

LEY 1273 DE 2009: ¿LOS JUECES DEL CIBER-CRIMEN?¹

Acuña-Gamba Eduardo José²

Sotelo-Vargas Diego Andrés³

Fecha de recepción: 10 de abril de 2015

Fecha de aprobación: 27 de agosto de 2015

Referencia para citación: Acuña, E. J., Sotelo, D. A. (2016). La política criminal en los menores adolescentes en Colombia. *Iter Ad Veritatem*, 14, 181-193.

1 Proyecto resultado de la investigación Delitos Informáticos en Colombia, perteneciente a la línea de investigación Derecho y Nuevas Tecnologías.

2 Estudiante de la Especialización en Derecho Administrativo. Universidad Externado de Colombia. Sustanciador Nominado. Juzgado Noveno Administrativo de Tunja. Correo electrónico: eduacu16@gmail.com.

3 Estudiante de la Especialización en Derecho Administrativo. Universidad Externado de Colombia. Abogado Litigante y Asesor. Correo electrónico: diegosotelo.abogado@gmail.com.

Resumen

El presente artículo es la reflexión de los autores respecto al desarrollo de la tecnología, ya que ha generado que las relaciones entre las personas y el Estado, en gran parte se vuelvan asimétricas, en el entendido de que el derecho no va a la velocidad con la que aparecen nuevas fuentes de riesgo en el mundo digital. Aunado a esto se hace difícil la capacitación del aparato Estatal, para dar una respuesta efectiva y garantizar los derechos de los asociados.

Sin embargo, en un esfuerzo por parte del Estado Colombiano se expide la Ley 1273 de 2009, que pretende dar respuesta al *ciberdelito*, pero que al revisarse desde la doctrina y el derecho comparado, se podrá vislumbrar la dificultad de la aplicación en el ámbito nacional, dando como resultado un desconocimiento o un mal ejercicio legal.

Palabras Claves: Derecho informático, Tics, Ciberdelito, Phishing, Sociedad de la Información, Seguridad Informática, Delitos informáticos.

Summary

This article is the reflection of the authors, about the development of technology, since it has not generated a cohesion between people and the State, which allows us to understand that the law is not speeding with the new sources of risk in the digital current world. In addition, the training of State Staffs is difficult, so that they can give effective responses that guarantee the rights of those involved.

However, on the part of the Colombian State the Law 1273 of 2009 was issued, that seeks to respond to cybercrime, but when it was reviewed from the doctrine and comparative law was found difficult to apply it at the national level, resulting a lack knowledge of those involved and wrong legal practice.

Keywords: Computer Law, ICTs, Cybercrime, Phishing, Information Society, Informatics Security, Computer Crime.

Résumé

Cet article est le reflet des auteurs par rapport au développement de la technologie, vu que ceci a généré que la relation entre les gens et l'État soit en grande partie asymétrique, étant entendu que le droit ne va guère à la même vitesse de nouvelles sources de risque qui apparaissent dans le monde numérique. Ajouté à phénomène, une formation de l'appareil d'État semble difficile pour répondre efficacement et de garantir les droits des partenaires.

Cependant, dans un effort de l'Etat colombien, il dresse la loi 1273 de 2009 qui vise à répondre à la cybercriminalité. Néanmoins au moment d'être révisé à partir de la doctrine et du droit comparé, il peut s'entrevoir la difficulté de l'application dans un cadre national, ce qui entraîne comme résultat une méconnaissance ou un mauvais exercice juridique.

Mots-clés: le Droit informatique – les TICE- la Cybercriminalité- le Phishing- la société de l'information-la sécurité- la cybercriminalité.

Introducción

Con la aparición de las nuevas tecnologías de la información, se han mejorado los procesos de producción, se facilitan los medios de comunicación, entre otras ventajas que en la actualidad no se podrían concebir de otra manera.

En la actualidad el mundo de las tecnologías de la información y comunicaciones (TIC) ha logrado traspasar las fronteras que separan o unen a todas las sociedades tanto centrales como periféricas, y que de una u otra manera nos hace sentir que en verdad nos encontramos frente a la globalización (Ruiz, 2011).

