Justicia Juris, ISSN 1692-8571, Vol. 8. Nº 1. Enero - Junio 2012 Pág. 75-83

El crimen on-line. Una mirada a la responsabilidad del proveedor de servicio de Internet

The Crime On-Line A look at the liability of the Internet Service Providers

MILLER SOTO SOLANO

Abogado, Magíster en Gestión e innovación de la Administración Pública, Magíster en Dirección de la Hacienda Pública y Doctor en Derecho y Economía de La Empresa de La Universidad de los Estudios de Verona –Italia-. Docente de la Universidad Autónoma del Caribe
miller.soto@uac.edu.co

Recibido: Septiembre 25 de 2011
Aceptado: Febrero 17 de 2012

RESUMEN

Internet es, sin lugar a dudas, el más grande avance tecnológico de la humanidad. Su arribo constituyó un suceso positivo que mejoró la calidad de vida del mundo contemporáneo. Sin embargo, no todo ha sido positivo en torno a la red informática; Internet es un escenario en el cual se pueden desarrollar actividades tanto lícitas como ilícitas. El presente artículo pretende, después de un análisis general sobre la problemática relativa a la criminalidad cibernética, realizar una reflexión relacionadas con el grado de responsabilidad o de irresponsabilidad de los proveedores de acceso o de servicio por los delitos cometidos en la red informática. Sin soslayar, la evolución que en el campo internacional ha tenido el tema.
Palabras clave: *internet, red informática, criminalidad cibernética, delitos informáticos, cibercrimen*

ABSTRACT

Internet is the greatest technological advancement of humanity. Its arrival was a positive development that improved the quality of life of the contemporary world. However, not everything has been good around the internet, because it is a space that can arise both licit and illicit activities. This reflective paper attempt, after a general analysis of the problems related to cybercrime; reflect with respect to the degree of responsibility or irresponsibility of the Internet Service Providers for crimes committed on the network. Without ignoring, the ability to highlight the developments that in the international arena has been the subject of the Criminal Responsibility of Internet Service Providers.
Key words: *Internet, computer network, cyber law, computer crime, cybercrime*

La evolución tecnológica dio lugar al surgimiento de nuevas formas de conductas vulneradoras de derechos. Agresiones que deben ser contrarrestadas mediante mecanismos técnicos y jurídicos en grado de evitarlas y, en caso de su ocurrencia, capaces de atribuir responsabilidad y aplicar sanción a quien las causa.

No existe un ordenamiento jurídico nacional capaz de prever la totalidad de las implicaciones que derivan de esta constante evolución. Es obvio, pues el proceso evolutivo de la sociedad va adelante y, muchas veces, es el origen del ordenamiento jurídico que la regula.

No se puede negar el gran avance que constituye Internet y su impacto en la calidad de vida del mundo contemporáneo. Sin embargo, no todo ha sido positivo en torno a la red informática; Internet es un escenario en el cual se pueden desarrollar actividades tanto lícitas como ilícitas. A partir de su uso, pueden surgir acciones vulneradoras de derechos; agresiones sociales que conducen a la necesidad de reglamentar la conducta del usuario en una realidad cibernética que, si bien se ha convertido en un espacio de libertades, no debe constituirse en un lugar gobernado por la anarquía y la ausencia de normas que garanticen su correcto desarrollo. Y es precisamente la ausencia de una entidad que la gobierne, lo que hace de Internet, un sistema, desde el punto de vista jurídico, incapaz de autoregularse.

> ...Muchos de los acontecimientos que tienen lugar en internet donde se vulneran derechos de terceros, no ocurren en los países donde los participantes o los servidores se encuentran físicamente. Por eso, para 'localizar' estos hechos, es común hablar del 'ciberespacio'. Así, Internet presenta características muy particulares y únicas donde no se cuenta con autoridad de Gobierno, donde existe un anonimato relativo, lugar donde no existen aduanas ni fronteras, que presenta un alcance mundial y posee acceso universal (Molina Quiroga, E. citado por Pinochet, F. 2010).

La criminalidad cibernética es un problema que ha venido aumentando conjuntamente con el ascenso de la población internauta[1]; ha sido objeto de múltiples iniciativas y estudios encaminados a buscar instrumentos jurídicos capaces de limitarla, gracias a ello, la red informática no es una realidad carente de normas, casi la totalidad de los países del planeta, ha abordado el problema del cibercrimen a través de acciones legislativas que, aunque intentan ser coherentes con la realidad interna de cada nación, no logran la coherencia global que un sistema tan complejo como Internet, requiere. Si se piensa, por ejemplo, en la posibilidad de que un individuo se lucre promocionando la prostitución en Italia (donde promocionar la prostitución es un delito) a través de una *"Web Site"* gestionada desde un país con el que Italia no tiene acuerdos de extradición, se podría entender dicha complejidad, que, tarde o temprano, tendrá que ser afrontada con medidas globales concretas tendientes a la creación de una normativa cibernética unificada en el contexto del derecho positivo global. Una regulación flexible, adaptable y aplicable en todos los rincones del planeta.

