querer tener algún conflicto legal con estas empresas nos encontraríamos en desventaja.

Si hubiese una ley de protección de datos y las redes sociales fueran de origen netamente boliviano habría una forma de limitar la actuación de las redes sociales, la tendencia es sacar leyes específicas, no existe una ley específica que proteja los datos de los usuarios de las redes sociales, por seguridad lo ideal sería sacar una ley específica general, en tema de protección de datos que sea complementaria a la acción de protección de privacidad, como se debe de tratar el dato, cuales son los derechos de los titulares de los datos, sus obligaciones de los responsables de los archivos de estos bancos de datos, poner una sanción que restringiría el tratamiento de los datos, una potestad sancionadora y fiscalizadora de los datos sería algo ideal en la normativa nacional.

Han habido esfuerzos europeos para poder ayudar a que las políticas de privacidad de estas empresas sean más flexibles y se adecuen a la normativa de estos países pero los esfuerzos se quedaron en eso debido a que la jurisdicción y competencia la pone el dueño de la red sociales, se trabaja respetando la privacidad de los datos y el consentimiento del titular de los datos y saber para que sube el dato.

El delito debe de estar regulado no solo por un país y la tendencia que se da en Latinoamérica es reformar el código penal tipificando estas conductas, el sujeto activo puede estar en un país el pasivo en otro país y el servidor de la red social en otro país, se no está legislado no es considerado como delito. Estas conductas deben estar reguladas, las tics son rápidas y el derecho es lento no se puede tratar de regular todo, debido a los adelantos tecnológicos se puede determinar,

quien fue el autor de los delitos informáticos, pues las direcciones ip pueden mostrar la ubicación de donde salió la información, pero no se puede demostrar con certeza quien la envió.

ENTREVISTA A EXPERTOS EN DERECHO INTERNACIONAL.

Tras un análisis global de toda la información almacenada, de las entrevistas a expertos en derecho internacional, se ha establecido dos puntos comunes en cuanto a la opinión de los expertos consultados en esta área:

- Es que debido a que no existe tratados y convenios internacionales que regulen el uso de la informática, los expertos en derecho internacional coinciden en que debe de tomarse en cuenta los esfuerzos impulsados por la comunidad europea, para la protección de datos personales utilizados a través de medios electrónicos y magnéticos.
- Se debe de tomar en cuenta los ejemplos de las constituciones latinoamericanas, hacer una reformulación específicas de las leyes y códigos para que realicen la protección de datos y así poder llegar a generar una normativa que proteja los datos de los usuarios bolivianos de las redes sociales.

CONCLUSIONES

Una vez realizado el análisis de datos recabados en el presente estudio y haber conocido las opiniones de expertos en temas informáticos, derecho informático, y derecho internacional, los datos de los usuarios de las redes sociales se encuentran en peligro, y este tema no solo es una preocupación para las autoridades nacionales, también los es para organismos internacionales.

Por descuido del propio usuario de las redes sociales o ya sea por el ataque de una persona especializada en el tema informático, queda demostrado que no todos los ataques a las redes sociales son realizados de manera malintencionada pues estos mismos son realizados por personas con cierto grado de conocimiento y hasta cierto estatus social, realizan estos ataques mermando de sobremanera el derecho al honor que es aquel que tiene toda persona a su buena imagen y reputación, y su derecho a la intimidad que está ligada íntimamente a la protección de la dignidad del individuo y su entorno.

La carencia de normativas específicas o una reglamentación jurídica para este tipo de casos crea un vacío jurídico legal, vulnerando un principio fundamental como es la seguridad jurídica misma que rige nuestro ordenamiento jurídico vigente, no existe un acuerdo, convenio o tratado internacional, referente a derecho informático y protección de datos, que adapte las costumbres de los países suscribientes.

Podemos mencionar que nuestros expertos en informática y redes sociales, tienen un conocimiento básico de protección de datos todo a través del uso de programas especializados en informática, y no así tomando en cuenta ningún tipo de legislación nacional para el resguardo de datos.

En tal razón al demostrar que no existen mecanismos de control normativo que regulen la protección de datos de los usuarios bolivianos de las redes sociales, el presente trabajo de investigación o tesis de grado demuestra la necesidad de la creación de mecanismos de control normativo para dichos usuarios, protegiendo de esta manera los datos de los usuarios bolivianos de las redes sociales.

SOBRE LOS OBJETIVOS PLANTEADOS

- El objetivo general es establecer mecanismos de control jurisdiccional del Estado Plurinacional Boliviano para garantizar la seguridad de los datos de los usuarios bolivianos de las redes sociales, y es necesario primeramente tipificar los delitos informáticos, crear una normativa específica que proteja los datos de los usuarios de las redes sociales y así poder evitar la serie de delitos informáticos a los que son expuestos los usuarios de estos medios de comunicación masiva, disponer normativamente de mecanismos eficaces y eficientes, realizar una tarea conjunta con el ministerio de educación para así poder coadyuvar una política de carácter infamativo dirigido principalmente a la población mas susceptible de ataques los adolescentes y niños, realizar campañas de concientización sobre la difusión de datos personales en las redes sociales enseñarles a estos las ventajas y las desventajas de las redes sociales, mostrarles las maneras más seguras de mantener sus datos personales seguros, incluir en los planes oficiales de estudio el conocimiento necesario relacionado con la seguridad y de la información de la protección de datos personales fomentando la formación específica en ese campo.
- Se analizo que los datos de los usuarios de las redes sociales, no son solo vulnerables a robo, usurpación, o utilizados para otros fines pues en el momento del registro, ya se tome en cuenta al titular de los datos como usuario de la red social, si no se es configurado correctamente el nivel de privacidad del perfil se es objeto de cualquier tipo de vulneración,

quedando demostrado que esta vulnerabilidad no solo proviene de terceros interesados en perjudicar específicamente al titular de los datos.