En este contexto, surgen nuevas formas de organización, acompañadas de nuevas estructuras de pensamiento. Por tal razón, existen preocupaciones frente a las nuevas exigencias de la sociedad de la información⁴, en la cual, esta desempeña un papel fundamental por la posibilidad de compartirla mediante la comunicación continua asombrando a la humanidad (Peres & Hilbert, 2009).

El concepto de la cibernética, se refleja en dos partes, por un lado se encuentra el hombre y por el otro la máquina, y su resultado es el dominio y uso del hombre frente a éstas, por tal razón las medidas tecnológicas tienen a un fin primordial y es aumentar la productividad, es aquí donde se presenta la relación de que la evolución del individuo que es análoga a la de la humanidad, y donde la tecnología desempeña un papel importante cuando se une con otras ciencias, ya que se podrían esperarse los mejores resultados (Sotelo Vargas. D., 2013, pp. 11-12).

4 El sociólogo Daniel Bell, introdujo la noción de la "sociedad de la información" en su libro *El advenimiento de la sociedad post-industrial*. Bell formula que el eje principal de la sociedad será el conocimiento y advierte que los servicios basados en él se convertirán en la estructura central de la nueva economía y la nueva sociedad. Con base en esto el autor señala, que ante este pensamiento se dio impulso a las tecnologías de la información y las comunicaciones (TIC's), con lo cual se promueve el ingreso a la sociedad de la información. La cual, ha permitido acelerar la instauración de un mercado mundial abierto y autorregulado (Bell, 1976).

Sin embargo, este avance ha generado grandes problemas para los estados, en la medida en que la legislación local se ve corta para enfrentar dichos problemas que son cada vez más frecuentes, y en muchos casos involucran a otros Estados, debido a que la conducta delictiva puede ser ejercida desde cualquier parte del mundo, aunado a esto la falta de cultura jurídica informática por parte del aparato judicial, toda vez que se ha preferido el uso de la tipificación tradicional frente a la legislación de nuevas tecnologías.

Esta investigación es necesaria, para verificar la eficacia de las normas jurídicas y la política pública, en relación con los delitos informáticos. Y posteriormente, tomar las medidas correspondientes, teniendo en cuenta la importancia de garantizar estos derechos en el contexto de la sociedad de la información: “Una vez más ha quedado demostrado que el cuestionamiento a la supuesta autonomía del denominado derecho informático, continúa en formación, no solo por la lógica antes expuesta sino por la escasez de investigaciones en esta rama” (Ríos Ferrer, Rolando Matos; Nadal, Rafael; Polo Maceira, Elena, 2009)

Problema

¿La actual política pública y normatividad en torno a los delitos informáticos cumple con los criterios de efectividad?

Justificación

En Colombia se han presentado las conductas delictuales por medio de las tecnologías más recientes, como lo son el uso de la computación y el internet, sin embargo el ordenamiento jurídico aún presenta falencias frente a este tipo de crímenes.

Por eso resulta de vital importancia el análisis que pretende realizar esta investigación, para verificar la efectividad que han tenido las regulaciones y como se han venido aplicando en el contexto nacional, a la luz de las exigencias actuales tanto legales como sociales.

Metodología

Se trata de una investigación descriptiva y documental, básicamente tendiente a determinar la formulación de un problema jurídico específico y que implica establecer si la actual política pública y normatividad en torno a los delitos informáticos cumple con los criterios de efectividad

Con el fin de dar respuesta, se realizará una revisión de la doctrina nacional y comparada sobre el tema.

1. Avances y Resultados

1.1 La importancia de la sociedad de la información

La sociedad de la información, provocó en los últimos años grandes revoluciones, en los diferentes paradigmas enmarcados dentro del conocimiento, la tecnología, la innovación, la productividad y el mercado; siendo la tecnología uno de los elementos clave en los procesos de productividad que afectan el mundo de manera política, económica y social. (Quiroga, 2010). Sin embargo, también se deben tener en cuenta los nuevos peligros que se avecinan, y las nuevas modalidades de crimen que se establecen a partir de estas grandes transformaciones.