Evidentemente, las peculiaridades de la estructura y el funcionamiento de la Red informática modificaron un sinnúmero de esquemas valorativos con los que los juristas de tiempos pasados, estaban acostumbrados a operar.

> …La incidencia de los hechos, tal y como estamos acostumbrados a , sufre una auténtica revolución cuantitativa y cualitativa con la multiplicación exponencial que supone su difusión por la red; en un medio, además, en el que hablar de espacio sólo resulta posible si redefinimos el concepto mismo de espacio desde el que operamos..."(Guardiola García, J. 2003).

No es extraño, pues, encontrarse con la configuración de nuevas conductas delictivas, tanto en relación con el medio y el modo de cometerlas, como en lo concerniente al objetivo de las mismas. Si bien la informática trajo consigo nuevas concepciones en todos los ámbitos, incluido el penal, fue la cibernética la que produjo una revolución que nos llevó a redefinir conceptos con los que ya no era posible operar. En virtud de tal redefinición, surge el concepto de "ciberdelito" o "delito cibernético" como una de las categorías del -ya conocido- delito informático.

A pesar de las innumerables definiciones existentes de delito informático, todas coinciden en que se trata de una conducta punible que utiliza la informática como medio o como fin. Ésta importante diferencia entre medio y fin, ha traído como consecuencia una de las más comunes clasificaciones de los delitos informáticos, es decir, aquella que se desprende del papel que juega la informática en la conducta criminal, y que clasifica el delito informático con base a dos criterios:

1. **Como medio o instrumento:** es aquel delito mediante el cual el sujeto activo se vale de un elemento informático para su comisión. Se trata de una conducta criminal que se materializa con la utilización de métodos electrónicos, computadoras, etc. Un ejemplo de éste tipo de conducta criminal, es la falsificación de documentos mediante la utilización de impresoras computarizadas de alta resolución.
2. **Como fin u objetivo:** el delito que concierne a la informática como fin u objetivo, es aquella conducta criminógena que atenta contra el elemento informático (computadora, aparato electrónico, etc.). Se trata de un delito cuyo fin es dañar el objeto informático. Un ejemplo de esta categoría de delito, es el llamado sabotaje informático cuyo fin es dañar o alterar datos almacenados de forma computarizada.

Si se analiza detenidamente los criterios antes mencionados, se termina concluyendo que, a diferencia de la primera hipótesis, el delito cuyo fin u objetivo es el elemento informático, no requiere de la utilización del mismo. Con base

---

[1] Las Estadísticas de Usuarios Mundiales del Internet fueron actualizadas a Marzo 31, 2011. Según un estudio publicado por Internet World Stats, la población internauta mundial pasó de 360.985.492 usuarios en el año 2000 a 2.095.006.005 usuarios en marzo del 2011, presentándose un incremento del 480.4% (dichas estadísticas son propiedad intelectual de Miniwatts Marketing Group.). recuperado el día 16 de abril de *www.internetworldstats.com.*

a ese criterio, disparar, por ejemplo, con un arma de fuego a una computadora hasta dañarla, sería entonces un delito informático. De hecho, el Código Penal colombiano gracias a la modificación hecha mediante la Ley 1273 de 2009 a través de la cual se adicionó el Título VII BIS denominado "De la protección de la información y de los datos", así lo establece en el artículo 269D relativo al Daño Informático[2]. Tal disposición, teniendo en cuenta que el elemento informático tiene todas las características de un bien mueble, contrasta con el artículo 265 del mismo Código Penal relativo al daño en bien ajeno. Luego entonces, con la entrada en vigor de la Ley 1273 de 2009, se podría decir que el legislador colombiano introdujo -para efectos de la normativa penal- una nueva categoría de bien: "El bien informático". Pero, más allá de éstas curiosidades conceptuales que afloran a partir de la intención de tutelar un bien jurídico, surgen interrogantes: ¿Qué bien jurídico se pretende proteger? ¿El "bien informático" como una nueva modalidad de bien, o la información contenida en el mismo? La respuesta a tales preguntas, ameritaría, además de un análisis profundo de la relación existente entre el bien y la información, el estudio de la exposición de motivos y los fundamentos que dieron lugar a ésta nueva disposición. No obstante, se puede intuir que el legislador colombiano pretendió proteger una categoría de información: aquella contenida en ordenadores[3]. Pues si la intención del legislador hubiese sido proteger todo tipo de información, bastaría con romper una revista para incurrir en la conducta típica consagrada en el artículo 269D del Código Penal, antes mencionado.

