Semana económica

ASOBANCARIA

No. 693
Marzo 2 de 2009

Directora: María Mercedes Cuéllar
http://www.asobancaria.com
Editores: Jaime Alberto Gómez Mejía, Margarita Henao Cabrera, José Ramiro Sanín, Gina Alexandra Pardo, Javier Ojeda

LA LEY DE DELITOS INFORMÁTICOS: NUEVA HERRAMIENTA DE PROTECCIÓN DE LA INFORMACIÓN QUE IMPONE CONDENAS HASTA DE DIEZ AÑOS

Las últimas décadas han estado marcadas por un sostenido y creciente desarrollo de las tecnologías de la información, entendidas como "una gama amplia de servicios, aplicaciones, y tecnologías, que utilizan diversos tipos de equipos y de programas informáticos, y que a menudo se transmiten a través de las redes de telecomunicaciones"[1]. Ello ha llevado hacia un entorno de desmaterialización de los datos, que ha transformado el mundo.

En esta edición de Semana Económica se mostrará que, si bien los adelantos tecnológicos traen beneficios evidentes, estos implican nuevos riesgos que hacen necesaria la adecuación del sistema jurídico, como en buena hora se ha logrado en nuestro país, al expedirse la Ley 1273 de 2008. Esta reciente norma impone condenas entre tres y diez años de prisión y prevé, además, una circunstancia de agravación cuando se cometa cualquier delito utilizando medios informáticos.

[1] Plan Nacional de Tecnologías de la Información y las Telecomunicaciones.

Penetración de las tecnologías de la información

El número de usuarios de internet banda ancha alcanzó, para el cuarto trimestre del año pasado, 437 millones de personas en el mundo. En ese periodo Latinoamérica creció el doble del promedio mundial (8,32% frente a 4,15%)[2].

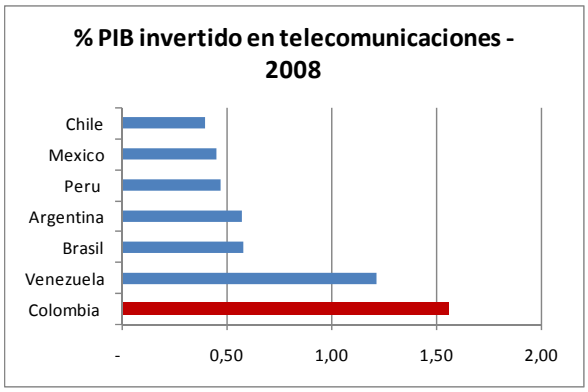
Colombia no ha sido ajena a la penetración de las tecnologías de la información. Los usuarios de Internet pasaron de 6.7 millones en diciembre de 2006 a 14 millones al terminar 2007[3]. Según el DANE, para este mismo año, el 29,7% de los hogares colombianos poseían computador, el 17,1% tenía acceso a internet y el 40,2% de las personas mayores de cinco años utilizó un computador por lo menos una vez al año.

Por otra parte, la Telefonía Móvil Celular y los Servicios de Comunicación Personal, alcanzaron una penetración[4] del 87,8%, lo que representa un incremento del 11,5% en la cantidad de líneas en servicio en 2008. Esto implica que el país está avanzando en el camino de la incorporación de Tecnologías de la Información y la Comunicación (TIC). El *World Cometitiveness Yearbook 2008*, señala a

[2] Vanier, Fiona. World broad Band Statistics Q3 2008. Diciembre 2008. Point Topic.
[3] Datos tomados del Plan Nacional de Tecnologías de la Información y las Telecomunicaciones.
[4] La penetración mide la densidad de telefonía móvil por cada 100 mil habitantes. Su calculo es (Número de líneas móviles/ Población)*100. Fuente: SIGOB

Colombia como la nación latinoamericana con mayor inversión en telecomunicaciones como porcentaje del PIB (gráfico 1).

Gráfico 1.



Fuente: World Cometitiveness Yearbook 2008, IMD. www.imd.ch

Un reto para el sector financiero

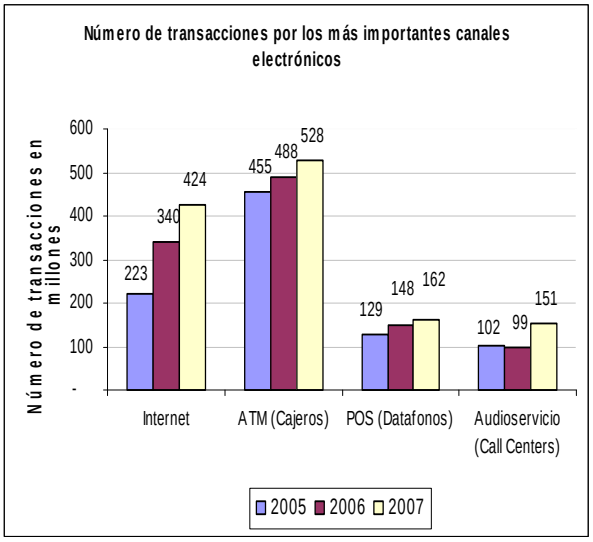
Los avances mostrados permiten el acceso más directo, abierto y libre a la información, lo cual ha sido aprovechado por una amplia variedad de sectores como la salud, la industria, e incluso por el gobierno, para la optimización de la prestación de los servicios y para el mejor relacionamiento con sus clientes. Todo esto se ha traducido en un cambio de costumbres sociales y empresariales, que son percibidas por el ciudadano como nuevas formas de interactuar y de administrar sus bienes.