Estas tecnologías, tienen un principal rasgo, es que permiten que todas las personas (las que tengan acceso a internet), dispongan de inmensos volúmenes de información en internet, lo cual, ha propiciado el nacimiento de una nueva sociedad y economía del conocimiento, donde la generación de riqueza está en la producción de bienes y servicios.

La sociedad basada en el conocimiento, en el uso e importancia de las TICs en los procesos de producción, tiene como principal receptor de cambio a las organizaciones, ya que, deben acomodarse a la mundialización de la economía y a los nuevos mercados que abren estas tecnologías.

Dicho cambio organizacional, abre la puerta a que emprendedores creen empresas sin que en muchos casos tengan que aportar recursos extras al tiempo necesario para el desarrollo de las aplicaciones. Desde este punto de vista, se puede ver como una posibilidad interesante de creación de empleos, en Estados Unidos medio millón de puestos de trabajo se crearon bajo esta modalidad (Fundación Telefónica, 2013).

Por tal razón, una de las recomendaciones hechas en la Cumbre Mundial sobre la Sociedad de la Información (CMSI) de 2003 fue que los gobiernos deberían “proporcionar un acceso adecuado a la información pública oficial a través de varias fuentes de comunicación, fundamentalmente Internet.” (Consumers International, 2010). Ello con el fin de ofrecer innovación, producto de una gran variedad de información, que circula en la internet, y que, se transforma constantemente en manos de todas las personas que estudian y transforman estos contenidos⁵.

5 Aquí radica la principal diferencia entre la sociedad de la información que planteaba Daniel Bell y la sociedad del conocimiento, luego, las sociedades del conocimiento de la “era de la información” se distinguen de las antiguas por su carácter integrador y participativo legado por el Siglo de las Luces y la afirmación de los derechos humanos, la importancia que estas nuevas sociedades conceden a los derechos fundamentales (UNESCO, 2005).

Este proceso de transformación y mejora del conocimiento, se da en la diferencia entre datos, información y conocimiento, en donde: En primer lugar, los datos se definen como un conjunto de cifras, números, palabras, sonidos o imágenes, y su uso incluye las funciones de creación, manipulación, procesamiento y almacenamiento. En segundo lugar, la información son todos aquellos datos ordenados; es la disposición de los mismos en patrones y que tienen una interpretación y significado. Por último, el conocimiento es la aplicación y uso productivo de la información (Valhondo, 2003, por ejemplo, la creación de bienes y servicios que mejoren la calidad de vida de las personas). En tal sentido, se colige que la información es pasiva y estática y el conocimiento y la innovación son dinámicos⁶.

En ese sentido, consideramos que cualquier persona de una sociedad tiene acceso a una gran cantidad de información, se debe apropiarse de ella para así transformarla en conocimiento. El obstáculo, estriba en que las personas realmente se apropien de la información y puedan mejorar el conocimiento, ya que, si no se realiza el proceso de apropiación se frustra el resto del proceso de innovación⁷.

Además, para lograr el desarrollo de este proceso de producción de conocimiento, existen otras razones, que tiene que ver con derechos que van más allá de la mera libertad de opinión y expresión, para incluir áreas tales como la gobernanza democrática de los medios, la participación en la cultura propia, los derechos lingüísticos, los derechos a disfrutar de los frutos de la creatividad humana, a la educación, la privacidad, la asamblea pacífica y la autodeterminación. Se trata de cuestiones de inclusión y exclusión, de calidad y accesibilidad. Resumiendo, son cuestiones también de dignidad humana (Consumers International, 2010).

Sin embargo, estos derechos se deben conciliar con otros factores determinantes, como la infraestructura y la capacidad de proporcionar formación e integrar la tecnología en la vida social y el cuidado de los delitos que se pueden cometer por esta vía. En la medida que esto sea entendido, las posibilidades de poner las TIC al servicio del desarrollo serán mayores y su eficacia como herramienta de desarrollo más rotunda⁸, cuidando la seguridad por estos medios (Ministerio de Ciencia y Tecnología, 2003).