Continuando con las clases de delitos informáticos, es pertinente resaltar que con la clasificación antes citada, coinciden la mayoría de los autores que han tratado el argumento. Algunos consideran delito informático sólo a aquella conducta que atenta contra los datos digitalizados y los programas informáticos contenidos en un sistema, es decir, lo que en la clasificación anterior hemos ubicado en la hipótesis de delito cuyo fin u objetivo es la informática. En cambio, aquellos en los cuales se utiliza la informática (computación, TICS, etc.) para cometer delitos estipulados en el Código Penal (como la estafa y la injuria), son llamados -por una parte de la doctrina- delitos computacionales. Sin embargo, a prescindir de los cambios en la denominación de la clasificación de delitos informáticos, hay una coincidencia sustancial en la materia. La de diferenciar el delito en el que se utiliza la informática como medio o instrumento, con el delito en el que la informática es el fin o el objetivo. A pesar de las coincidencias existentes desde el punto de vista sustancial, hay una clasificación de delito informático que está directamente relacionada con Internet y que no es tenida en cuenta en la categorización antes indicada. Se trata de establecer una diferencia entre aquellos delitos que se cometen mediante el uso del objeto informático conectado a Internet (On-line) y aquellos cuya comisión se configura a través de un elemento informático que, conectado o no a la red, prescinde de ella (Off-line). Tal diferencia, cobra relevancia a la hora de afrontar el tema, por ejemplo, de las responsabilidades que pueden ser atribuidas al proveedor de servicios de Internet por conductas delictivas cometidas por sus clientes (argumento que se tratará más adelante). De hecho, si se examina el Código Penal colombiano, se puede establecer, analizando el Título VII BIS "De la protección de la información y de los datos", que las hipótesis delictivas tratadas en todo el articulado del mencionado Título, pueden ser cometidas On-Line, y sólo algunas de ellas, pueden ser cometidas Off-line. Inclusive, existen conductas típicas cuya comisión se materializa única y exclusivamente a través de Internet. Un ejemplo de ello es la disposición establecida en el artículo 269G del Códico Penal:

> 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.

La comisión del delito consagrado en tal disposición, exige una conexión a Internet que requiere -necesariamente- de un objeto informático que sirva como puerta de entreada a la red. Y puesto que, no es posible hacer referencia a "Sitio Web" en un contexto que prescinda de Internet y de las herramientas necesarias para ingresar, resulta lógica la relación existente entre informática y ciberespacio. Una

---

[2] Código Penal Colombiano. 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.

[3] Recuerde que la Real Academia Española define informática como: Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores.

relación que, en el plano del cibercrimen, resulta -inexorablemente- dependiente. Dicho en otras palabras, un "ciberdelito" o "delito cibernético" será siempre un delito informático. Dicho esto, podemos establecer que el delito informático es susceptible de otro tipo de clasificación; aquella que deriva de su relación con Internet. O sea, el delito informático se clasifica en delito informático on-line y delito informático off-line.

Tal clasificación, no es ajena a la clasificación de delito informático aludida inicialmente. Recuérdese que un delito puede ser considerado informático porque utiliza la informática como medio o instrumento, o porque la usa como fin u objetivo. Pues bien, un "delito informático off-line" puede materializarse en cualquiera de los dos contextos, esté o no -el objeto informático- conectado a la red, y un "delito informático on-line", que siempre entrará en la categoría de delitos que utilizan la informática como medio o instrumento para su comisión, puede entrar -dependiendo de las circunstancias propias del delito- en el grupo de delitos informáticos cuyo fin u objetivo, es la informática. No se olvide que a través de Internet es posible cometer delitos tan tradicionales como la estafa, la injuria, la calumnia y, siendo posible la conexión a Internet de un respirador artificial, incluso el homicidio, entre otros.

Pero más allá de las complicaciones para determinar la clasificación de los delitos informáticos, resulta imprescindible tener claridad de conceptos a la hora de evaluar las circunstancias inherentes a cada hecho punible. Esto, en razón al asunto relativo a las responsabilidades. Puesto que, para determinar -por ejemplo- el grado de responsabilidad o de irresponsabilidad que eventualmente pudiera atribuírsele a un proveedor de servicio de internet, se hace necesario establecer que se está, precisamente, frente a un delito informático on-line, categoría de delito que bien puede denominarse "ciberdelito" o "delito cibernético" en virtud de las características del espacio en el cual se comete. Un espacio virtual que se conoce como "Ciberespacio" o "Espacio Cibernético".