- Los expertos en informática coinciden en que los datos de los usuarios de las redes sociales, son vulnerables a todo tipo de ataques y coinciden en que la mejor forma de prevenir los mismos es la educación al momento de utilizar estos sitios, conocer el tipo de red social a la que se pertenece, conocer los términos de usuarios y privacidad, ayudarían a evitar el robo de datos, los expertos en derecho informático y derecho internacional coinciden en que es necesario primeramente tipificar los delitos informáticos, y la creación de una normativa específica que proteja los datos subidos en internet, y después la creación de una normativa que proteja los datos de los usuarios de las redes sociales.
- La tendencia que existe en Latinoamérica es la reformulación de las normativas que protejan primeramente los datos los bancos de datos el tratamiento y administración de los mismos, sancionar estos delitos informáticos para así poder llegar a ser más específicos, en cuanto al tema de protección de datos que son subidos por el usuario de las redes sociales.

RECOMENDACIONES

Primeramente debe de normarse temas como el comercio electrónico, la firma electrónica y otro que ayudarían a un mejor uso de la informática y de las redes sociales, pues una gran parte de los diferentes beneficios de las redes sociales se encuentra disponible a través del comercio electrónico tema que aun no ha sido normado en nuestra legislación y ayudaría bastante a una mejor utilización de la informática y las redes sociales.

El Estado Plurinacional Boliviano debe concientizar a la población más vulnerable como son los adolescentes y niños, a través de políticas educativas, un mejor control de parte de los padres hacia sus hijos, ayudaría primeramente a realizar esta concientización, el uso del internet por parte de los niños y adolescentes debe de ir a la par con el control de los padres ver y analizar en qué clase de paginas estos utilizan su tiempo, saber la clase de contactos que tienen sus hijos en las redes sociales, tratar de ser parte del entorno en el cual se encuentra su hijo en tema de redes sociales.

Los usuarios de las redes sociales deben de conocer los términos de usuario que aceptan al momento de mostrar su aceptación en el contrato de adhesión, pues estos datos de son subidos manera voluntaria a la red social, el usuario debe de saber que esta información inmediatamente es subida pasa a domino de la red social, y conocer todos los términos de usuario que van en beneficio del usuario de las redes sociales.

Debe de impulsarse un mejor manejo profesional de parte de los expertos en informática ayudando así a la población, a tener un mejor conocimiento del tema que es poco conocido por la población en general.