6 Para un análisis más profundo, acerca de la diferencia entre información, datos, conocimiento e innovación véase por ejemplo (Valdés, 2002) y (Nonaka & Takeuchi, 1999)

7 Además, para lograr el desarrollo de este proceso de producción de conocimiento, existen otras razones, que tienen que ver con derechos que van más allá de la mera libertad de opinión y expresión, para incluir áreas tales como la gobernanza democrática de los medios, la participación en la cultura propia, los derechos lingüísticos, los derechos a disfrutar de los frutos de la creatividad humana, a la educación, la privacidad, la asamblea pacífica y la autodeterminación. Se trata de cuestiones de inclusión y exclusión, de calidad y accesibilidad. Resumiendo, son cuestiones también de dignidad humana (Consumers International, 2010).

8 De igual manera, lo ha expresado la UNESCO cuando afirma que “en las sociedades del conocimiento emergentes se da efectivamente un círculo virtuoso, en función del cual los progresos del conocimiento producen a largo plazo más conocimientos, gracias a las innovaciones tecnológicas (UNESCO, 2005).

1.2 De los Delitos Informáticos

Dentro de las finalidades del Estado se encuentran la de respetar y velar por los derechos de los ciudadanos, razón por la cual, los Estados hacen su mayor esfuerzo por garantizarlos frente a las nuevas tecnologías, reconociendo así que es un fenómeno que trasgrede sus fronteras y debe ser revisado desde el punto de vista jurídico internacional.

Lo anterior, posibilita la creación de espacios jurídicos transnacionales que, en principio, brinden garantías y herramientas jurídicas que hacen más fácil la persecución de las nuevas conductas delictuales, que se presentan en el siglo XXI.

Por esta razón se crea el “Convenio de Ciberdelincuencia” del Consejo de Europa que se firma en noviembre de 2001 en Budapest y trae una clasificación de los delitos informáticos, organizados en los siguientes grupos. El primer grupo a saber son aquellos que hacen referencia a los Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

- Acceso ilícito a sistemas informáticos.
- Interceptación ilícita de datos informáticos.
- Interferencia en el funcionamiento de un sistema informático.
- Abuso de dispositivos que faciliten la comisión de delitos.
- Algunos ejemplos de este grupo de delitos son: el robo de identidades, la conexión a redes no autorizadas y la utilización de *spyware* y de *keylogger*.

En un segundo grupo se encuentran los delitos informáticos tales como:

- Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.
- Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.
- El borrado fraudulento de datos o la corrupción de ficheros algunos ejemplos de delitos de este tipo.

En el tercer grupo, nos encontramos con aquellos delitos cuyo contenido es el punto importante y que permite clasificarlos de la siguiente manera:

- Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

- Delitos relacionados con infracciones de la propiedad intelectual y derechos afines (Consejo de Europa, 2008).

Para ejemplificar este delito se puede hacer mención a la copia y distribución de programas informáticos, o piratería informática.

De igual forma, buscando criminalizar los actos de racismo y xenofobia cometidos por medios informáticos, se expide en enero de 2008 el “Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa” que versa sobre las medidas que se deben tomar en casos de:

- Difusión de material xenófobo o racista.
- Insultos o amenazas con motivación racista o xenófoba.
- Negociación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.

Si bien este convenio es la guía para que los países, realicen los ajustes a sus legislaciones o creen una especial,

No es sino hasta con la promulgación de la ley 1273 de 2009 que modifica el código penal, en su artículo 53 dando como agravante el uso de medios informáticos, electrónicos o telemáticos para la realización de conductas punibles, e incluye el capítulo “de la protección de la información y de los datos” como solución a esta problemática creando delitos como los siguientes: Obstrucción ilegítima de sistema informático o red de telecomunicación (Artículo 269B); Interceptación de datos informáticos (Art. 269C); Daño informático (Art. 269D); Uso de software malicioso (Art. 269E); Violación de datos personales (Art. 269F); Suplantación de sitios web para capturar datos personales (Art. 269G). En el capítulo segundo se incorporaron estos tipos penales: Hurto por medios informáticos y semejantes (Art. 269I) y Transferencia no consentida de activos (Art. 269J). (Sotelo Vargas, D., 2013, p. 21).

