

CRIMINALIDAD INFORMÁTICA EN COLOMBIA

Universidad la Gran Colombia

Jenny Paola López Avella

Código: 6000 811 435

Diplomado: Técnicas del Juicio Oral

¿La ley 1273 de 2009 un verdadero alto a los delitos informáticos en nuestro país?

JUSTIFICACIÓN DE LA PREGUNTA

Desde siempre a la tecnología se la ha dado valor de acuerdo a la necesidad de la sociedad por evolucionar y aumentar su nivel de bienestar; así por ejemplo, cuando el hombre tuvo la necesidad de comunicarse, surgieron los diferentes medios que hoy conocemos para ello, por mencionar algunos tenemos: la radio, el teléfono, la televisión, los periódicos, y la internet que hoy nos ofrece la posibilidad de permanecer comunicados y conectados con miles de servicios a través de las redes. Sin embargo, el hombre aparte de satisfacer sus necesidades ha buscado la forma de emplear el internet, el conocimiento, la información y los computadores, para cometer delitos que atentan o ponen en riesgo la vida y/o la dignidad de los individuos o del interés público.

Por lo anterior, dada la necesidad de prevenir y castigar este tipo de actos que como se mencionó en párrafo anterior, atentan contra la vida y/o la dignidad de los individuos o del interés público, se expidió la ley 1273 de 2009 que define y determina la sanción de los delitos informáticos, con el objeto de proteger la información y los datos personales.

Sin embargo resulta un poco inconsolable que aún cuando ya han pasado cinco años desde que se promulgó esta Ley, no se esté impartiendo su correcta aplicación por no saber interpretarla por desconocimiento en la materia, y más si tenemos en cuenta que para este tipo de delitos se han impuesto las sanciones económicas más altas de nuestro código.

RESUMEN

En el desarrollo de este trabajo, mediante el tipo de investigación descriptiva se definirá y hará claridad sobre lo que es un delito informático y un delito clásico consumado a través de medios informáticos ya que es allí donde se falla hermenéuticamente, luego se identificarán las características del delito informático, en seguida sus sujetos, posteriormente la clasificación que se les da en nuestro país, acto seguido las cifras de delitos informáticos en Colombia, a continuación se manifestará la normatividad jurídica aplicable, consecutivamente si existe o no jurisprudencia que abarque el tema y por último opiniones críticas y profesionales sobre el actuar de los delegados del Fiscal General de la Nación y de los operadores judiciales frente a la interpretación y aplicación de esta Ley y cuál sería el posible remedio a esta situación.

ABSTRACT

In this paper we define and make clear what is a cyber crime and a classic crime completed through computerized means , then the characteristics of computer crime will be identified , then their subjects , then the classification is given in our country thereupon cybercrime figures in Colombia , then the applicable legal regulations shall be revealed, consecutively if there is case law that addresses the issue and finally reviews and professional opinions on the actions of the delegates of the Attorney General's Office and the judicial officers against the interpretation and application of this Act.

PALABRAS CLAVE

Computador, conocimiento, datos, delito, información, internet, seguridad, tecnología.

KEY WORDS

Computer, know, dates, Crimes,information,internet, security, technology.

INTRODUCCIÓN

En la actualidad se ha vuelto una necesidad adaptarse a los nuevos avances tecnológicos, conocer el uso de las redes sociales, la tecnología, el internet, los buscadores, los teléfonos móviles dado que son herramientas que le han permitido a hombre desarrollar sus actividades sociales y laborales, pero al mismo tiempo su indebido o desprevenido ha generado riesgos para quienes los utilizan. Sin embargo, para algunas personas resulta difícil imaginar que se pueda atentar contra ellos sin la necesidad de empuñar un arma o ser agredidas virtualmente, cuando la realidad es que solo es cuestión de hacer un clic para que por ejemplo se genere un detrimento patrimonial en contra nuestra o resulte vulnerada nuestra imagen.