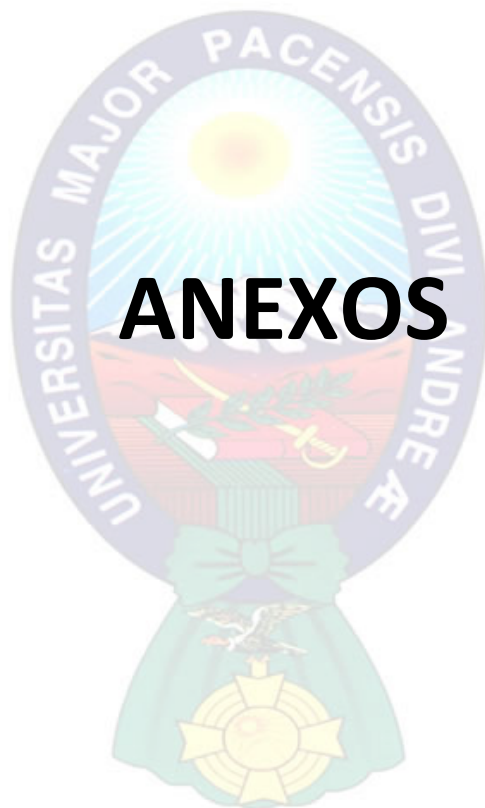
BIBLIOGRAFÍA

- BECERRA Ramírez, Manuel.1991. Derecho Internacional. Editorial Impresos Chávez S.A. de C.V. Primera Edición Ciudad de México D.F.
- DAVARA Rodríguez, Miguel Ángel. 2008. Guía Práctica de Protección de Datos para Abogados. Editorial Da Fa Ma. Primera Edición, Madrid España.
- Definición de Datos. <http://definicion.de/datos/>
- Definición de Red Social. <http://michfer.wordpress.com/2008/08/07/redes-sociales-definicion/>
- Delincuencia Informática, www.scribd.com/doc/16302561/DELINCUENCIA-INFORMATICA.
- FLORES CUETO, Juan Jose, Las redes sociales [jflores@usmpvirtual.edu.pe/](mailto:jflores@usmpvirtual.edu.pe)
- Formación de Web 2.0, <http://scopeo.usal.es/images/documentoscopeo/scopeo.001.pdf>.
- Guía de seguridad en redes sociales, Internet Web Social Media Network Creativi Advertising Blog.
- HERDEGEN, Mathias. Derecho Internacional Público, Editorial Circuito de Maestría Marco de la Cueva. Primera Edición Ciudad de México D.F., 2005.
- HERNANDEZ Sampieri, Roberto. FERNÁNDEZ Collado, Carlos. BAPTISTA Lucio, Pilar. 1997. Metodología de la Investigación, Pagina61. Primera Edición Editorial. Panamericana Formas e Impresos, Colombia.
- HERRERA Jimenez, Francisco José, Web 2.0 y didácticas de lenguas, Pagina2, www.francisco@lajanda.org,
- Internet. www.tiss.es, Documentación elaborada por tecnologías de la Información San Sebastián.
- Introducción al Internet,

- JINESTA Ernesto.1997. Control Jurisdiccional de la Administración Pública.<http://www.ernestojinesta.com/ernestojinesta/curriculuartrev/control.PDF>. Revista Judicial Costa Rica Año XX, N°63.
- lainsindias.net/indianopedia/Teoria_de_redes_sociales .
- Las Redes Sociales, www.delfingroup.es/blog/
- LOZA, Leandro. 2010. Aspectos Legales y Normativos de las Redes Sociales.file:///C:/Users/familia/Desktop/DERECHO INFORMATICO/Aspectos Legales y Normativos de las Redes Sociales _ Abogados Derecho Informático y Nuevas Tecnologías - Estudio Juridico.htm.
- LOZARES, Carlos. Teoría de redes sociales, Pagina 104,
- LOZARES, Carlos. Teoría de redes sociales.
- MORDUCHOWICZ, Roxana. MARCON, Atilio. SYVESTRE, Vanina. BALLESTRINI, Florencia. Los Adolescentes y las Redes Sociales, Pagina 3. 2010. Revista del Ministerio de Educación, República Argentina.
- Problemática Legal de las Redes Sociales.2010. file:///C:/Users/familia/Desktop/DERECHOINFORMATICO/Redes_sociales_problematicelegal.htm.
- Redes Sociales, pagina 116.
- Redes Sociales, pensamiento sistemático, es.wikipedia.org/wiki/Red_social.
- Servicios que ofrece internet, pan.inictel.gob.pe/users/jcasachagua/ofrece.htm.
- TELLÉZ, Jorge. Derecho Informático, Página 13. Editorial, Impresos Chávez S.A. de C.V. Primera Edición Ciudad de México D. F.
- Teoría de las redes sociales,
- TREDINICK, Felipe. 1997. Derecho Internacional Público y Relaciones Internacionales, Página 2. Editorial “Los Amigos del Libro”, La Paz-Cochabamba.
- VILLAROEL Ferrer, Jaime Carlos.2007. Derecho Procesal Orgánico y Ley de Organización Judicial, Pagina 58. Editorial “El Original- San José”. Cuarta Edición Ciudad de El Alto, La Paz Bolivia.

- ZAMBRANO Pasquel, Alfonso, **Delincuencia de cuello blanco**,
www.alfonsozambrano.com/doctrina.../delitocuelloblanco_azp.pdf.





ANEXO I

INFORMACION SOBRE REDES SOCIALES Y DELITOS INFORMATICOS EN BOLIVIA.

- Una red social es una estructura social compuesta de personas, las cuales están conectadas por uno o varios tipos de relaciones, tales como amistad, parentesco, intereses comunes, intercambios económicos, relaciones sexuales, o que comparten creencias, conocimiento o prestigio.

es.wikipedia.org/wiki/Red_social

- Estructura social de relaciones entre usuarios que pueden ser de distinto tipo, como intercambios financieros, amistad, etc. También es el medio de interacción de distintas personas como por ejemplo juegos en línea, chats, foros, spaces, etc. Ejemplos de redes sociales son Facebook y MySpace. ...

www.delfingroup.es/blog/

- pues, eso, una red que es social .Te haces tus amigos, compartes tus gustos y todo ese rollo. ¿Que parece una tontería? Pues que le pregunten al magnate Rupert Murdoch si le pareció una estupidez pagar todo lo que pagó por MySpace. ...

negrosobreblanco.es/

- servicio dirigido a comunidades de usuarios en los que se les permite intercambiar fotos, archivos, aplicaciones, mensajes de texto y otro tipo de contenidos online. Las redes sociales son cada vez más populares y se han convertido en un excelente soporte publicitario y de marketing viral. ...

www.muypymes.com/marketing/ventas/83-diccionario-practico-...

- “estructura social que se puede representar en forma de uno o varios grafos en los cuales los nodos representan individuos y las aristas relaciones entre ellos. Son la socialización definitiva de Internet”.

www.periodistashoy.es/mundo-2-0/13-terminos-digitales-que-de...

- Una red social es una estructura de relaciones entre personas y pueden ser físicas o digitales; las físicas son las que se desarrollan sin ayuda de los medios electrónicos (un pueblo, un vecindario,...). Mientras que las digitales tiene lugar a través de Internet.

www.logrosperu.com/blog/2011/05/conceptos-basicos-2-0-que-...

