

# El desconocimiento de las normas y el mal uso de LOS MEDIOS INFORMÁTICOS PUEDE OCASIONAR PROBLEMAS

López López César Augusto.  
cesarnex@gmail.com  
Universidad Piloto de Colombia

*Resumen*— Este artículo hace referencia al desconocimiento de las leyes sobre protección de la información y de los datos, la importancia de conocer normas institucionales de las empresas y las leyes que rigen en Colombia, ya que son violadas o vulneradas a diario pero la mayoría, son por desconocimiento de las mismas, los usuarios realizan actos que para ellos son normales que no afectan a nadie o que si los afectan no tienen ninguna pena legal, porque si los usuarios supieran que lo están realizando está mal y que tiene una serie de penas legales vigentes no lo realizarían.

*Índice de Términos*— *Datos, Información, Ley 1273 de 2009, Redes Sociales, Usuarios.*

## I. INTRODUCCIÓN

El desconocimiento de un buen uso de un medio informático (computadores, tabletas o celulares) ya sea en la oficina o en la casa, puede llegar a causar varios problemas y algunos muy graves. El desconocimiento de normas institucionales y peor aun leyes nacionales sobre el uso de medios informáticos es algo muy común en Colombia, la violación de muchas de estas leyes se realizan a diario y la mayoría de veces no se dan por enteradas las personas que están siendo afectadas y no necesariamente por personas conocedoras de dichas leyes, que por ello se aprovechan, si no lo contrario individuos que también desconocen que los actos que realizan ya sean burlas, chistes o solamente acciones que para ellos son comunes, que se ven a diario, estas acciones pueden estar violando leyes en Colombia.

El mundo digital se ha integrado en toda la sociedad de una forma vertiginosa, en nuestros diarios vivir son más las personas que se apoyan en medios informáticos y el internet para utilizar sus servicios

o realizar actividades, enviar un correo electrónico, participar en foros de discusión, tener una sesión de chat, comunicaciones de voz, descarga de libros, música, videos, ingresar a redes sociales etc. Pero se desconocen una serie de reglamentos o normas que están constituidas para la protección de la información, que se maneja por estos medios y por desconocerlas ya sea por falta de información en medios electrónicos, televisivos, escritos o por pasarlas por alto puede ocasionar problemas de índole legal.

## II. LEY 1273 DE 2009

El día cinco de enero de 2009 entro en vigencia la ley colombiana contra delitos informáticos denominada, “De la protección de la información y de los datos” la ley por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Dicha ley es desconocida por la mayoría de personas que ingresan a sitios web, manipulan equipos informáticos, manipulan datos, información y bienes intangibles en medios electrónicos, son varios artículos que pueden llegar a afectar a personas que manipulan cualquier dispositivo que contenga datos o información.

Hoy en día las redes sociales tienen inundado el internet por decirlo así, la publicidad, el mercadeo, la forma de conseguir nuevos clientes, todo se traslado a las redes sociales, el ¿por qué? Es simple cada día son más los usuarios que hacen parte de

ellas, ya no es necesario tener un computador para poder ingresar a internet, ahora se puede desde un celular una tableta y cada uno de ellos trae aplicaciones de redes sociales las cuales se han convertido en una ola que cada día va creciendo arrastrando mas y mas nuevos usuarios que ven atractivo ver perfiles, ver comentarios de estados, ver fotos de amigos, conocidos o simplemente persona que les llaman la atención, nada malo al contrario interesante y un mundo nuevo para muchos pero el saber darle un buen uso a los equipos como a las redes sociales es algo que no se explica al interactuar con ellos.

Empecemos con algunos detalles de las redes sociales por ejemplo realizar comentarios, crear grupos, subir fotos etcétera el decir que las redes sociales son libres para escribir, publicar y opinar de cualquier persona o entidad, desconociendo que pueden ser afectadas y pensando que no estamos haciendo nada malo. Luego de que Nicolás Castro un estudiante de la universidad Jorge Tadeo Lozano fuera detenido presuntamente por crear un grupo en la red social Facebook grupo en el cual amenazaba a un hijo de un presidente, los delitos en las redes sociales son más reconocidos, los fotomontajes dañando el buen nombre de una persona, la injuria, la calumnia y el más común la violación de los datos personales. Todo por desconocimiento de la ley no hay en alguna parte de la inscripción o creación de cuentas en redes sociales que publiquen que cada país cuenta con leyes para sistemas informáticos y datos personales o por lo menos que Colombia cuenta con la ley 1273.