Con la ley 1273 sancionada por el congreso el 05 de enero de 2009 y por medio de la cual se complementó la Ley 599 de 2000 el 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"*, se buscó castigar a aquellos que cometieren atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos manifestado en el primer capítulo de nuestro código penal en los artículos 269 A a 269 H y quienes cometieren atentados informáticos y otras infracciones manifestado en el segundo capítulo en los artículos 269 I a 269 J. No obstante lo anterior, para algunos autores críticos sobre el tema, se ha venido interpretando erróneamente en gran proporción desde un plano clásico del derecho penal, en donde lo informático se vincula a uno de los bienes jurídicamente tutelados protegidos por la ley penal.

DESARROLLO DEL TEMA

1. EL DELITO INFORMÁTICO Y EL DELITO CLÁSICO INFORMÁTICO:

El Dr. Alexander Díaz García (redactor del proyecto de la ley 1273 de 2009) ha manifestado que aunque desconoce las razones, muchos delegados fiscales y Jueces de la Republica están juzgando equivocadamente los delitos

informáticos como delitos clásicos, situando al delito informático como una circunstancia de agravación con el objeto de aumentar la pena . El Dr. Henry William Torres, docente de la Universidad La Gran Colombia indica que este tipo de delitos:

“Tienen una estrecha relación con las actividades criminales que en primera instancia los diferentes tratadistas han tratado de encuadrar en figuras típicas de carácter tradicional, dado que muchos de ellos no constituyen una nueva categoría delictiva sino que son los mismos delitos que ya se vienen castigando, delitos contra las personas, el honor, la libertad, la seguridad pública, la nación tales como robo, hurto, fraude y falsedad. Pero no se puede negar que el internet, el conocimiento, la información, los computadores han originado nuevas conductas difíciles de controlar” ¹

Por lo anterior, con base en lo apuntes hechos por el ya mencionado redactor de la Ley 1273 de 2009 y demás doctrinantes, es necesario diferenciar entre lo que es el delito informático y el delito clásico informático para determinar en donde se halla la incorrecta interpretación de estos.

Así las cosas, para el Dr. Alexander Díaz el delito informático es aquel donde se hurta información y datos personales que están en un medio digital y el delito clásico informático se entiende como el ilícito consumado a través de medios electrónicos. El Dr. José Darío Salazar miembro del Senado de la República define los delitos informáticos como aquellos que atentan contra la seguridad y la privacidad de las personas. ²

A continuación se presentan dos casos a manera de ejemplo con el objeto de dilucidar la diferencia entre estas dos definiciones dadas por el experto en la materia:

- Andrea le envía un correo electrónico a Bibiana amenazándola para que esta le entregue \$ 5.000.000 a cambio de guardarle un secreto intimo: este no sería un delito informático en razón a que se pide dinero a Bibiana por lo que

¹ TORRES, H. (2002). "DERECHO INFORMÁTICO". Bogotá: Ediciones Jurídicas Gustavo Ibáñez Ltda. p 21-41.

² Programa "Senado en contacto Colombia y su gente" Canal Congreso.

estamos frente a una extorsión (delito tipificado en el artículo 244 de la ley 599 de 2000) hecha por un medio electrónico, pero no se configura como un delito informático. Es como si se hiciera esa misma amenaza por medio de una llamada o empleando cualquier otro medio. Suele confundirse erróneamente aduciendo que es un delito de extorsión informática cuando lo correcto es que es una extorsión clásica donde se usó un medio electrónico para su comisión.

- Carlos ingresa al computador de Diana y extrae su hoja de vida sin consentimiento y/o autorización de Diana, en este sentido sí estamos frente a un claro caso de delito informático, en razón a que se están violando los datos personales de Diana. Conducta que sería castigada con la sanción respectiva de la Ley 1273 de 2009.