- conjunto de relaciones que el individuo establece con otras personas, y que no tienen necesariamente como referente espacial o territorial el lugar de residencia. ...

pitagoras.blogia.com/2008/012401-glosario-intervencion-social-...

- Ya sea para ligar, hacer negocios o compartir aficiones, existen decenas de sitios web dedicados a crear y gestionar redes sociales, lugares donde invitar a los amigos y conocer a los 'amigos de los amigos', o aquellas comunidades de intereses comunes. ...

redesdeconvivencia.es/mod/glossary/view.php

- Aunque su uso en EE. UU. data ya de hace ocho años, su popularización en España se sitúa en 2008, cuando Facebook lanzó su versión española y la red Nettby hizo su aparición.

alocubano.wordpress.com/2008/12/25/la-musica-y-la-moda-apo...

- Site que permite a sus usuarios relacionarse online con otros usuarios, a fin de compartir contenidos, interactuar y crear comunidades sobre intereses similares. Ejemplo: Facebook.

www.adpv.com/ayuda.php

- Plataforma web, es decir, un servicio al que se accede a través de una página web por medio de un navegador que permite a los usuarios crear un

perfil suyo y poder hacerlo público o semipúblico. Un perfil es similar a una página web personal pero si necesidad de saber programar. ...

www.xn--coldiseo-j3a.com/glosario.html

- sitios web que permiten a los usuarios interactuar entre ellos y compartir elementos (fotos, comentarios,...)

www.focusmedia.es/es/terminologia-basica-online/

Ordenanza municipal, pretende regular los temores muy bien fundamentados por autoridades, educadores, padres de familia y la sociedad en general. El día de hoy el intendente y concejal Jimenez, señalaron su preocupación referente al uso de computadores con acceso a internet; toda vez que los operativos realizados a los denominados “Cafes intenets” sorprendieron su conocimientos sobre el uso de computadoras, señalando lo siguiente:

◦ Con un “Clik” es fácil ingresar a “Links” pornográficas, programados en las computadoras

◦ Las computadoras tienen videos pornográficos

A cuyo efecto la solución a corto plazo seria el USO OBLIGATORIO DE UN “SOFWER DE BLOQUEO” de paginas pornográficas, a cargo de los dueños de los denominados “Cafes Intenets”

Por otra se pretende regular aspectos físicos, en el servicio de internet que ofrecen estos cafes intenets, referente al espacio adecuado para el usuario TODA VEZ QUE EXISTIRIAN DENUNCIAS DE “toques impúdicos”.

Se tendrá que esperar la promulgación de la ORDENANZA MUNICIPAL, para hacer una revisión minuciosa de artículos, toda vez que se prevee en términos generales una eventual ineficacia de los objetivos perseguidos.

Publicado por BOLIVIA Y EL DERECHO

Enviar por correo electrónico Escribe un blog Compartir con Twitter Compartir con Facebook Compartir con Google Buzz

Etiquetas: ordenanza municipal que pretende regular cafes intenets, ronol orozco rosales

Los ciberdelincuentes, auténticos *okupas* de las redes sociales

En su último informe, Symantec precisó que hay un crecimiento continuo del uso de plataformas 2.0 para distribuir ataques, focalizados en vulnerabilidades de Java.

Informe de Amenazas

En 2010 se generaron 286 millones de nuevas amenazas en la Web, que estuvieron acompañadas del surgimiento de tendencias tales como la sofisticación de los ataques dirigidos a las empresas o el aumento continuo de sitios de redes sociales como plataforma de distribución de ataques. Estos y otros datos se desprenden del último informe anual de Symantec sobre los peligros que existen hoy en día en Internet.

De acuerdo al documento, también hay una variación en las tácticas de los ciberdelincuentes, cada vez más focalizados en vulnerabilidades de Java para irrumpir en los sistemas informáticos tradicionales, y se observa un “notable cambio de foco hacia los dispositivos móviles”.

En el mundo empresarial, se registró un gran número de acciones orientadas a las vulnerabilidades de las compañías, con el objetivo de hacer colapsar sus sistemas informáticos. La mayoría de estas actividades se centró contra “un conjunto de empresas que cotizan en la bolsa, corporaciones multinacionales y organismos gubernamentales, así como un número sorprendente de empresas más pequeñas”.

Para aumentar su grado de éxito, los delincuentes investigaron a las víctimas clave de cada organización, para luego poner en práctica sus habilidades de ingeniería social para ingresar a las redes corporativas. Por otro lado, las

filtraciones de datos ocasionadas por hackeo generaron en promedio que más de 260 mil identidades fueran expuestas por fugas o filtraciones en 2010, lo que correspondió aproximadamente a cuatro veces más que cualquier otro incidente.

Okupas sociales. Esta clase de plataformas, por su creciente popularidad, motivó un gran volumen de malware, siendo el uso de URL abreviadas una de las principales técnicas de ataque. “El año pasado, se publicaron millones de estos enlaces en portales para engañar a las víctimas y cometer ataques de phishing y malware, lo que aumentó exitosa y considerablemente el porcentaje de infecciones”, señaló el informe.

ymantec precisó que, en un escenario típico, el atacante ingresa a una cuenta de red social y publica un enlace abreviado en un portal. “La página luego distribuye automáticamente la dirección a canales de noticias de amigos de la víctima, propagando el vínculo potencialmente a cientos o miles de personas, en cuestión de minutos”, resumió.

