El mundo cibernético y los delitos Informáticos.

Autor: Eddy Hardany Cedeño Velasco

RESUMEN

El uso de la tecnología tiene la ventaja de facilitar muchas tareas de nuestro diario vivir; como la comunicación, el negociar en internet, pagos virtuales on-line, automatizar muchas tareas o peticiones que se presenten en el trabajo o estudio, entre otras que nos hace llenar de comodidad en todo lo que debemos hacer; pero todo no es tan bueno como parece, estas actividades del mundo cibernético también tiene su peligrosidad y es que hay personas que la utilizan indebidamente y realizan actos ilícitos que son conocidos como delitos informáticos, como también hay individuos que a veces ni se dan cuenta de lo que hacen por desconocimiento; en este artículo se dará a conocer la importancia de la ética informática en los distintos ámbitos de la vida social para identificar y concientizar al ciudadano Colombiano sobre las consecuencias del uso indebido de la información y las tecnologías.

Palabras clave: Ética, Informática, Tecnología, Delito.

1. INTRODUCCIÓN

El mundo se ha transformado gracias a la tecnología, en especial a la de los computadores y las telecomunicaciones. Sin duda, esto ha sido un importante avance que ha beneficiado tanto al mundo empresarial como a las personas.

También existe un lado oscuro, y es el de los delitos informáticos: aquellos robos, suplantación de identidades, ataques maliciosos, robo de material confidencial y muchos otros que se cometen haciendo uso de la tecnología. La semana pasada se publicaron noticias en diferentes medios sobre el inusitado crecimiento de este tipo de delitos y de la vulnerabilidad que existe en todo el mundo ante ellos.

Hay que tomar medidas y precauciones para asegurarnos de que cada vez sea más difícil que nos ataquen por medio de vías informáticas. Vale advertir que la seguridad empieza por las personas. Si no se tiene conciencia clara de que hay hackers que están pendientes de fallas, omisiones, descuidos y otras debilidades que se presentan entre los ciudadanos y en empresas, nunca se podrá prevenir el estar en la mira de estos criminales. Es como si un ciudadano se pone a hablar por un iPhone 4S por la carrera 10a., en el centro de Bogotá, a las 9 de la noche, sin tener presente que muy seguramente puede ser atracado para robarle su celular. Esto es no tener conciencia de la seguridad.

Hay formas, difíciles de entender, usadas por los delincuentes informáticos para conseguir información que les facilite el hurto digital. Un ejemplo es el shoulder surfing o "navegación por el hombro". Es una táctica muy utilizada por los delincuentes para robar claves. Consiste en caminar por aeropuertos, cafés y restaurantes que ofrezcan Internet gratis y pararse detrás de una persona para ver si está accediendo a su cuenta del banco o algún sitio que le exija la clave. Así espían por encima del hombro del usuario y miran qué clave teclea.

Es difícil, por supuesto, estar al día con todas estas técnicas que utilizan los delincuentes informáticos, pero también será difícil ser víctima de este tipo de delitos si se tiene conciencia de que se debe navegar en forma segura, no dejar el computador abierto ni prestárselo a nadie por más amigo que sea-, tener claves difíciles de adivinar y cambiarlas con frecuencia, siempre con la conciencia de la seguridad informática y de las vulnerabilidades que muchas veces ofrecemos. Y si se es víctima, se debe consultar con un abogado antes de presentar la denuncia, porque muchas veces se formula con lo típico y normal, y muy pocas veces como el delito informático que se cometió.

(Santos Calderon, 2012, págs. 1-2)

Es muy importante conocer este mundo cibernético y no hacer caso omiso a la realidad que se vive por medio de este factor de tecnologías de información y las comunicaciones ya que se siente y se visualiza en este siglo xxi de la cual pertenecemos, en donde todo lo que percibimos se hace a través de este gremio de las comunicaciones, internet y sobre todo la vida socio-cultural de los seres humanos (redes sociales, e-mail, entre otras).