Siendo así, de los más comunes en Colombia el *Phishing*, que básicamente trata de suplantar la identidad de una empresa o persona con el fin de obtener información privada, tales como contraseñas, datos personales sensibles, en otros. En Colombia, se ha hecho evidenciable, que se hace más frecuente en el sector financiero, suplantando entidades bancarias a través de páginas web, que simulan las reales

Entre las características principales de este delito informático está que se puede cometer desde cualquier lugar del mundo, difícilmente se identifica al delincuente en flagrancia, y normalmente se efectúa por medio de redes delincuenciales, en las que cada persona tiene una tarea específica para lograr el robo de la

información y del dinero. Según Asobancaria, éstas redes o cadenas de fraude reparten el 90% del dinero robado entre los distintos miembros de la red, quedando solo un 10% como ganancia por sus acciones delictivas.

Para fortalecer la seguridad de sus clientes y evitar que el número de víctimas de *phishing* aumente, los bancos han diseñado distintos mecanismos de verificación, que van desde nombres de usuarios, claves y preguntas personales, hasta el uso de *tokens* que crean claves numéricas cada determinados segundos y, la posibilidad de inscripción de IPs fijas, desde las cuales se hagan todas las transacciones de manera segura” (Ministerio de Tecnologías de la Información y las Comunicaciones, 2013).

Frente al desconocimiento de la legislación actual, que busca proteger a los ciudadanos que hacen uso de los medios informáticos y que depositan la confianza en el uso del internet, se ha buscado generar consciencia en el ciudadano quien es el principal afectado, y que en esa medida debe tener la suficiente pericia para protegerse.

Para Kreiner⁹, la recomendación específica para los usuarios en Colombia es que siempre pongan el vínculo o URL completa en el navegador que utilicen, para ingresar a su banco. Esto le ahorrará inconvenientes. Si se tomaran en cuenta dichas recomendaciones, sería factible que se redujeran los casos que se presentan y que en el mejor de los casos llegan a manos de las autoridades para su debida judicialización.

Sin embargo, es frecuente que en los Blogs, Redes sociales, Foros, se realicen comentarios que puedan transgredir derechos de otras personas, como es el caso de Gonzalo Hernán López fue condenado a 18 meses de prisión y pagar una multa de 9,5 millones de pesos por insultar públicamente a otra persona, a través del espacio para la participación de los lectores en un artículo del sitio web del diario El País.

Esta pena ya ha sido considerada arbitraria y desproporcionada frente a la realidad que plantea el uso de Internet, al tiempo que confunde opinión con información. “Los comentarios en los foros tienen carácter de opinión y por ello se les aplican las reglas de la opinión: que no se puede aspirar a que lo dicho sea cierto o veraz y que tampoco debe ser imparcial”, dijo Pedro Vaca, director de la Fundación para la Libertad de Prensa a El Espectador, sobre este tema. Lo cierto es que, tras este fallo, se crea una jurisprudencia en la cual todas las

9 El experto también recomienda a los usuarios que cada vez que se realicen transacciones en línea:

- Se aseguren de que su sesión en el sitio web del banco esté completamente cerrada antes y después de realizar cualquier transacción.
- Revisen el saldo frecuentemente: Los defraudadores pueden cambiar las cuentas destinatarias y los montos de las cuentas, sin que la persona lo note.
- Se registren en los servicios para recibir alertas en su teléfono cada vez que se realiza una transacción bancaria. La mayoría de bancos lo prestan gratuitamente.

(Ministerio de Tecnologías de la Información y las Comunicaciones, 2014).

opiniones que se expresen en los espacios que destinen los sitios web para los comentarios de sus lectores podrán ser judicializadas si llegaran a nombrar cosas que no son ciertas de alguna persona. Así mismo, sienta un precedente que también podría aplicarse a redes sociales y servicios de mensajería. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2014).

Esto evidencia, el desconocimiento de la temática que se aborda por parte de los operarios judiciales, ya que no atienden al desarrollo jurídico internacional, como es el caso de Europa, quien ha desarrollado conceptos y leyes de gran impacto en favor de las libertades y derechos individuales que se tienen frente al uso de las tecnologías de la información, es por que en Colombia no se puede retroceder, en el entendido de que se crean las herramientas jurídicas como la ley 1273 de 2009, pero se tiene un conocimiento precario frente a lo que regula.