A continuación, un listado de los principales datos duros que rodean a la seguridad informática:

- **286 millones de nuevas amenazas:** polimorfismo y nuevos mecanismos de entrega como kits de herramientas de ataque Web continuaron aumentando la cantidad de diversos programas malware.
- Los kits de herramientas de ataque Web tuvo 93 por ciento de incremento en el volumen de ataques Web en 2010. El uso de URL abreviados también contribuyó.
- Argentina ocupa el tercer puesto en la clasificación regional de países con mayor actividad maliciosa en Internet. El primer lugar lo ocupa Brasil, seguido de México.
- **14 nuevas vulnerabilidades de día cero:** desempeñaron un papel clave en ataques focalizados como Hydraq y Stuxnet. Éste último se valió de cuatro vulnerabilidades de día cero diferentes.

- Puesto que los delincuentes del ciberespacio están comenzando a centrar sus esfuerzos en el espacio móvil, aumentó el número de nuevas vulnerabilidades reportadas, al pasar de 115 vulnerabilidades en 2009, a 163 en 2010.
- **\$15 dólares por 10.000 bots:** Symantec detectó un anuncio que listaba el precio de 10.000 equipos infectados con bots en \$15 en un foro clandestino en 2010. Los bots normalmente se utilizan en spam o campañas de rogueware, sin embargo cada vez más se utilizan también en ataques DDoS.
- **\$0.07 a \$100 dólares por tarjeta de crédito:** el precio de los datos de las tarjetas de crédito en foros clandestinos oscilaron ampliamente en 2010.

Fuente: <http://www.canal-ar.com.ar/noticias/noticiamuestra.asp?Id=10637>

Publicado por BOLIVIA Y EL DERECHO

En un tiempo en el que **la protección de la privacidad es la gran asignatura pendiente de Internet**, uno de los ejercicios prácticos “obligados” es el de conocer **a quién pertenecen nuestros datos una vez decidimos compartirlos en una red social**. Obviamente, no hay un criterio único en el tratamiento de los datos personales y contenidos por parte de las distintas redes sociales, sino que es cada una de ellas la que, de manera unilateral, determina sus propios parámetros de privacidad, poniendo a disposición del usuario una serie de herramientas que le ayudan a redefinirlos.

Lo anterior no significa que el margen de acción de los prestadores de servicios de Internet sea absoluto. Todos los operadores de Internet que dirigen sus servicios específicamente al territorio español –incluidas las redes sociales- están sujetos a lo dispuesto por la legislación española, por lo que una serie de principios mínimos han de ser cumplidos en todo caso. Eso es, al menos, lo que dispone el artículo 4 de la LSSI. Cuestión distinta es el grado de cumplimiento normativo que las autoridades exigen a los operadores extranjeros, pero ése es otro debate.

Y como las decisiones conscientes y libres –entre ellas, la de elegir la/s red/es social/es a la/s que queremos pertenecer- sólo pueden ser tomadas desde el

conocimiento, **ahí va un poco de información acerca del tratamiento que las principales redes sociales que operan en España hacen de nuestros datos**, principalmente fotografías y contenidos, según anuncian en sus propios términos y condiciones.

Empecemos por **Facebook**. En sus condiciones de uso, la red con sede en Palo Alto te informa de que tú “eres el propietario de todo el contenido y la información que publicas en Facebook”. Lo anterior implicaría que el usuario es en todo momento dueño de sus contenidos, pero esto no es así. La propia red matiza más adelante en sus términos de uso, respecto de aquellos contenidos objeto de propiedad intelectual tales como fotografías y videos, que “nos concedes una licencia (...) para utilizar cualquier contenido de PI que publiques en Facebook”. Esta licencia finaliza “cuando eliminas tu contenido de PI o tu cuenta, a menos que el contenido se ha compartido con terceros y éstos no lo han eliminado”. Es decir, que tus contenidos son tuyos, pero también de Facebook, y de todos los demás usuarios si así lo has permitido.

La red de microblogging **Twitter** se expresa, por su parte, en términos similares. Establecen sus condiciones de uso que “el usuario se reserva los derechos de cualquier contenido enviado, publicado o presentado a través de los servicios”. Pero, al publicar dicho contenido, el usuario “otorga el derecho a Twitter de poner a la disposición de otras compañías, organizaciones o individuos asociados con Twitter el contenido para la sindicación, difusión, distribución o publicación de dicho contenido en otros medios y servicios”. Osea, más de lo mismo, o incluso más.

Tuenti, la red social española con más usuarios, establece un matiz importante en la licencia que el usuario concede a la red. Y es que, rezan sus términos de uso, “al publicar contenidos en tu perfil (...) conservas todos tus derechos sobre los mismos y otorgas a TUENTI una licencia limitada para reproducir y comunicar públicamente los mismos”. Hasta ahí todo igual, pero esta autorización, continúan sus términos, “es con la única y exclusiva finalidad de que TUENTI pueda prestarte el servicio”. Además “la anterior licencia quedará resuelta una vez que elimines tu contenido del Servicio o des de baja tu perfil.” Es decir, que al

compartir un contenido en Tuenti, el usuario le concede a la red social una licencia para que le sea prestado el servicio, sin que pueda Tuenti, con carácter general, ceder esos contenidos a terceros.