2. CARACTERÍSTICAS DEL DELITO INFOMÁTICO:

Para el Dr. Julio Alejandro Téllez Valdés abogado e investigador de la Universidad Nacional Autónoma de México las principales características de los delitos informáticos son las siguientes:

- Son conductas criminales de cuello blanco: en razón a que solo personas que tienen cierto tipo de conocimientos relacionados con la materia pueden ejecutarlos.
- Son acciones ocupacionales: ya que muchas veces por su ubicación laboral se maneja información de carácter netamente confidencial.
- Son acciones de oportunidad.
- Provocan serias pérdidas económicas: en razón a quien las ejecuta casi siempre lo hace para beneficiarse económicamente.
- Ofrecen posibilidades de tiempo y espacio: en razón a que en unos pocos segundos y sin importar en qué lugar se encuentre se puede ejecutar. Para su realización no se requiere estar presencialmente.
- Son muchos los casos y pocas las denuncias en razón al poco conocimiento.
- Son muy sofisticados.
- Presentan grandes dificultades para su comprobación: en razón a que se requiere de conocimientos muy amplios en esta materia.

- En su mayoría son imprudenciales: es decir, sin intención de hacerlo.
- Ofrecen facilidades para su comisión a los menores de edad.
- Tienden a incrementarse cada vez más.

3. SUJETOS:

Para el INEI³ los sujetos que participan en la comisión de este tipo de conductas son el S. activo quien realiza toda o una parte descrita por la acción penal (poseen habilidades para el manejo de la informática) es el ya mencionado delincuente de cuello blanco y el S. pasivo que es la persona quien resulta vulnerada en su bien jurídicamente tutelado.

4. CLASIFICACIÓN:

De acuerdo al artículo *“Caracterización de los delitos informáticos en Colombia”* desarrollado por estudiantes del grupo semillero de investigación de la corporación universitaria de América (Barranquilla – Colombia), este tipo de delitos en nuestro país podrían clasificarse de la siguiente manera:

- Los que afectan el patrimonio económico: por ejemplo cuando se compra o vende a través de portales de compra, o se manifiestan falsos premios, páginas falsas.
- Las que buscan el abuso de menores: las que comercializan videos, fotografías.
- Las que afectan la propiedad intelectual: comercialización de obras sin pagar derechos de autor.
- Las que afectan la información como bien jurídico: Por ejemplo un empleado que usa su permiso para acceder a cierta información secreta de la empresa para la cual trabaja y la entrega a la competencia, robos de información privilegiada. O como lo señalamos anteriormente robar información personal.

³ INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA – PERÚ

Los tipos de delitos informáticos reconocidos por la Organización de Naciones Unidas son los siguientes:

1. FRAUDES COMETIDOS MEDIANTE MANIPULACIÓN DE COMPUTADORAS:

- Manipulación de los datos de entrada: Consiste en la sustracción de datos. Este no requiere conocimientos técnicos en informática por tal razón puede ser cometido por cualquier persona que tenga acceso a la información.
- Manipulación de programas: Para su comisión si requiere de conocimiento en la materia. Se le denomina “Caballo de Troya” Este consiste en modificar o insertar programa de forma encubierta en el sistema para que realice alguna función no autorizada y a su vez este pueda ser utilizado normalmente.
- Manipulación de datos de salida: Se realiza precisando un objetivo al funcionamiento del sistema informático.

2. FALSIFICACIONES INFORMÁTICAS:

- Como objeto: Cuando se alteran datos de los documentos almacenados en el computador.
- Como instrumentos: Se realizan falsificaciones de documentos en computador.

3. DAÑOS O MODIFICACIONES DE PROGRAMAS O DATOS COMPUTARIZADOS

- **SABOTAJE INFORMÁTICO:** Cuando se borran, suprimen o modifican funciones o datos del computador sin autorización con la intención de obstaculizar el normal funcionamiento del sistema, por medio de las siguientes técnicas, se hará una breve explicación de las mismas sin que ello implique mayor profundidad por ser de materia computacional por decirlo de alguna manera:

- **Virus:** para la Fundación GCF Aprende Libre⁴ son programas informáticos que tienen como objetivo alterar el funcionamiento del computador, sin que el usuario se dé cuenta. Estos, por lo general, infectan otros archivos del sistema con la intención de modificarlos para destruir de manera intencionada archivos o datos almacenados en el mismo.
- **Gusanos:** Es un programa cuya finalidad es la de ir consumiendo memoria del sistema, se copia así mismo sucesivamente, hasta que desborda la memoria RAM del computador.⁵
- **Bomba lógica o cronológica:** Requiere la programación de la destrucción o modificación de datos en un momento dado del futuro.