Se sabe que el cambio al mundo cibernético año tras año se va evidenciando, ha sido muy significativo porque en cuanto al manejo de la información y las tecnologías va avanzando ya que facilita muchas situaciones que hoy en día se resuelven fácilmente, mientras que años atrás no se contaba con esta agilidad frente los diferentes inconvenientes que resultaban no se podían atender de manera eficiente como por ejemplo: la búsqueda de información, procesos empresariales y gubernamentales, la comunicación entre personas sin importar la distancia en el mundo, el marketing de negocios, entre otras que va a la vanguardia del día a día por la necesidad requerida.

De esta manera la sociedad en general debe tomar conciencia frente a la ética de la informática porque toda esta situación que se vive desde las familias, tiene como consecuencia procesos que podría girar a un entorno muy drástico en cualquier vida de un ser humano que haga uso indebido a las tecnologías de información y las comunicaciones.

2. ÉTICA DE LA INFORMACIÓN

Según Capurro (2005), la definición de ética de la información se remonta aproximadamente a la década de 1970 cuando los equipos de computación comenzaron a utilizarse en el campo de la información de carácter científico-técnico, surgiendo incógnitas con respecto al almacenamiento y accesibilidad a documentos generados, localizados en bases de datos de tipo bibliográficas. Luego este concepto se amplió con el uso masivo de la Red Internet, por los problemas éticos generados.

En la actualidad la ética de la información comprende las interrogantes éticas relacionadas con el proceso de la digitalización, la comunicación de sus resultados y la utilización adecuada de la información generada. La ética de información trata todo lo relacionado con el uso y mal uso de la información, tales como, la propiedad intelectual, acceso a la información libre o restringida, censura, uso de información de las instituciones gubernamentales, la intimidad y confidencialidad, integridad de los datos, flujo internacional de información, entre otros. También, la ética profesional realiza el análisis de cómo se emplean los principios éticos a nuestras decisiones y acciones como profesionales de la información (Fernández, 2000).

En este mismo orden de ideas, la ética de la información puede concebirse como una teoría descriptiva y emancipadora bajo dos perspectivas históricas o sistemáticas, en la primera, analiza las diferentes estructuras y relaciones de poder que establecen la actividad informativa en las diversa culturas y épocas, mientras que en la segunda trata la crítica al proceso de relaciones morales en el campo de la información, albergando los aspectos individuales, colectivos y universales (Capurro, 2005).

Es importante señalar, que esta nueva disciplina, surge en los últimos años como multidisciplinaria del campo filosófico y científico, está dentro de los nuevos desafíos morales y éticos representados por la revolución digital y de la computadora. El uso de ésta ética no será útil para resolver los problemas específicos de la ética informática, pero tratará de mantener los principios morales que guiaran los procedimientos para resolver éstos, ya que las normativas, códigos profesionales de conducta, y las legislaciones para el uso de los equipos de computadores o de la información, están basadas en una ética filosófica.

Según Floridi (2000) la Ética de la Información, se ocupa de dos aspectos importantes, los cuales se indican a continuación:

- Problemas conceptuales que surgen en la aplicación de preexistir teorías, conceptos, normas tradicionales.

- Defensa del destino teórico en el campo de la moral, la deontología del estado moral de la entidad información, la metodología ética, el papel de la información en el razonamiento moral, la epistemología moral y las decisiones en los contextos dominados por las nuevas tecnologías y la epistémica de la responsabilidad. La pregunta principal, qué es bueno para una entidad informativa y para la infosfera «el ambiente de la información»

Cabe destacar, que el mismo autor señala la existencia de cuatro Leyes Morales de la ética de la información para garantizar el bienestar de cada entidad informativa y la infosfera:

- Nunca se tiene que producir entropía «ausencia de información semántica» en la infosfera.
- Debe prevenirse la entropía en la infosfera.
- Se tiene que eliminar la entropía en la infosfera.
- Se debe garantizar el bienestar, la cantidad, calidad y variedad de la información en la infosfera.