Youtube da un paso más allá que el resto de redes sociales, posiblemente invitada por su propia naturaleza. Y es que al compartir un video en YouTube, el usuario otorga a favor de ésta una licencia similar a las ya expuestas, pero es que, además, concede idéntica licencia a favor del resto de usuarios “para utilizar, reproducir, distribuir, realizar obras derivadas de, mostrar y ejecutar dicho contenido en la medida de lo permitido por la funcionalidad del servicio”. Como dato curioso, señalar que ambas licencias quedan canceladas cuando el usuario elimina o borra sus videos, pero no así los comentarios, cuya cesión tiene “carácter perpetuo e irrevocable”.

LinkedIn, la red social destinada a compartir contactos profesionales, reconoce que “tú eres el propietario de la información que facilitas a LinkedIn y puedes solicitar su eliminación en cualquier momento a menos que hayas compartido información o contenido con otros y éstos no la hayan eliminado o haya sido copiada o almacenada por otros usuarios”. Poca novedad en este sentido, pero el usuario otorga una licencia a LinkedIn para “comercializar mediante todas las modalidades de explotación conocidas actualmente o descubiertas en un futuro cualquier información que facilites a LinkedIn”.

La **Wikipedia**, si es que se puede considerar a ésta como red social, dispone lo siguiente. El usuario, al compartir un contenido, “acepta licenciarlo bajo la Creative Commons Attribution/Share-Alike License 3.0 (Unported). Por razones de compatibilidad, también deberá licenciarlo bajo la GNU Free Documentation License. (...) Los reutilizadores pueden elegir la(s) licencia(s) que deseen”. En definitiva, que el usuario que comparte contenido en la Wikipedia pierde el control del mismo, si bien obliga a quien pretenda reutilizarlo a compartirlo en idéntica manera.

Lo dicho, ni mejor ni peor. **Cada red social presenta sus propias peculiaridades, no solamente en cuanto a las prestaciones que ofrecen a sus usuarios sino en cuanto al tratamiento que confiere a los contenidos compartidos por éstos.** Sólo con información es válida la elección.

ANEXO II

ENTREVISTAS A EXPERTOS EN INFORMATICA, REDES SOCIALES Y DERECHO INFORMATICO, CREACION DEL IBI (OFICINA INTERGUBERNAMENTAL PARA L INFORMATICA) EN BOLIVIA.

ENTREVISTA PARA EXPERTOS EN INFORMATICA Y REDES SOCIALES

Lic. Msc. Edwin Alberto Fernández Camargo experto en informática.

1 *¿Cuál vulnerables son los datos de los usuarios de las redes sociales? ¿Por qué?*

La vulnerabilidad en estos sitios se da a nivel de base de datos. A este tipo de vulnerabilidad solo tenemos acceso a un documento virtual que lo aceptamos y comprometemos a cumplirlo, al momento de crear una cuenta (tanto en Facebook, Twitter y otros).

2 *¿Cómo se puede prevenir esta vulnerabilidad?*

Lo recomendable es leer estos compromisos para conocer qué tipo de derechos tenemos al colocar nuestra información en un servidor de las redes sociales para conocer en primera instancia a que nos exponemos.

La vulnerabilidad a nivel de usuarios se da principalmente por que los usuarios son responsables de la información que levantan para mostrar en su perfil, a ese nivel debemos tener en cuenta la educación electrónica que tiene cada persona.

Para poder evitar este tipo de vulnerabilidad son necesarios dos aspectos, primeramente leer estos documentos virtuales al momento de crear una cuenta y

analizar qué derechos tenemos y principalmente la educación electrónica de las personas.

3 *¿Qué acciones podría tomar el Estado para proteger los datos de los usuarios de las redes sociales?*

Se debería poder legalizar la firma digital, de esta manera, al firmar un documento virtual (caso de redes sociales), el estado boliviano tendría todos los derechos de demandar (si corresponde) y/o defender a un boliviano si es que se vulnera su confidencialidad de datos personales y/o demandar resarcición de daños y perjuicios.

Lic. en Informática Jesús Reynaldo Pérez experto en informática.

1 *¿Cuál vulnerables son los datos de los usuarios de las redes sociales? ¿Por qué?*

Los datos subidos a estos sitios de plataforma web, son fáciles de Hackear, en el mundo de la informática existen demasiados programas que son subidos a la red que son fáciles de obtener y descargar, las redes sociales y su simple tipo de ingeniería informática, es fácil de romperla seguridad de estos sitios a través de estos programas, no puede comprarse con el tipo de seguridad que tiene por ejemplo un banco o alguna institución gubernamental nacional o extranjera, pues para poder mejorar la seguridad de estos sitios se necesita de crear o encontrar programas ... , una persona común y corriente puede utilizar los mismos para robar información que es subida a estos sitios y utilizarlos de manera perjudicial, tomando en cuenta que los diferentes tipos de redes sociales que existen en la actualidad los datos de los usuarios están a la vista de todo aquel que desea verlos, las redes sociales que son tan populares en la actualidad no enseñan a sus usuarios que en el mismo sitio web, la información que es subida puede restringirse según lo desea el usuarios, esta puede ser visible para sus amigos o para todo el mundo que desea conocerlos, de una u otra forma si una persona con un conocimiento básico de computación puede llegar a hacer estragos en estos sitios.