Sobre "Ciberespacio" es pertinente traer a colación unas consideraciones sobre la naturaleza del término expresadas por Aguirre Romero, M (2004)

> **…**Aunque el término "Ciberespacio" provenga del mundo de la literatura de ficción -apareció en la obra de W. Gibson, Neuromante, en 1984 y allí es definido como una "alucinación consensual"-[4], lo cierto es que prendió pronto en el vocabulario popular para identificar una nueva realidad que estaba formándose poco a poco. Esta introducción indirecta de un término recogido de otro ámbito ha hecho que su aplicación no sea, muchas veces, lo suficiente precisa a la hora de manejarlo. Sin embargo, su implantación rápida muestra el grado de identificación obtenido por el término con la realidad a la que designa, aunque esta realidad esté por describir, definir y explicar.
>
> En otras ocasiones, se ha definido el ciberespacio como un espacio virtual de interacción, es decir, básicamente como un espacio-sistema relacional. A diferencia de otros tipos de espacios, que pueden ser utilizados para distintas funciones, pero que tienen una naturaleza física primaria, el ciberespacio surge directamente como un espacio relacional. Dos personas pueden encontrarse en un lugar y comenzar allí algún tipo de relación, pero ese espacio estaba ahí antes y seguirá después de que esa relación termine. El ciberespacio existe solamente como espacio relacional; su realidad se construye a través del intercambio de información; es decir, es espacio y es medio. Una red sin interacción entre sus miembros deja de ser una red; la red existe porque existen relaciones entre sus integrantes.

Esta realidad, de la que surge una -paradójicamente- llamada "realidad virtual", suscita nuevas realidades (no virtuales) como consecuencia de las nuevas formas de actividad criminal que se desarrollan al interior del ciberespacio. Si tenemos en cuenta, como lo hemos expresado anteriormente, que el "delito informático on-line" es una categoría de delito que necesariamente utiliza la informática como medio o instrumento, sea o no la informática su objetivo, podríamos determinar las hipótesis delictivas que componen lo que hemos denominado "criminalidad cibernética" o "cibercrimen". Sin embargo, al hipotizar acciones tipificadas en cualquier código penal y considerando la creciente influencia que el "mundo real" ejerce en el "mundo virtual", terminaríamos por concluir que casi la totalidad de los delitos, son susceptibles de ser cometidos on-line. A excepción de aquellos cuya materialización exija el contacto físico y real entre el sujeto activo y su víctima.

---

[4] William Gibson, W citado por Aguirre Romero, M (2004), en una entrevista realizada el 23 de noviembre de 1994 para el programa de la TV sueca Rapport, el escritor contestó a la pregunta sobre qué era el "Ciberespacio":
—What is cyberspace?
—Cyberspace is a metaphor that allows us to grasp this place where since about the time of the second world war we've increasingly done so many of the things that we think of as civilization. Cyberspace is where we do our banking, it's actually where the bank keeps your money these days because it's all direct electronic transfer. It's where the stock market actually takes place, it doesn't occur so much any more on the floor of the exchange but in the electronic communication between the worlds stock-exchanges.
So I think that since so much of what we do is happening digitally and electronically, it's useful to have an expression that allows that all to be part of the territory. I think it makes it easier for us to visualize what we're doing with this stuff.

Si se observa, por ejemplo, la clasificación de delitos informáticos consagrada en el "convenio sobre la ciberdelincuencia" firmado en Budapest, se puede notar -una vez más- que la denominación de la clasificación nada tiene que ver con la sustancia. Razón por la cual se hace necesario una lectura entre líneas que permita establecer e interpretar la categoría de delito informático, más por el contenido de la disposición, que por el nombre de la categoría en la cual se ha ubicado.

Con el objeto de fijar un marco de referencia en el ámbito de las tecnologías y los delitos para la Unión Europea, en noviembre del año 2001 se celebró en Budapest el "Convenio de Ciberdelincuencia del Consejo de Europa"[5]. En este convenio se propuso una clasificación de los delitos informáticos en cuatro grupos:

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, que comprende:

    - 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.

2. Delitos informáticos, que comprende:

    - 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.

3. Delitos relacionados con el contenido, que hace referencia a:

    - 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.

4. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines:

    - Un ejemplo de este tipo de delitos es la copia y distribución de programas informáticos, o piratería informática.