Estas cuatro leyes clarifican las grandes líneas de cómo pueden vivir las personas, como agentes responsables en la Sociedad de la información o post-información. A continuación se conceptualizan los principios que según Floridi (2000) adopta la ética de la información:

- **La uniformidad**: todo se procesa, se tratan los funcionamientos, cambios, acciones y eventos como procesos de información, pero el proceso no será tomado como tal, sino se seleccionará lo más significativo de la actividad.
- **La reflexividad de procesos de información**: cualquier proceso de información necesariamente genera y es responsable de la información.

- **La inevitabilidad de procesos de información**: la ausencia de información también es un proceso de información.
- **La uniformidad de ser**: una entidad es un paquete consistente de información, que puede nombrarse y la ética trata cada entidad como una entidad de información.
- **La uniformidad de agencia**: un agente es cualquier entidad, capaz de definir fenómenos para la producción de información y que puede afectar la infosfera. No todas las entidades de información son agentes.
- **La uniformidad de no ser**: no ser, es la ausencia o negación de cualquier información o lo que se denomina entropía de información, esta es una cantidad específica de desorden, degradación o aleatoriedad en un sistema de energía productiva de información, es el ruido.
- **La uniformidad del ambiente**: la infosfera es el ambiente constituido por la totalidad de las entidades, incluyendo los agentes, los procesos, sus conveniencias y relaciones.

Además, el ambiente de la información o infosfera, también posee propiedades, según Floridi (2000) son: consistencia, implementabilidad, ocurrencia, persistencia, estabilidad, seguridad, confidencialidad, integridad, exactitud, autenticidad y fiabilidad, entre otras.

Por otra parte, la ética de la información debe satisfacer cuatro propiedades para lograr sus objetivos, éstos son los siguientes:

- **Estabilidad**: la evolución de la tecnología ha significado una expansión rápida del ciberespacio, la sustitución de actividades realizadas por humanos por computadores o sistemas expertos y el impacto de las tecnologías de información y comunicación directamente es sobre los seres humanos.

- **Modularidad**: la ética se apoya en el razonamiento modular e incremental, los sistemas de información y los componentes del ciberespacio son productos complejos de ingeniería, por lo tanto, se debe modular éste.
- **Rigurosidad**: establecimiento de una teoría ética basada en un razonamiento riguroso.
- **Entereza**: debe haber un lugar en la ética de la información para la codificación de los valores, y permitir un análisis reflexivo para el estudio de casos típicos, ser legítima, excluir la trivialidad, ya que cada declaración se juzga para ser verdad.

Sin embargo, la ética de la información no es la última palabra en materia de moralidad, no proporciona un listado de soluciones a los problemas morales que surgen, pero puede mejorar la perspectiva y es lo más conveniente para la cultura informática de la organización y la sociedad de la post-Información. Esta ética mejora la comprensión de los hechos morales, mantiene el sentido del valor, la rectitud y las equivocaciones en las acciones humanas más intangibles y explicables, no solamente en nuestra vida personal sino también en las organizaciones. Además, proporciona una mejor visión y discernimiento no sólo de los problemas morales en su propio campo especial, sino también, de los fenómenos conceptuales y morales que forman el discurso ético, ampliando la perspectiva a la información y a su espacio lógico.

(Silva Neit & Espina, 2006, págs. 8-11)

Cabe destacar que el desarrollo tecnológico es prioritario para el mejoramiento continuo de las diferentes actividades y gremios que utiliza el sector empresarial y gubernamental; este abarca desde las familias hasta todo lo que nos podamos imaginar; es por esta razón que la ética informática juega un papel fundamental ya que la sociedad debe estar preparada para afrontar esta situación que acobija a toda la ciudadanía Colombiana y el mundo; hoy en día podemos observar que los niños desde los 2 años de nacido ya comienzan hacer uso de las tecnologías por medio de los teléfonos celulares y no se quieren despegar viendo, videos de YouTube y diferentes juegos que traen estos, pero esto no lo es todo, también en reuniones familiares, fiestas entre amigos y hasta en las jornadas laborales, se puede analizar que las personas están prestando más atención a sus dispositivos tecnológicos que a las mismas reuniones pero a qué conlleva esto? A qué, se debe culturizar la ética informática, que la sociedad pueda entender y comprender que las tecnologías son muy importantes pero que se debe saber utilizar y aprovechar.