### ***Las empresas***

Los que trabajan en el mundo empresarial deben recibir claras y específicas instrucciones que los ayuden a garantizar la seguridad de la información, la mayoría de las empresas cuentan con una serie de políticas de seguridad las cuales están compuestas por normas que se deben cumplir, pero el problema en algunas empresas es que estas políticas y normas no son comunicadas a todos sus empleados y ocurre lo mismo que con las redes sociales y equipos informáticos de las personas del común que es el desconocimiento de la norma.

En una empresa se pueden presentar varios inconvenientes por desconocimiento de las normas institucionales y las leyes colombianas, los equipos

informáticos son de la empresa y pueden llegar a ver varios reglamentos y normas sobre ellos, entonces no se puede llegar a asegurar que son equipos personales, lo mismo pasa con los correos institucionales, la información y los datos contenidos en dichos equipos informáticos hacen parte de la empresa y por ello se debe tener muy claro que no es debido guardar la información personal en dichos equipos, ni utilizar el correo institucional para enviar correos de índole personal, está establecido en varias normas de las empresas que los encargados de seguridad pueden intervenir y revisar los correos y equipos de las organizaciones.

En las empresas también se pueden llegar a presentar inconvenientes por ignorar normas o leyes como por ejemplo: querer hacer una broma ya que un compañero dejó sesión del equipo abierta y se envió un correo a alguien desde la cuenta de él, o copiar alguna foto personal que se encontró en el equipo y luego se publicó en una red social, también la instalación de algún software para descargar música, esto en empresas que no cuentan con un buenas políticas de seguridad que permitan tener bloqueado los equipos para estas instalaciones. Algunas de estas faltas que para muchas personas pueden ser inofensivas y con ello no hacerle daño a nadie están penalizadas en los siguientes artículos de la ley 1273.

Los siguientes hechos se pueden presentar por desconociendo de la ley y esto puede llegar a ocurrir legalmente, por ejemplo:

*A. El encontrar un equipo de cómputo de un compañero o conocido del trabajo, del estudio o simplemente un conocido que dejó el equipo solo, sin bloquear y se presentó el acceso al equipo por curiosear que contiene, mirar fotos, copiar algún archivo, puede que legalmente este violando la ley 1273.*

**Artículo 269A:** *Acceso abusivo a un sistema informático.* El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y

en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

*B. Al realizar el arreglo de un computador ya sea de una empresa como ingeniero de soporte o de mesa de ayuda o alguien con un conocimiento en el tema y arregle él un computador a un conocido o desconocido, que muchas veces se pueden presentar algunos errores involuntarios, como borrar carpetas de usuarios, formatear discos sin tomar copias, eliminar información de bases de datos, actualizar versiones de programas que hacen incompatibles los datos actuales. Anteriormente no pasaba nada más que un susto y verse obligado a recuperar de alguna forma la información y todo terminaba como una anécdota. A partir de la ley el propietario de la información se puede denunciar (no demandar) y si un juez lo considera podría tener prisión con el siguiente artículo.*

**Artículo 269D: Daño Informático.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

*C. Muchas veces se descarga algún tipo de software para descargar música, videos, editores de imágenes, de videos etc. No solo en los hogares si no también en algunas empresas que todavía no cuentan con unas buenas normas de seguridad implementadas por las aéreas de sistemas o tecnologías, y la persona que descarga dicho software nunca se detiene a preguntarse si este tipo de software puede llegar a presentar problemas como la instalación de un virus o que lo que se está descargando no sea una canción si no un virus que pueda llegar a afectar la maquina o un sistema de información, y todo por una irresponsabilidad y puede ser denunciado con el siguiente artículo.*

**Artículo 269E: Uso de software malicioso.** El que, sin estar facultado para ello, produzca, trafique,

adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

*D. Los casos más comunes de desconocimiento de la ley se presenta en las redes sociales en donde se maneja diferente tipo de información, para muchos no valiosa pero que si lo es, información que por lo general son datos personales que muchas veces no se cuidan. En las redes sociales se presentan muchos sucesos que son normales para muchos y que se ven a diario que no parecen extraños como: subir fotos, realizar comentarios, crear grupos etc. Pero qué puede suceder si las fotos que aparecen son fотomontajes o personales y no tuvieron la autorización de los actores para subirlas, otro caso que se presenta son los comentarios que se escriben los cuales pueden llegar a ser injurias, denuncias, calumnias o amenazas. La creación de grupos los cuales contienen nombres sin pensar o solamente por colocarle un nombre como matar, violar, robar y con ello amenazan a personas. Son actitudes, actividades que se hacen sin un sentido común, todas las personas o usuarios de las redes sociales no cuentan con la educación, ni la información necesaria para saber que pueden estar violando el artículo.*