Luego, con la intención de criminalizar los actos de racismo y xenofobia cometidos mediante sistemas informáticos, en enero del año 2008 se promulgó un "Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa" mediante el cual se incluyó, entre otros elementos, las medidas a 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.

Finalmente, haciendo particular referencia al Título VII BIS (De la Protección de Información y de los Datos) del Código Penal Colombiano, se pueden señalar un número determinado de hipótesis delictivas que se analizaran a continuación.

El capítulo I referente a "Los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", presenta los siguientes delitos:

- Acceso abusivo a un sistema informático (artículo 269A). Consiste en acceder o permanecer, sin la autorización de quien tenga el legítimo derecho a excluirlo, dentro de un sistema informático protegido o no con una medida de seguridad.
- Obstaculización ilegítima de sistema informático o red de telecomunicación (artículo 269B). Consiste en impedir u obstaculizar el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.
- Interceptación de datos informáticos (artículo 269C). Consiste en intercepar, sin orden judicial que lo autorice, 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.
- Daño informático (artículo 269D). Se refiere a la destrucción, daño, borrado, deterioro, alteración o supresión de datos informáticos, sistemas de tratamiento de información o sus partes o componentes lógicos.
- Uso de software malicioso (artículo 269E). Consiste en la producción, trafico, adquisición, distribución,

[5] "The Convention on Cybercrime" o "Convenio sobre cibercriminalidad de Budapest" o "Convención sobre Delitos Informáticos" o "Convenio sobre ciberdelincuencia", es el único acuerdo internacional que cubre todas las áreas relevantes de la legislación sobre ciberdelincuencia (derecho penal, derecho procesal y cooperación internacional) y trata con carácter prioritario una política penal contra la ciberdelincuencia. Fue adoptado por el Comité de Ministros del Consejo de Europa en su sesión N. 109 del 8 de noviembre de 2001, se presentó a firma en Budapest, el 23 de noviembre de 2001 y entró en vigor el 1 de julio de 2004.

venta, envío, introducción o extracción del territorio nacional, de software malicioso u otros programas de computación de efectos dañinos.

- Violación de datos personales (artículo 269F). Hace referencia a la obtención, compilación, sustracción, ofrecimiento, venta, intercambio, envío, compra, interceptación, divulgación, modificación o empleo de códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, para beneficio propio o de un tercero.
- Suplantación de sitios web para capturar datos personales (artículo 269G). Ya citado con anterioridad, consiste en el diseño, desarrollo, trafico, venta, ejecución, programación o envío de páginas electrónicas, enlaces o ventanas emergentes, sin estar autorizado para ello.

Por otra parte, el capílo II (De los atentados informáticos y otras infracciones) del mismo Título VII BIS, consagra otros dos tipos penales:

- Hurto por medios informáticos y semejantes (artículo 269I). Hace referencia a la superación de medidas de seguridad informáticas, para realizar la conducta señalada en el artículo 239[6] a través de la manipulación de un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o la suplantación de un usuario ante los sistemas de autenticación y de autorización establecidos.
- Transferencia no consentida de activos (artículo 269J). Consiste en conseguir, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, la transferencia no consentida de cualquier activo en perjuicio de un tercero.

A prescindir del hecho que se trata de la inclusión de nueve tipos penales con los cuales el legislador -con la expedición de la Ley 1273 de 2009- quiso ponerse a tono con una realidad que en el contexto internacional ya había sido afrontada por muchos países, no deja de ser notable la intención. Sin embargo y a la luz de los hechos que en el ámbito global se han presentado desde los primeros años del advenimiento de Internet, no podemos desconocer que en lo que concierne a la normatividad relativa a criminalidad cibernética, Colombia está en pañales. Especialmente, en lo referente al tema de la responsabilidad de los Proveedores de Servicio de Internet.

El último intento del legislador por afrontar el tema relativo a la responsabilidad de los Proveedores de Servicios de Internet, se vivió por cuenta del Proyecto de Ley 241 de 2011 "Por la cual se regula la responsabilidad por las infracciones al derecho de autor y los derechos conexos en internet"[7]. Intento infructuoso en razón a que, después de seis meses de discusión al interior del Congreso, se tomó la decisión de archivarlo por falta de consenso en buena parte de los sectores de la opinión pública. Dicho Proyecto, que contenía disposiciones muy similares a la Ley Hadopi[8], consagraba -en el artículo segundo- una disposición inquietante (por decir lo menos):