2 ¿Cómo se puede prevenir esta vulnerabilidad?

Este tipo de vulnerabilidad es prevenible si el usuario de las redes sociales, primeramente cambia su contraseña de usuario cada quince días como mínimo, esta contraseña de usuario debe de contener al menos quince o dieciocho caracteres intercalados como entre letras mayúsculas, minúsculas y números no debe de olvidar que utilizando datos como su nombre y fecha de nacimiento en su contraseña se expone a que su perfil de usuario sea vulnerado por descuido propio, el usuarios de las redes sociales debe de ponerle un límite al tipo de información que se sube a estos sitios pues mucha información hace más vulnerable al usuario. No olvidemos que un cualquier buscador de la web la fotos y otros datos son los primeros en aparecer cuando buscamos a alguna persona y estas fotos y datos son los que ponemos en las redes sociales, otra forma sencilla de prevenir que los datos de los usuarios de las redes sociales sean vulnerados es conectarse en un solo sitio en específico de preferencia el hogar del usuario o el negocio de café internet de algún conocido.

3 ¿Qué acciones podría tomar el Estado para proteger los datos de los usuarios de las redes sociales?

El Estado puede tomar como primera acción la concientización primeramente en las escuelas colegios y universidades mostrando a estos sitios como algo que no es un juego o un pasatiempo pues tiene grandes beneficios al momento de crear una mejor relación del individuo y de sus contactos, si fuera posible crear una normativa específica que pueda sancionar a las personas que causan perjuicio al robar o manipular los datos de sus contactos u otras personas.

Lic. en Informática Andrés Albino experto en informática y redes sociales.

1 ¿Cuál vulnerables son los datos de los usuarios de las redes sociales? ¿Por qué?

Los datos que son subidos a las redes sociales son los básicos, nombre, edad, sexo, correo electrónico, pero también estos pueden ser específicos que ayudan bastante a la individualización como el número de teléfono fijo, celular, intereses, pensamiento político, creencias, empresa en la que trabaja, etc., estos mientras más y más variados son los que exponen a los dueños de los mismo, se puede llegar a violar las redes sociales y el protocolo de seguridad de estos sitios, aprovechando la información pública que es subida a las redes sociales, un delincuente puede hacer un trabajo de ingeniería social planteándose una serie de estrategias para poder vulnerar la seguridad, y así poder conseguir la información que desea, el delincuente informático sabe que el eslabón más débil de las redes sociales es el usuario de las mismas así que no necesita realizar un trabajo directamente con la red social sino con el usuario, puede utilizar el “phising” que a través de promesas falsas de premios y otros puede llegar a obtener la información que desea, con los diferentes programas que puede tener a la mano puede infectar maliciosamente un correo electrónico que con solo abrirlo infecta y transfiere datos que puede ser utilizado por el delincuente informático, o si bien este pudo romper la seguridad de la red sociales puede a través de las aplicaciones de la red social obtener los datos que necesita ya sea para suplantar la identidad del usuario perjudicado u otro fin que se haya propuesto.

2 ¿Cómo se puede prevenir esta vulnerabilidad?

Esta vulnerabilidad puede ser prevenida primeramente a través de la educación, el usuario de las redes sociales debe de estar consciente que la información que sube a estos sitios es visible si él lo desea, entonces antes de formar parte de una red social debe de conocer las distintas políticas de protección que existen en las redes sociales, analizar y conocer bien la red social de la que forma parte saber los alcances de la misma y si está de acuerdo con los protocolos de seguridad poder crear un perfil de usuario, todo lo demás ya viene por añadidura a su forma de desenvolverse en la red social.

3 *¿Qué acciones podría tomar el Estado para proteger los datos de los usuarios de las redes sociales?*

Ya que en el Estado Plurinacional de Bolivia, no existe una legislación ni leyes que puedan diferenciar los diferentes delitos informáticos varios delitos de este tipo no pueden ser descubiertos ni penados, un ejemplo conocido por las personas relacionadas con la informática fue el de una persona que a través de un gran trabajo de ingeniería social pudo clonar las páginas del banco visa, cuando fue descubierto no tuvo la pena que ameritaba un delito de esa envergadura, si bien existe una policía informática en Bolivia, esta no puede actuar de manera eficiente debido a que los delitos informáticos no están regulados de manera específica, y si no se puede limitar el uso de la informática, menos se pueden proteger los datos de los usuarios de las redes sociales en específico.

No hay leyes que puedan normar las transacciones en línea el comercio electrónico, la firma electrónica no está regulada y todas esas cosas en materia informática impiden el desarrollo de la informática en Bolivia.

ENTREVISTA PARA EXPERTOS EN DERECHO INFORMÁTICO

Dra. Karina Medinaceli experta en Derecho Informático.