3. EL DELITO INFORMÁTICO

El 5 de enero de 2009 el Gobierno Nacional sancionó la L. núm. 12731, mediante la cual fue adicionado un nuevo título VII bis al Código Penal (en adelante CP) de 2000 (L. 599 de 2000), denominado De la protección de la información y de los datos informáticos. La reforma al CP siguió parcialmente los estándares técnico-dogmáticos sugeridos por el Convenio de Budapest del Consejo de Europa (2003) contra la cibercriminalidad (Tít. I, art. 2°)2.

Los datos y de los sistemas informáticos" que los contienen, procesan o transmiten en forma automática. Con ello el legislador penal colombiano confirmó su deseo de garantizar la seguridad de las funciones informáticas propiamente dichas, en contra de ataques cibercriminales5, como figuras autónomas frente a los tipos penales tradicionales.

Una de las figuras ampliamente modificadas por esta ley fue el delito de acceso abusivo a sistema informático3. Tipo penal pionero en nuestro medio jurídico que inicialmente fue regulado por el art. 195 del CP4 —dentro del capítulo VII, título III, dirigido a castigar La violación de la intimidad, reserva e interceptación de comunicaciones, y que en esta oportunidad fue incluido en el art. 269A, dentro de las figuras que castigan especialmente "Los atentados contra la confidencialidad, la integridad y la disponibilidad de

1 Ley publicada en el Diario Oficial núm. 47.223 del 5 de enero de 2009.

2 Precisamente, la “Convention on Cybercrimen” (ETS. núm. 185/2003), consultada en lengua inglesa, en: http://conventions.coe.int/Treaty/EN/ Reports/Html/185.htm.

3 L. 1273 de 2009, art. 4°: “La presente ley rige a partir de su promulgación y deroga todas las disposiciones que le sean contrarias, en especial el texto del artículo 195 del Código Penal”. La ley hizo en este caso una derogatoria especial.

4 El CP, art. 195 decía así: “El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa”.

Respecto a los delitos informáticos contemplados antes de la reforma, y en particular sobre el acceso abusivo a sistema informático protegido con medida de seguridad, v. Posada Maya (2006b, pp. 23 y ss.) y Castro Ospina (2001).

Los datos y de los sistemas informáticos” que los contienen, procesan o transmiten en forma automática. Con ello el legislador penal colombiano confirmó su deseo de garantizar la seguridad de las funciones informáticas propiamente dichas, en contra de ataques cibercriminales5, como figuras autónomas frente a los tipos penales tradicionales.

Sin embargo, la evolución del mencionado art. 269A no ha sido pacífica. En efecto, el cinco de marzo de 2009, esto es, dos meses después de entrar en vigencia la “ciber-reforma”, el Gobierno Nacional sancionó la L. 12886 —mediante la cual se expidieron normas para fortalecer el marco legal que permite garantizar la reserva de la información derivada de acciones de “inteligencia y

contrainteligencia"— que, con evidente falta de planeación legislativa, revivió y modificó, en el art. 25, el invalidado art. 195 CP7 y derogó los arts. 4° y 269A adicionados por la reciente L. 1273 de 2009.

Para completar el diagnóstico, debe decirse que la L. 1288 de 2009 fue declarada inexequible

5 Este objetivo fue ampliamente ratificado en: República de Colombia, Departamento Nacional de Planeación, Consejo Nacional de Política Económica y Social. Documento Conpes No. 3701: "Lineamientos de política para Ciberseguridad y Ciberdefensa", Versión Aprobada (14 de julio), Bogotá, Ministerio del Interior y de Justicia (y otros), 2011. Consultado en:

https://www.dnp.gov.co/LinkClick.aspx?fileticket=

lf5n8mSOuM%3D&tabid=1260

6 Ley publicada en el Diario Oficial núm. 47.282 del 05.03.2009. La modificación más importante de la norma original consistió en eliminar la exigencia de que el sistema informático estuviera protegido con una medida de seguridad informática. También se modificó la punibilidad, esto es, se derogó la pena de multa progresiva en modalidad de unidad multa y se instauró la pena de prisión.