> …Artículo 2. Régimen de responsabilidad. Los prestadores de servicio de Internet, los proveedores de contenido, y los usuarios serán responsables por el uso de los contenidos, de conformidad con las normas generales sobre responsabilidad civil, penal y administrativa.
>
> La información utilizada en sistemas o redes informáticas será protegida por la legislación sobre derecho de autor y derechos conexos si reúne las condiciones de tal protección.
>
> Tal redacción, considerando la precisión que debe caracterizar a cualquier disposición legal, resulta irresponsable en la medida que -haciendo referencia al régimen de responsabilidad civil, penal y administrativa- no se puede, sin más especificidad, reputar responsable a nadie (mucho menos al usuario) por el "uso de los contenidos" sin determinar el tipo de contenido y las circunstancias inherentes al uso del mismo.
>
> No obstante los tropiezos que -justamente- tuvo el Proyecto mencionado, se evidencia una necesidad por parte de la política, de establecer disposiciones tendientes a regular el tema de las responsabilidades propias de la red que, se espera, no constituyan un

---

[6] Código Penal colombiano, Articulo 239. Hurto. El que se apodere de una cosa mueble ajena, con el propósito de obtener provecho para sí o para otro, incurrirá en prisión de treinta y dos (32) a ciento ocho (108) meses.
La pena será de prisión de dieciséis (16) a treinta y seis (36) meses cuando la cuantía no exceda de diez (10) salarios mínimos legales mensuales vigentes.

[7] Proyecto de ley apodado "Ley Lleras" en razón a que fue radicado por quien entonces era el Ministro de Justicia (Germán Vargas Lleras). Se presenta como una exigencia del Plan Nacional de Desarrollo 2010-2014 y de los tratados de libre comercio con Estados Unidos y la Unión Europea.

[8] "La Ley Hadopi, también llamada Ley Creación e Internet, o, de manera más formal, Ley promotora de la difusión y la protección de la creación en Internet, es una ley francesa que pretende regular y controlar Internet para perseguir las infracciones de copyright. Esta ley también se ha dado a conocer como ley Oliviennes en referencia al autor del informe en el que se inspira la ley, Denis Olivennes, o como ley de los tres avisos o de la respuesta gradual.
Tras pasar por múltiples instancias del Estado (por orden, CNIL, Senado, Asamblea Nacional, Comisión mixta paritaria y de nuevo la Asamblea Nacional), el Consejo Constitucional censuró las medidas clave y la ley fue promulgada sin estas medidas el 12 de junio de 2009. La ley debía ser complementada por un nuevo proyecto de ley, que fue presentado al Consejo de Ministros el 24 de junio de 2009" Recuperado el 16 de abril de 2012 de http://es.wikipedia.org/wiki/Ley_HADOPI

óbice para la positiva dinámica de un mundo cuya principal característica es la libertad. Y, ciertamente, ese es el reto: lograr establecer un número determinado de reglas sin obstaculizar los aspectos positivos de la red.

Afrontar el tema de las responsabilidades de los proveedores de acceso o de servicio de internet (Access-Service Providers) generadas en el ámbito del cibercrimen, es una necesidad. Se trata de responsabilidades que, si bien no excluyen ni reemplazan la indiscutible responsabilidad del autor, deben ser objeto de un ponderado análisis que permita establecer específicas normas que regulen su función jurídica teniendo en cuenta que se trata de una pieza clave en el engranaje de la red con posibilidades técnicas de control sobre la información que en ella se difunde.

Antes de entrar en materia, es necesario hacer mención de un tema que, todavía hoy, genera polémica en el mundo jurídico: la responsabilidad penal de las personas jurídicas. Holanda fue uno de los primeros paises en reconocer dicha responsabilidad mediante el artículo 51 del Código Penal de 1976[9].

A pesar de que el reconocimiento de la responsabilidad penal en cabeza de personas jurídicas resulta contradictorio con la dogmática tradicional, muchos autores coinciden en afirmar que tal innovación constituye un instrumento eficaz en la lucha contra las diferentes modalidades de delitos económicos cometidos por las empresas. Y, aunque la mencionada responsabilidad de las organizaciones no excluye la responsabilidad atribuible a las personas físicas ni pretende promover la impunidad, no dejan de ser razonables las críticas que argumentan el deterioro del derecho penal individual a causa del surgimiento de la responsabilidad penal colectiva. De hecho, en América del Norte, donde la única procesada es la persona jurídica en la mitad de los procesos de derecho penal de la empresa, existen campos en los que la responsabilidad individual ha perdido importancia gracias al advenimiento de la responsabilidad penal de las personas jurídicas. Sin embargo, ello no se constituye en un debilitamiento de la responsabilidad individual, sino, por el contrario, la responsabilidad en cabeza de la organización viene a reforzarla debido a que obliga a las personas jurídicas a adoptar medidas organizativas tendientes a impedir la comisión de hechos delictivos. Bien se sabe que la empresa se encuentra en una posición de ventaja frente al Estado a la hora de controlar la conducta de sus agentes.