1.3 ¿La respuesta es una justicia especializada en delitos informáticos?

La capacitación de los operadores jurídicos es importante, para dar viabilidad a la Ley 1273 de 2009, ya que cada vez es más frecuente que se presenten este tipo de casos en el sistema judicial Colombiano.

“el vertiginoso incremento de las tasas de vulnerabilidades y formas de acceder a la información privilegiada contenida en sistemas informáticos advierte la necesidad de entrenar a los funcionarios de la rama judicial para enfrentar adecuadamente la investigación y el juzgamiento de los delitos en contra de las infraestructuras de computación y comunicación” (Segrera, Martha; Cano, Jeimy, 2010, p. 180).

Ya que el desinterés por parte de los operarios judiciales, demuestra en sus fallos, que tramitan conductas delictuales informáticas, por la tipificación tradicional lo que conlleva a consecuencias jurídicas diferentes, y en algunos casos más gravosas que otras, y muchas veces quienes atienden a la novedad de la temática “son ingenieros y no son abogados, y están más interesados en conocer sobre la legislación informática los ingenieros que los abogados.” (Díaz Alexander 2014).

Quien ha redactado el proyecto, que ahora es la ley 1273 de 2009, Díaz Alexander (2014) reconoce que no es la falta de tipificación de estas conductas, sino el desinterés por parte del aparato judicial ya que se ha “hablado con el Consejo Superior de la Judicatura sobre mecanismos para difundir información entre la rama al respecto”. El Abogado y juez Díaz, ha escrito un libro con el fin de que se pueda consultar por los diferentes operarios judiciales, sin embargo no se ha tenido respuesta por estos últimos, lo que es un hecho lamentable para la rama judicial y la administración de

justicia, “Esto pasa mañana y ya no se vuelve a hablar de delitos informáticos como si no existiera la gravedad del problema.”

Dejando claro que cuando no hay un acuerdo en torno al concepto de los delitos informáticos, fácilmente se entorpece el juzgamiento de los crímenes cometidos bajo esta modalidad”, pues en muchos de los casos los jueces se han inclinado por entender los delitos informáticos como una forma novedosa de cometer fechorías tradicionales. En consecuencia, muchos de estos delitos son procesados como crímenes tradicionales” (Segrera, Martha; Cano, Jeimy, 2010, p. 182).

Conclusiones

Vemos que el proceso de revolución de las tics, ha suscitado una serie de cambios a nivel político, económico y social. El uso intensivo de las tics, consideramos, es una herramienta para cerrar la brecha económica y social entre los países en desarrollo y los países desarrollados. Por tal razón, debemos diseñar políticas que promuevan el acceso a la información, además de construir canales de infraestructura que posibiliten este acceso.

Sin embargo, de nada sirve todos estos esfuerzos si no hay una efectiva protección para los ciudadanos que realizan actividades en la web, ya que este, es el destinatario final de la protección que pueda brindar la ley 1273 del 2009, y no reporta ninguna utilidad ni mejora toda vez que el sistema judicial frente a la temática es inoperante. Se presenta en el trabajo, que la legislación, si bien cumple con las exigencias Europeas, no es aplicada con la rigurosidad, debido a la falta de conocimiento por parte del aparato judicial.

No basta con la capacitación del aparato judicial, para enfrentar todo el tesoro de delitos informáticos, sino se realiza una transformación cultural previa (alfabetización digital) que prevenga la ocurrencia de tales delitos, aunado a esto,es vital para la protección de los derechos de los ciudadanos, la cooperación internacional, ya que es un fenómeno que suele transgredir las fronteras estatales y el lugar de afectación del bien jurídico no es el mismo desde donde se realiza la acción delictual.

En ese sentido, es tarea del Estado, llenarse de valentía y tomar las decisiones. Ello con el fin de, hacer frente a la modificación de la realidad social hecha por las TICS, luego estas aceleraron los procesos de globalización hacia una economía basada en el uso de la información y el conocimiento **Fuente especificada no válida**. Con los temas que vinculan la tecnología y el derecho, suele suceder lo mismo que con la hidra mitológica, que cortándole una de sus cabezas, rebrotan siete.