7 L. 1288 de 2009, art 195. Acceso abusivo a un sistema informático. "El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en pena de prisión de cinco (5) a ocho (8) años".

(Posada Maya, 2013, pág. 4)

La ley 1273 de 2009, establece y regula los delitos informáticos en Colombia, lo que indica que la irresponsabilidad del uso indebido de las tecnologías de información y las comunicaciones conlleva a tener problemas ilícitos con la justicia de tal forma que podría perder el derecho de la libertad condicional; por esto es mejor documentarse y conocer esta norma para no cometer delitos informáticos.

A continuación se dará a conocer la ley que regula el delito informático:

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 "Por medio del 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 tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según la Revista Cara y Sello, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos.

De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y "De los atentados informáticos y otras infracciones".

El capítulo primero adiciona el siguiente articulado (subrayado fuera del texto):

– 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 1000 salarios mínimos legales mensuales vigentes.

– 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 trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

– 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 1000 salarios mínimos legales mensuales vigentes.

– 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 1000 salarios mínimos legales mensuales vigentes.

– 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.

Al respecto es importante aclarar que la Ley 1266 de 2008 definió el término dato personal como "cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica". Dicho artículo obliga a las empresas

un especial cuidado en el manejo de los datos personales de sus empleados, toda vez que la ley obliga a quien "sustraiga" e "intercepte" dichos datos a pedir autorización al titular de los mismos.

– 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 1000 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.

Es primordial mencionar que este artículo tipifica lo que comúnmente se denomina "phishing", modalidad de estafa que usualmente utiliza como medio el correo electrónico pero que cada vez con más frecuencia utilizan otros medios de propagación como por ejemplo la mensajería instantánea o las redes sociales. Según la Unidad de Delitos Informáticos de la Policía Judicial

(Dijín) con esta modalidad se robaron más de 3.500 millones de pesos de usuarios del sistema financiero en el 2006[2].

Un punto importante a considerar es que el artículo 269H agrega como circunstancias de agravación punitiva de los tipos penales descritos anteriormente el aumento de la pena 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 si 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.

Es de anotar que estos tipos penales obligan tanto a empresas como a personas naturales a prestar especial atención al tratamiento de equipos informáticos así como al tratamiento de los datos personales más teniendo en cuenta la circunstancia de agravación del inciso 3 del artículo 269H que señala "por quien tuviere un vínculo contractual con el poseedor de la información".

Por lo tanto, se hace necesario tener unas condiciones de contratación, tanto con empleados como con contratistas, claras y precisas para evitar incurrir en la tipificación penal.

Por su parte, el capítulo segundo establece:

– Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239[3] 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 del Código Penal[4], es decir, penas de prisión de tres (3) a ocho (8) años.

– 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 1500 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[5] .
Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Así mismo, la Ley 1273 agrega como circunstancia de mayor punibilidad en el artículo 58 del Código Penal el hecho de realizar las conductas punibles utilizando medios informáticos, electrónicos ó telemáticos.

Como se puede apreciar, la Ley 1273 es un paso importante en la lucha contra los delitos informáticos en Colombia, por lo que es necesario que se esté preparado legalmente para enfrentar los retos que plantea.

En este sentido y desde un punto de vista empresarial, la nueva ley pone de presente la necesidad para los empleadores de crear mecanismos idóneos para la protección de uno de sus activos más valiosos como lo es la información.

Las empresas deben aprovechar la expedición de esta ley para adecuar sus contratos de trabajo, establecer deberes y sanciones a los trabajadores en los reglamentos internos de trabajo, celebrar acuerdos de confidencialidad con los mismos y crear puestos de trabajo encargados de velar por la seguridad de la información.

Por otra parte, es necesario regular aspectos de las nuevas modalidades laborales tales como el teletrabajo o los trabajos desde la residencia de los trabajadores los cuales exigen un nivel más alto de supervisión al manejo de la información.

Así mismo, resulta conveniente dictar charlas y seminarios al interior de las organizaciones con el fin de que los trabajadores sean conscientes del nuevo rol que les corresponde en el nuevo mundo de la informática.