4. ACCESO NO AUTORIZADO A SERVICIOS Y SISTEMAS INFORMÁTICOS:

- ya sea por motivos de curiosidad como es el caso de muchos piratas informáticos que son aquellos que aprovechan las faltas de rigor de las medidas de seguridad. Este tipo de casos ocurren cuando se emplean contraseñas débiles.
- Reproducción no autorizada de programas informáticos de protección legal: En este el bien jurídicamente tutelado es la propiedad intelectual, por tal razón el Dr. Henry William Torres no lo considera un delito informático.⁶

⁴ Fundación Goodwill Community Foundation International Aprende Libre.
http://www.gcfaprendelibre.org/tecnologia/curso/virus_informaticos_y_antivirus/los_virus_informaticos/1.do. [recuperado: 09 octubre 2014].

⁵ RUBIO, Erika. "Cartilla informática". [en línea]. Recuperado el día 18 de septiembre 2014. [Disponible en : < <http://es.calameo.com/books/0015085588d21cf34bb0b>>

⁶ TORRES, Henry."Derecho Informático". Ediciones Jurídicas Gustavo Ibáñez Ltda. Bogotá. 2002. P 21-41.

5. CIFRAS

En el 2012 la revista semana publicó un artículo en el que señalaba que todos estos delitos según la presidencia del Colegio Colombiano de Juristas han tenido un incremento considerable, con base en las estadísticas con las que cuenta ese organismo y se permiten afirmar que "Colombia está en el tercer lugar en Latinoamérica, después de Brasil y México, en delitos informáticos" adicionalmente manifestaron que cada mes en el país se presentaron cerca de 187 denuncias por fraudes a entidades bancarias por cuentas de estas acciones delictivas.⁷

6. NORMATIVIDAD JURÍDICA APLICABLE

La normatividad jurídica aplicable para delitos informáticos en Colombia es la Ley 1273 de 2009 que complementó nuestro código Penal cuyo objeto busca castigar a aquellos que cometan atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos manifestado en el primer en los artículos 269 A a 269 H y quienes cometieren atentados informáticos y otras infracciones manifestado en el segundo capítulo en los artículos 269 I a 269 J, se tipificaron las conductas de:

- Acceso abusivo a un sistema informático: Cuando una persona accede sin autorización en un sistema informático.
- Obstaculización ilegítima de sistema informático o red: Cuando una persona impida u obstaculiza el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos o a la red.
- Interceptación de 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.

⁷ INSTITUTO NACIONAL DE ESTADÍSTICA INFORMÁTICA. Delitos informáticos. [en línea]. Lima – Perú. 2001. [fecha de consulta: 23 octubre 2014].Capítulo-III.Disponible en: <<http://es.scribd.com/doc/140203386/Libro-Delitos-Informaticos-INEI-pdf>>