Referencias

Bell, D. (1976). *The comino of Pos- Industrial Society a Venture in social forecasting*. Harmondsworth: Peregrine.

Cano Martínez, Jeimy José. (Coord.). (2010). *El peritaje informático y la evidencia digital en Colombia: conceptos, retos y propuestas*. Bogotá (Colombia): Universidad de Los Andes.

Colombia. Ley 1273 de 2009. 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. Diario Oficial 47.223 de enero 5 de 2009.

Consejo de Europa (2001). Convenio sobre la Ciberdelincuencia de BUDAPEST Tomado el 3 de noviembre de 2014 http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF

_____ (2008) Protocolo Adicional al Convenio de Ciberdelincuencia Tomado el 13 de noviembre de 2014 http://www.plataformaong.org/conferencia/wp-content/uploads/2014/10/Protocolo_adicional_convencion_cibercrimen.pdf

Consumers International. (2010). *Acceso al conocimiento: Una guía para todos*. Malasia: Kuala Lumpur.

Díaz Alexander (2014). En busca de cura para los delitos informáticos. Tomado el 3 de noviembre de 2014 <http://www.elespectador.com/noticias/politica/busca-de-cura-los-delitos-informaticos-articulo-492170>

Fundación Telefónica. (2013). *La sociedad de la información en España 2012*. Barcelona: Ariel.

García de la Cruz, Juan Manuel. (2009). *Delitos informáticos*. Argentina: El Cid Editor.

Ministerio de Ciencia y Tecnología. (2003). *La sociedad de la información en el siglo XXI: un requisito para el desarrollo*. Madrid: Ministerio de Ciencia y Tecnología.

Ministerio de Tecnologías de la Información y las Comunicaciones (2013). *Phishing: ten Ciber ciudadanía y denuncialo*. Tomado el 3 de noviembre de 2014 <http://www.enticconfio.gov.co/index.php/delitos-informaticos-formadores/item/892-phishing-ten-ciberciudadoy-denuncialo.html>

_____ (2014). *Comentarios en Internet: ¿Opinión o Información?* Tomado el 8 de noviembre de 2014 <http://www.enticconfio.gov.co/index.php/delitos-informaticos-formadores/item/1118-comentarios-en-internet-¿opinion-o-informacion?.html>

_____ (2014). ¿Cómo actúan algunos Ciberdelincuentes? Tomado el 7 de noviembre de 2014 <http://www.enticconfio.gov.co/index.php/delitos-informaticos-formadores/item/1106-¿cómo-actúan-unos-ciberdelincuentes?.html>

Nonaka, L., & Takeuchi, H. (1999). *La organización creadora del conocimiento*. D. F. México : Oxford University Press.

Quiroga, D. P. (2010). *La revolución de las tecnologías de la información y la gestión del conocimiento*. En D. P.

_____ *La gestión del conocimiento y las tecnologías de la información y la comunicación en las organizaciones* (pp. 29-63). Cali: Universidad Autónoma de Occidente.

Ríos Ferrer, Rolando; Matos Nadal, Rafael; Polo Maceira, Elena (2009). *Las categorías derecho informático y delito informático: su dimensión socio-económica en el nuevo marco empresarial cubano*. Argentina: El Cid Editor.

Sotelo Vargas, Diego Andrés. (2013). “*El Habeas Data en las redes sociales online: Responsabilidad y vigilancia*”, Bogotá. En: Revista *Dissertum* edición VI. Universidad de La Sabana, pp. 11–30.

UNESCO. (2005). *Hacia las sociedades del conocimiento*. Paris: Jouve Mayenne France.

Valdés, L. (2002). *La re-evolución empresarial del siglo XXI*. España: Norma.

Valhondo, D. (2003). *Gestión del conocimiento, del mito a la realidad*. Madrid: Díaz de Santos.

Vilaseca, J., & Torrent, J. (2005). *Principios de economía del conocimiento: Hacia una economía global del conocimiento*. España: Ediciones Pirámide.