**Artículo 269F: Violación de datos personales.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Estos son algunos artículos que los usuarios violan de forma inconsciente por desconocer la ley y cada uno de estos artículos puede llegar a presentar agravaciones punitivas que llevan a condenas más largas, el resto de artículos de la ley son:

**Artículo 269B:** *Obstaculización ilegítima de sistema informático o red de telecomunicación.* El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

**Artículo 269C:** *Interceptación de datos informáticos.* El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

**Artículo 269G:** *Suplantación de sitios web para capturar datos personales.* El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

**Artículo 269H:** *Circunstancias de agravación punitiva:* Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

**Artículo 269I:** *Hurto por medios informáticos y semejantes.* El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

**Artículo 269J:** *Transferencia no consentida de activos.* El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

### III. LA INVESTIGACIÓN

Después de que haya ocurrido algún incidente o una denuncia se adelanta una investigación y si por desconocimiento aparte de la ley se desconoce que hay medios, ciencias y tecnologías que permiten identificar, preservar, analizar y presentar datos que sean validos dentro de un proceso legal.

Si se desconoce que existe la informática forense o nunca se ha llegado a escuchar de ella, investigue e infórmese sobre esta ciencia antes de realizar cualquier acto en medios electrónicos porque si se cree que realizar acciones en los equipos electrónicos no deja huella o nunca se sabrá desde donde o quien lo hizo están en un error.

#### **Informática Forense**

Es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional.

La informática forense es una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso.

Dentro de lo forense encontramos varias definiciones:

- A. Computación forense (computer forensics) que entendemos por disciplina de las ciencias forenses, que considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso; o como la disciplina científica y especializada que entendiendo los elementos propios de las tecnologías de los equipos de computación ofrece un análisis de la información residente en dichos equipos.
- B. Forense en redes (network forensics) Se encarga de los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular. Esta conjunción de palabras establece un profesional que entendiendo las operaciones de las redes de

computadores, es capaz, siguiendo los protocolos y formación criminalística, de establecer los rastros, los movimientos y acciones que un intruso ha desarrollado para concluir su acción. A diferencia de la definición de computación forense, este contexto exige capacidad de correlación de evento, muchas veces disyuntos y aleatorios, que en equipos particulares, es poco frecuente.

- C. Forense digital (digital forensics) Forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos (¿quién?, ¿cómo?, ¿dónde?, ¿cuándo?, ¿porqué?) de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática.

### IV. CONCLUSIONES

Es importante estar bien enterado de las leyes que rigen en cada país y en cada organización con los medios electrónicos para no incurrir en ninguna falta, un buen uso de dichos medios puede evitar muchos inconvenientes de índole legal, moral y porque no económico.

La frase de libertad de expresión está siendo mal interpretada en las redes sociales, con comentarios que están siendo utilizados para desprestigiar, ofender y acusar a personas o entidades sin tener un fundamento claro de los hechos ó acciones, solamente por tener un concepto erróneo, que las redes sociales son para opinar lo que se piensa.

## APÉNDICE

Artículos de la ley 1273.

Artículo 2.

Artículo 3.

Artículo 4.

## RECONOCIMIENTO

Reconocimiento a la Universidad Piloto de Colombia por realizar el esfuerzo de generar los diplomados para reforzar los conocimientos en áreas del interés de los estudiantes y a mi familia por el apoyo.

## REFERENCIAS

- [1] AGIRRE, Jorge Ramió. Dr. Libro Electrónico de Seguridad Informática y Criptografía versión 4.1
- [2] GÓMEZ VIEITES, Álvaro. Enciclopedia de la Seguridad Informática. México: Alfaomega Grupo Editor, 2007, 696 p.
- [3] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Tecnología de la Información – Técnicas de Seguridad – Código para la práctica de la gestión de la seguridad de la información. ISO 17799:2005. 2 ed. Geneve, Suiza. 2005. 170 P.
- [4] DUSSAN CLAVIJO, Ciro Antonio. Políticas de seguridad informática. En: Entramado, Enero – Junio, 2006 Vol 2, No. 1, p. 86-92.
- [5] LEY 1273 DE 2009 Disponible en <  
[http://www.secretariassenado.gov.co/senado/basedoc/ley/2009/ley\\_1273\\_2009.html](http://www.secretariassenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html)
- [6] Delitos en redes sociales Disponible en <  
<http://historico.elpais.com.co/paisonline/notas/Diciembre062009/delitosred.html>

## Autores

Presentado por:  
César Augusto López López.  
Ingeniero de Sistemas  
Universidad Piloto de Colombia  
2010

*“Este documento está diseñado para crear conciencia sobre el buen uso de los medio informáticos”*