Lo anterior, teniendo en cuenta los perjuicios patrimoniales a los que se pueden enfrentar los empleadores debido al uso inadecuado de la información por parte de sus trabajadores y demás contratistas.

Pero más allá de ese importante factor, con la promulgación de esta ley se obtiene una herramienta importante para denunciar los hechos delictivos a los que se pueda ver afectado, un cambio importante si se tiene en cuenta que anteriormente las empresas no denunciaban dichos hechos no sólo para evitar daños en su reputación sino por no tener herramientas especiales.

(Gandini, Isaza, & Delgado, 2018)

4. CONCLUSIONES

Las tecnologías de la información y las comunicaciones son muy importantes porque se ve en el diario vivir y es por esta razón que la sociedad en general debe tomar conciencia en el ámbito de la informática, ya que como vimos existe una normatividad en Colombia que regula este fenómeno mundial y estas son los delitos informáticos que se pueden cometer como cualquier otro delito; un ejemplo claro de comparación es el siguiente:

Si tú sales de la casa y caminas 10 cuadras, estás exento a peligro por mucho que hayan policías custodiando la ciudad; en este caso es el internet, en el momento que ingresas a navegar en internet, pues estás exento a cualquier tipo de peligro cibernéticamente y también hay policías en el mundo.

Se espera que con la ayuda de este artículo, la ciudadanía Colombiana se pueda concientizar en generar cultura con la ética informática para no cometer delitos informáticos.

5. BIBLIOGRAFIA

Acurio del Pino, S. (s.f.). *Delitos informáticos generalidades.* Obtenido de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Cuevas Moreno, R. (2006). *Ética de los negocios y la economía de la informática y la comunicación.* Contaduría y Administración UNAM. Obtenido de https://doaj.org/article/b70fdd36d54b483fb904aa2d5012ab1f

Ferruzola Gomez, E., & Cuenca Espinosa, H. (2014). *Cómo responder a un delito informático.* Ciencia UNEMI. Obtenido de https://doaj.org/article/42ad44aa7d864c08b80f7a6cdce69b41

Gachamá, F. (2009). *Hacker ético vs. delincuente informático: Una mirada en el contexto colombiano.* Inventum Ingeniería, Tecnológica e investigación. Obtenido de https://doaj.org/article/3f64e606a57d41b8a5230c7e56a91b9e

Gandini, I., Isaza, A., & Delgado, A. (2018). *Delta Asesores*. Obtenido de https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

Informática Forense Colombia. (12 de 03 de 2017). Obtenido de https://www.informaticaforense.com.co/delito-informatico/

MAYER LUX, L. (2017). El bien Jurídico protegido en los Delitos Informáticos. *Revista Chilena de derecho*.

Montaño, P. (2013). Delitos Informáticos. *Revista de derecho*.

Posada Maya, R. (2013). EL DELITO DE ACCESO ABUSIVO A SISTEMA INFORMÁTICO: A PROPÓSITO DEL ART. 269A DEL CP DE 2000. *Revista de derecho comunicaciones y nuevas tecnologías*, 4.

Quesada Jimenez, M. (04 de 03 de 2008). *Innovación y experiencias educativas.* Obtenido de https://psico.edu.uy/sites/default/files/etica_informatica.pdf

Reyes Cuartas, J. (2007). El delito informáticoi en Colombia. *Derecho penal y criminología*.

Ruiz, M. (21 de 12 de 2016). *El diario.es*. Obtenido de https://www.eldiario.es/hojaderouter/tecnologia/software/etica-deontologia-informatica-desarrolladores_0_593191114.html

Santos Calderon, G. (12 de 11 de 2012). El mundo de la tecnología el auge de los delitos informáticos. *El Tiempo*, págs. 1-2. Obtenido de http://usc.elogim.com:2586/vid/tecnologia-auge-delitos-informaticos-406202770

Silva Neit, & Espina, J. (2006). Etica informática en la sociedad de la información. *Revista Venezolana de gerencia*, 8-11.

Tacuma, T. E. (2017). ETICA INFORMÁTICA. *Revista Daena*.