1 *¿Cuáles vulnerables son los datos de los usuarios de las redes sociales? ¿Por qué?*

Existen diferentes tipos de redes sociales y dependiendo de la utilización que el usuario les dé a las mismas, ya sea que están destinadas para el ocio como es facebook o LinkedIn que permite desenvolverse a través del ámbito laboral, primeramente se debe de crear un perfil de usuario y necesariamente esto es voluntario, lo realiza una persona física que es el titular del dato, coloca información personal como su nombre, lugar de ubicación, fecha de nacimiento,

fotografías de diferente tipo, coloca y comparte videos, vierte opiniones, y todo de forma voluntaria, la problemática se da en el desconocimiento de los usuarios al aceptar el contrato electrónico tipo estándar que está obligado a aceptar si quiere formar parte de la red social, al leer este contrato nos muestran las diferentes condiciones de privacidad, e indica que toda la información subida a la red social, comentada, compartida, y aun así la suprimida, le pertenece a la red social, no especifica que es lo que hará con estos datos en un futuro, no se sabe si esta información puede ser vendida compartida ,etc., es una clara desventaja para el titular de los datos, nadie nos obliga a abrir una cuenta en una red social pero debemos de aceptar estas condiciones si queremos ser parte de una red social, este hecho es positivo para poder marcar presencia en la red y no ser víctima de usurpación de identidad, incluso solo abrir un perfil que este mantenido en blanco, hace que se marque presencia y el nombre del titular de los datos no sea usurpado, las redes sociales tienen una serie de mecanismos como la denuncia en caso de que alguien este usurpando datos que no le corresponden o este mostrando temas no aptos para menores de edad, habría que socializar estos términos en la población vulnerable como adolescentes y niños, pese a que en estas páginas no se permite el uso a menores de 18 años aun así es que los adolescentes y niños tiene perfiles de usuarios, es necesario un monitoreo a través de los padres para poder saber qué es lo que hacen sus hijos en la red.

En una red social es necesario diferenciar el grado de participación que se tiene, pues los datos subidos pueden ser expuestos a tus amigos, amigos de tus amigos y al público en general creando así una posibilidad infinita de vulnerabilidad de datos, debe de haber una conciencia de la información que se sube, en entornos demasiado íntimos, se han dado caso que personas empleadoras de varias instituciones gubernamentales y privadas han revisado los perfiles de las personas que van a contratar, y han descubierto parte de la vida de estas personas que no va con la imagen de la institución que desea contratarlas debido al fácil acceso de estos datos y por que los mismos están abiertos sin restricción al público, colocamos información innecesaria en las redes sociales.

2 ¿Cómo se puede prevenir esta vulnerabilidad?

Los mecanismos de denuncia son una forma de prevenir la vulnerabilidad de los datos de los usuarios de las redes sociales, en el contrato tipo estándar indica que si subimos información con apta para menores, que promueva la xenofobia, temas de discriminación, etc., nuestro perfil de usuario puede ser cerrado, el perfil es gratuito pero diríamos que estamos pagando con nuestra información, al momento de subir información comentarla eliminarla esta pasa inmediatamente a dominio de la red social, una opción que se brindan las redes sociales es poder escoger el tipo de fotos en las que uno desea aparecer, tomando en cuenta que no toda la información es subida a estos sitios de manera voluntaria, puede llegar a ser que otra persona allegada nuestra, la suba y nos comprometa directamente en aspectos de naturaleza mas intima, la jurisdicción y competencia pertenecen netamente al lugar de procedencia de las redes sociales y en caso de querer tener algún conflicto legal con estas empresas nos encontraríamos en desventaja.

3 ¿Qué acciones podría tomar el Estado para proteger los datos de los usuarios de las redes sociales?

Si hubiese una ley de protección de datos y las redes sociales fueran de origen netamente boliviano habría una forma de limitar la actuación de las redes sociales, la tendencia es sacar leyes específicas, no existe una ley específica que proteja los datos de los usuarios de las redes sociales, por seguridad lo ideal sería sacar una ley específica general, en tema de protección de datos que sea complementaria a la acción de protección de privacidad, como se debe de tratar el dato, cuales son los derechos de los titulares de los datos, sus obligaciones de los responsables de los archivos de estos bancos de datos, poner una sanción que restringiría el tratamiento de los datos, una potestad sancionadora y fiscalizadora de los datos sería algo ideal en la normativa nacional.

4 ¿Que mecanismo de Control jurisdiccional debería impulsar el Estado para garantizar la seguridad de los datos de los usuarios de las redes sociales?

Han habido esfuerzos europeos para poder ayudar a que las políticas de privacidad de estas empresas sean más flexibles y se adecuen a la normativa de estos países pero lo esfuerzos se quedaron en eso debido a que la jurisdicción y competencia la pone el dueño de la red sociales, se trabaja respetando la privacidad de los datos y el consentimiento del titular de los datos y saber para que sube el dato.

El delito debe de estar regulado no solo por un país y la tendencia que se da en Latinoamérica es reformar el código penal tipificando estas conductas, el sujeto activo puede estar en un país el pasivo en otro país y el servidor de la red social en otro país, se no está legislado no es considerado como delito. Estas conductas deben estar reguladas, las tics son rápidas y el derecho es lento no se puede tratar de regular todo, debido a los adelantos tecnológicos se puede determinar, quien fue el autor de los delitos informáticos, pues las direcciones IP pueden mostrar la ubicación de donde salió la información, pero no se puede demostrar con certeza quien la envió.