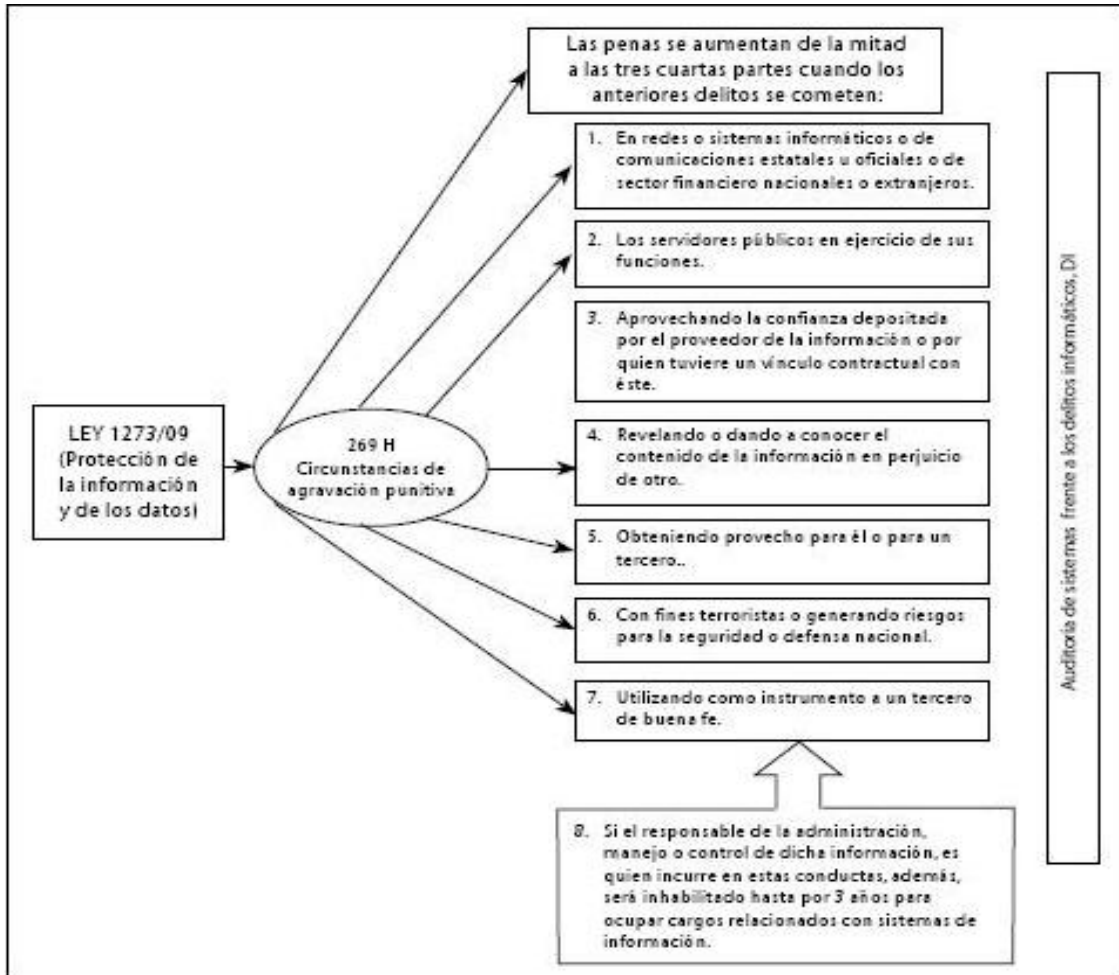
- Daño informático: Cuando una persona que sin estar facultada destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o cometa estos actos contra un sistema de tratamiento de información.
- Uso de software malicioso: Cuando una persona que sin estar facultada produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos
- Violación de datos personales (hacking): Orientado a proteger los derechos fundamentales de las personas como la dignidad humana, este tipo de delito se da cuando una persona no autorizada, obtiene, compila, sustrae, ofrece, vende y en general manipula códigos personales, datos personales, contenidos en ficheros, archivos, bases de datos o medios semejantes.
- Suplantación de sitios web para capturar datos personales: Cuando una persona no autorizada que diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes. Además las que modifiquen el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una página diferente, haciendo creer que es una página de confianza (por ejemplo ofreciendo empleos).
- Transferencia no consentida de activos: Cuando una persona con ánimo de lucro y valiéndose manipulación informática, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero.

		Se comete cuando	Penas
LEY 1273/09 (Protección de la información y de los datos)	269 A Acceso abusivo a un sistema informático	Aprovechan la vulnerabilidad en el acceso a los sistemas de información o debilidades en los procedimientos de seguridad.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
	269 B Obstaculización ilegítima de sistema informático o red de telecomunicación	Bloquean en forma ilegal un sistema o impiden su ingreso, igualmente, el acceso a cuentas de correo electrónico de otras personas, sin el debido consentimiento.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
	269 C Interceptación ilícita de datos informáticos	Obstruyen datos sin autorización legal, en su sitio de origen, en el destino o en el interior de un sistema informático.	Prisión de 36 a 72 meses vigentes
	269 D Daños informáticos	Cuando una persona que sin estar autorizada, modifica, daña, altera, borra, destruye o suprime datos del programa o documentos electrónicos y se hace en los recursos de TIC.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
	269 E Uso de software malicioso	Cuando se producen, adquieren, distribuyen, envían, introducen o extraen del país software o programas de computador que produce daños en los recursos de TIC.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
	269 F Violación de datos personales	Sin estar facultado sustrae, vende, envía, compra, divulga o emplea datos personales almacenados en medios magnéticos.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
	269 G Suplantación de sitios web para capturar datos personales	Crean una página similar a la de una entidad y envía correos (spam o engaños), como ofertas de empleo y personas inocentemente, suministran información personal y claves bancarias, y el delincuente informático ordena transferencias de dinero a terceros.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes

Auditoría de sistemas frente a los delitos informáticos, DI

Las circunstancias de agravación se encuentran consagradas en el artículo 269 H de la ley 599 de 2000, cuando el delito se comete en redes, sistemas informáticos y de comunicaciones del Estado o del Sector Financiero Nacional o Extranjero, cuando se origina o promueve por un funcionario público, o cuando se dé a conocer información confidencial en perjuicio de otro para

obtener provecho de propio o de terceros, cuando se actúa con fines terroristas para atentar contra la seguridad o Defensa nacional, o cuando se utiliza a un tercero de buena fe como instrumento.



7. JURISPRUDENCIA

Aunque hoy no hay jurisprudencia referente a este aspecto en razón a que es un tema reciente, para mitigar este flagelo la DIJIN – Área de delitos contra el patrimonio económico ha venido trabajando de forma preventiva: atendiendo las inquietudes de los ciudadanos y dando recomendaciones para no ser víctimas de los delincuentes informáticos y para ello creó un portal en internet⁸,

⁸http://www.policia.gov.co/portal/page/portal/UNIDADES_POLICIALES/Direcciones_tipo_Operativas/Dirccion_Seguridad_Ciudadana/Planes_de_Seguridad/Recomendaciones_de_seguridad/delitos_informaticos

investigativa: coordinando sus actividades con la Fiscalía y las autoridades competentes para recopilar el material probatorio y políticamente: participando en la promulgación y elaboración de proyectos de ley que permitan tipificar estas prácticas.

8) CONSIDERACIONES AL RESPECTO DE EXPERTOS EN LA MATERIA

El 13 de mayo de 2014 el Dr. Alexander Díaz Adujo en entrevista para foros el Espectador, que aunque en Colombia han sido castigadas un número considerable de personas bajo esta ley, no es un número significativo de éxitos para atacar efectivamente este delito, premisa que argumenta en que esto se da no porque no existan medios legales sino porque los operadores judiciales y los delegados del Fiscal General de la Nación no entienden muy bien la tipificación de la conducta informática porque tienden a tipificarla en los delitos clásicos y no en los nuevos que son los informáticos Art 269 A- 269 J de la Ley 599 del 2000.

Para sustentar el punto anterior se plantea el siguiente ejemplo, Eduardo y Helena eran pareja hasta hace seis meses, ya que Eduardo contrajo al tiempo un romance con otra mujer, Helena disgustada recordó que en su computador tenía algunos videos que se había realizado con Eduardo mientras sostenían relaciones sexuales, así que ella decide publicarlos en una red social con el objeto de vengarse. Este sería otro ejemplo de delito informático, no obstante para algunos Fiscales delegados y jueces estamos frente a un delito de injuria cometida a través de medios informáticos.

Además, la ley establece que a quien se le impute este delito no tendrá la posibilidad de modificar la medida de aseguramiento, por tal motivo no tendrían beneficios como el de prisión domiciliaria. Los delitos informáticos tienen la sanción económica más alta del Código Penal colombiano. La pena económica más baja está en 100 salarios mínimos mensuales legales vigentes, cerca de los 60 millones de pesos. La máxima puede llegar a los 600 millones de pesos, dependiendo del delito.