El derecho comparado permite entender, a través de la doctrina[10], las modalidades de imputación de responsabilidad penal de las personas jurídicas, que identifica tres modelos: el modelo de transferencia de responsabilidad que consiste en transferir a la organización la culpabilidad de la persona física que ha cometido la falta; el modelo de la culpabilidad de empresa, cuyos fundamentos de la responsabilidad se encuentran en factores inherentes a la misma; y el modelo mixto que reune las características de los dos modelos anteriores, es decir, inicia con la transferencia de responsabilidad y sucesivamente elige y gradúa la sanción de acuerdo a la culpabilidad de la empresa.

En el contexto de éste modelo mixto de imputación, se encuentra la teoría de la identificación. Tal teoría exige que la conducta ilícita haya sido cometida por un superior, y no por cualquier agente de la entidad. De esta forma, resulta suficiente que el superior haya autorizado, permitido o tolerado la comisión del delito, o incluso, que la infracción derive de un ejercicio deficiente de vigilancia.

En el caso de los Proveedores de Internet, cobra vital importancia el tema relacionado con la vigilancia. Las particularidades técnicas de estas organizaciones, conducen a pensar que son las únicas que poseen los instrumentos necesarios para detectar y, muchas veces, evitar la comisión de infracciones cibernéticas. La existencia de la Policia de internet (instituida por algunos paises), por ejemplo, se circunscribe más a un tema de autoridad que, a pesar de representar un factor positivo que lucha contra la impunidad, resulta inútil a la hora de evitar la comisión de tales conductas. No es como en la realidad Off-line donde un policía puede actuar en caso de detectar la intención de un individuo a punto de cometer un delito de tal forma que logre evitarlo. Las peculiaridades de la Red no permiten que la autoridad ejerza su función sino en un momento posterior a la comisión de la conducta delictiva. Es aquí donde el Proveedor de Servicio de Internet entra a jugar un papel preponderante en materia de prevención de la criminalidad cibernética.

Sobre el tema de la Responsabilidad de los Proveedores de acceso y servicio de internet, la legislación alemana del 22 de julio de 1997 sobre los servicios de información y comunicación, ofrece una solución con la cual está de

[9] El art. 51 del Código Penal Holandés prevé la punición de las personas jurídicas, pudiéndose en los casos de delitos cometidos por ellas llevarse a cabo el procedimiento penal en su contra, incluyendo la imposición de pena, o contra las personas físicas que han dirigido los hechos, o contra ambos, por lo que dice "el adagio en Holanda es, por tanto, Societas delinquere potest!". Indica que esta posibilidad de penar a las personas jurídicas ha llevado en Holanda a una persecución penal en delitos económicos o defraudatorios, no habiéndose suscitado ningún problema especial con la utilización del art. 51, pudiéndose multar a los entes ideales por una acción punible con un máximo de un millón de florines

[10] Gómez-Jara Diez, C., Gunther Heine y Laufer: "Modelos de auto responsabilidad penal empresarial, propuestas globales contemporáneas". Aranzadi. 2006.

acuerdo casi la totalidad de la doctrina italiana que, además, sirvió como modelo de las disposiciones contenidas en la Directiva europea 2000/31/CE. (Picotti, L., 383, 2000).

La responsabilidad del proveedor de servicio de internet requiere -para los fines penales- el efectivo conocimiento del material ilícito (por ejemplo, pornográfico) subido a la Red informática. "Elemento que tiene una importancia fundamental para evitar las tentaciones de recurrir al dolo eventual que podría reducirse a un simple *'Dolus In Re Ipsa'* y, por ende, a una presunción de dolo" (Manna A., 47, 1999). De éste modo, se limita la denominada posición de garantía que, por mandato legal de múltiples paises, deben asumir los proveedores de internet. El Proveedor de Internet no es siempre responsable por no ejercer el control dado que, desde el punto de vista técnico, resulta excesivamente complejo controlar todos los contenidos de sus usuarios. "En otras palabras, es altamente improbable que el Proveedor de Internet logre controlar los numerosísimos accesos en red, sobretodo, a la luz del derecho de anonimato de aquel ingresa el dato a la red". (Manna A., p.47, 1999) Por tal razón, la legislación alemana exige un presupuesto para establecer una obligación penalmente sancionada: la posibilidad técnica de control. Y, si bien parte de la doctrina considera que el proveedor de servicio de internet no debe ser excluido de eventuales imputaciones de naturaleza penal, tal inclusión debe considerar formas de responsabilidad dolosa de tipo concursal, y no de fugaces criterios de imputación subjetiva o ambiguas formas de dolo que ocultan conductas estructuralmente culposas.