El Dr. Andrés Guzmán Caballero, experto en investigación forense e informática Director de la Unidad jurídica de ADALID compañía de América Latina con un portafolio diversificado que incluye tres marcadas líneas de negocio: Seguridad de la Información, Servicios Legales de Alta Tecnología y Sistemas Forenses, manifiesta su posición que coincide con la del Dr. Alexander señalando que "La legislación colombiana de delitos informáticos es suficiente, el problema es de conocimiento en la materia de parte de jueces, fiscales y organismos de policía judicial" y que "En Colombia no existen fiscales ni jueces especializados en delitos informáticos. Si a un ciudadano le roban el carro puede dirigirse a una Fiscalía especializada en Automotores, pero si a esa misma persona la roban en Internet debe dirigirse a un fiscal que en la mañana, por ejemplo, llevó un caso por inasistencia alimentaria"

CONCLUSION

La falta de conocimientos y experiencia en el manejo del área informática es un factor relevante a la hora de tratar de mitigar este tipo de delitos y es por esta misma razón que la creación de normatividad jurídica al respecto puede no tener los resultados esperados y más si se tiene en cuenta la incesante evolución de la tecnología que además de ser beneficioso para la sociedad hay quienes buscan emplearla para medios fraudulentos.

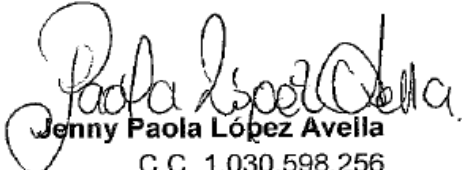
Además los operadores judiciales y los delegados del Fiscal General de la Nación deben interesarse y capacitarse en este tema ya que ellos son quienes ejercen como administradores de justicia.

REFERENCIAS

- ZULUAGA, Camila. *En busca de cura para los delitos informáticos*. El Espectador [en línea]. 13 de mayo de 2014. [fecha de consulta: 02 de octubre de 2014]. Disponible en: <<http://www.elespectador.com/noticias/politica/busca-de-cura-los-delitos-informaticos-articulo-492170>>.
- MARTÍNEZ, Jairo. *Colombia, el primer país que penaliza los delitos informáticos*. La Patria [en línea]. 30 de marzo de 2012. [fecha de consulta:

02 octubre 2014]. Disponible en: <<http://www.lapatria.com/tecnologia/colombia-el-primer-pais-que-penaliza-los-delitos-informaticos-1980>>.

- INSTITUTO NACIONAL DE ESTADÍSTICA INFORMÁTICA. *Delitos informáticos*. [en línea]. Lima – Perú. 2001. [fecha de consulta: 23 octubre 2014]. Capítulo-III. Disponible en: <<http://es.scribd.com/doc/140203386/Libro-Delitos-Informaticos-INEI-pdf>>
- Manjarrés, I & Jiménez, F. (2012). *Caracterización de los delitos informáticos en Colombia*. *Pensamiento Americano*, 71-82.
- PÉREZ, Camilo. *¿En Colombia se investigan los delitos informáticos?* Colombia Digital [en línea]. Colombia. 01 mayo 2011. [fecha de consulta: 18 septiembre 2014]. Disponible en: <<http://colombiadigital.net/actualidad/articulos/informativos/item/4810-en-colombia-se-investigacion-los-delitos-informaticos.html>>.
- TÉLLEZ, Julio. "Derecho Informático". Editorial MC Graw Hill. México. 1996
- ESCOBAR, Camilo. *El derecho preventivo en los delitos informáticos*. [en línea]. 04 septiembre 2014. [fecha de consulta: 18 de septiembre de 2014] Disponible en: <http://oiprodat.com/2014/09/04/el-derecho-preventivo-en-los-delitos-informaticos/>
- *Delitos informáticos han aumentado en Colombia, advierten especialistas*. *Semana* [en línea]. 11 de agosto de 2012. [fecha de consulta: 18 de septiembre de 2014]. Disponible en: <<http://www.semana.com/nacion/articulo/delitos-informaticos-han-aumentado-colombia-advierten-especialistas/267571-3>>
- TORRES, Henry. "Derecho Informático". Ediciones Jurídicas Gustavo Ibáñez Ltda. Bogotá. 2002.
- RUBIO, Erika. "Cartilla informática – Virus y vacunas". Calameo. [en línea]. [fecha de consulta: 18 de septiembre de 2014]. Disponible en: <<http://es.calameo.com/read/0015085588d21cf34bb0b>>


Jenny Paola López Avella
C.C. 1.030.598.256