A manera de conclusión

Finalmente, y antes de exponer una breve reflexión en torno a la enorme responsabilidad que tienen los proveedores de internet, es pertinente precisar que dicha responsabilidad, más que consistir en colocar a estas organizaciones en la mira del derecho penal como probables cómplices de los delitos cibernéticos, se hace necesaria en virtud de las características técnicas que poseen, para la prevención de una modalidad de crimen que, día a día, cobra más fuerza. En el caso de Colombia, se requiere una legislación que, con respecto a los Proveedores de Servicio de Internet, contemple la hipótesis de delitos omisivos impropios[11], a través de la expresa obligación jurídica de impedir un evento criminal. En el entendido, claro está, que es titular de una posición de garantía que podría verse limitada por razones técnicas.

Es cierto que el anonimato constituye un invaluable instrumento para la libertad de expresión. Sin embargo, ésta libertad generada por el desarrollo tecnológico y que ha dado origen a la red informática y a todas sus formas de articulación, ha hecho germinar nuevas formas de conductas ilícitas y comportamientos capaces de vulnerar derechos de todo tipo. Conductas y comportamientos que deben ser contrastados con la ayuda de instrumentos técnicos y jurídicos capaces de evitar o, al menos, de reducir su ocurrencia. Una tarea realmente difícil desde el punto de vista técnico, si se tiene en cuenta las características multiformes de un planeta que, en Internet, tiene el privilegio de encontrarse en un único espacio global. De hecho, diariamente se conocen nuevos aspectos de la red que evidencian el enorme potencial de crecimiento; un fenómeno de naturaleza global que impone la necesidad de reglamentar las dinámicas que en su interior se desarrollan. Una necesidad que debe mirar de manera especial a quien ofrece el acceso, a quien abre la puerta: El proveedor. Un actor que, por el hecho de tener las posibilidades técnicas para ser la autoridad de Internet, debería tener, además, las posibilidades jurídicas que le ofrezcan el poder de controlar y vigilar las dinámicas que en allí se desarrollan.

En síntesis, el tema de la criminalidad en internet supone una complejidad tal que amerita su estudio profundo y la creación de una regulación adecuada, que, en el caso de Colombia, no existe. Urge la necesidad de que el legislador colombiano empiece a llenar los vacíos que hay en materia de delitos informático y, muy especialmente, de los delitos cuya ocurrencia se materializa en internet. Ámbito en cual, los vacíos son aun mayores.

[11] Bien se sabe que el delito omisivo impropio, es aquel cuyo autor, a través de la omisión, facilita la materialización de una conducta penalmente relevante.

Referencias

Aguirre Romero, J. (2004) Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI, *Espéculo. Revista de estudios literarios*. Universidad Complutense de Madrid Recuperado el día 15 de abril de http://www.ucm.es/info/especulo/numero27/cibercom.html

Consejo de Europa (2001) Convenio sobre ciberdelincuencia, Noviembre 8 de 2001. Budapest.

Gómez-Jara Diez, C., Gunther Heine y Laufer. (2006) Modelos de auto responsabilidad penal empresarial, propuestas globales contemporáneas. Aranzadi, Pamplona, España.

Guardiola García, J. (2003).La responsabilidad penal de los prestadores de servicios de la sociedad de la información a la luz de la Ley 34/2002 y de la Directiva 2000/31/CE. *Revista de Derecho, Universidad de Valencia. No.2 de Noviembre de 2003* Recuperado el día 20 de abril de 2012 disponible en http://www.uv.es/revista-dret/num2/jguardiola.htm

Manna, A. (1999) *Perfiles problemáticos de la nueva ley en temas de pedofilia*. CEDAM, Milán.

Picotti, L. (2000) Fundamentos y límites de la responsabilidad penal de los proveedores de acceso y servicio en internet. *Revista de Derecho y Procesal Penal,* No.3. p. 383-384. Aranzandi, Verona.

Pinochet, F (2010*) La responsabilidad penal de los proveedores de acceso a Internet ISP.* Recuperado el día 20 de abril de 2012 disponible en http://www.elderechodeinternet.cl/blog/actualizaciones/laresponsabilidad-penal-de-los-proveedores-de-acceso-a-internet-isp/#_ftn1

República de Colombia, Código Penal Colombiano o Ley 599 de 2000.

República de Colombia, Ley 1273 de 2009.

Wikipedia Ley Hadopi, Recuperado el día 15 de marzo de 2012 de http://es.wikipedia.org/wiki/Ley_HADOPI