El sector financiero no ha sido indiferente a estos cambios, por el contrario, ha sido uno de los sectores que más aplicaciones ha dado a los desarrollos tecnológicos e informáticos. En el gráfico 2 se muestra la aceptación y el alto crecimiento del uso de Internet y de otros medios electrónicos en la realización de operaciones financieras.

Las principales razones y ventajas para usar los medios y canales electrónicos están representadas en la reducción de los costos de administración del efectivo y los cheques, lo que les significa a los clientes disponer de facilidades, tales como mayor seguridad por no tener que manejar efectivo, y ahorro de tiempo asociado a los desplazamientos necesarios para hacer transacciones.

Además, en la medida que estos medios facilitan el desarrollo de la intermediación financiera, el mejoramiento de la transparencia en las transacciones y el mayor control de los flujos de fondos, las autoridades financieras los promueven con el propósito de reducir el riesgo sistémico y para proveer un mejor servicio a los clientes.

Gráfico 2.



Fuente: Asobancaria.

Si bien es cierto que los avances tecnológicos implican grandes facilidades en nuestra vida cotidiana, el carácter sensible de los datos que se transmiten y se reciben (de contenido íntimo o económico) exige un manejo cuidadoso y responsable, que garantice la seguridad y la integridad de la información, de manera que pueda consolidarse la confianza del público.

La seguridad de la información es un elemento clave para el desarrollo económico de una sociedad digital incluyente, lo cual sólo es posible con la utilización de sistemas sencillos y confiables. Esta es una de las conclusiones de la reunión de las Naciones Unidas sobre la Sociedad de la Información, realizada en Túnez en 2005.

No obstante, a pesar de las grandes ventajas del desarrollo tecnológico, este proceso no ha estado exento de

inconvenientes. Ha traído consigo el surgimiento y la transformación de las actividades ilícitas, con una amplia variedad de modalidades; en algunos casos las conductas se encaminan a causar un perjuicio a la plataforma que soporta un sistema informático, y en otros, la tecnología se convierte en el instrumento para la comisión de la conducta ilícita.

El reto que enfrentamos consiste en lograr combatir desde todos los frentes las figuras cada vez más complejas, que utilizan los "ciberdelincuentes". El esfuerzo privado por adaptar sistemas de seguridad, debe ser respaldado por las herramientas que la ley les otorga a los jueces, con las cuales puedan desarrollar eficazmente su función. No de otra manera el Estado podrá, como lo ordena la Constitución, proteger a todas las personas en su vida, honra, bienes y libertades.

Dentro de ese marco, las entidades bancarias han venido realizando enormes esfuerzos para mitigar los fraudes bancarios realizados por medios informáticos. Así, han desarrollado, constantemente, acciones de protección de los datos que manejan; definen protocolos y hacen verificaciones permanentes de la seguridad de sus sistemas de información; y realizan monitoreo sobre los links de su sitio web para que éstos no sean modificados ni se suplanten sus certificados digitales.

El riesgo de este tipo de fraudes no depende exclusivamente de la seguridad sobre sus propios sistemas, sino también de la vulnerabilidad que se presenta por prácticas inseguras de los clientes al realizar las transacciones. Al respecto los bancos han venido realizando trabajos importantes en materia de educación al cliente, a través, por ejemplo, de la ejecución de campañas informativas, en las que transmiten mensajes que permiten a los usuarios conocer y aplicar mejores prácticas en la utilización de medios electrónicos para realizar transacciones.

Instituciones como la Policía Nacional, la Fiscalía y el DAS han realizado esfuerzos significativos tendientes a enfrentar este problema, mediante la creación de unidades especiales de informática forense.

No obstante los avances señalados, estos se enfrentaban a la insuficiencia de herramientas legales que dificultaba judicializar las conductas criminales.

La falta de una regulación adecuada en estos temas era reconocida. En efecto, la dra. María Fernanda Guerrero en un artículo titulado "La Ciberdelincuencia: La ley patriótica y los efectos globales en las regulaciones nacionales y en particular en el caso de colombiano"[5] manifestó que:

"Parece que la inseguridad jurídica y la judicialización de derecho son las reglas generales en Colombia. No existe una normatividad adecuada para contrarrestar las conductas criminales en la Red incluyendo el ciberterrorismo y los ciberdelitos (delitos contra Internet (Virus), a través de Internet (acceso indebido) y por la Internet (Abuso de proveedores de servicios)). Por distintas causas, que ahora no se explican, en Colombia continúa imperando la impunidad, las estadísticas indica todavía la reiterada cifra negra y la atipicidad relativa en éstas materias continúa siendo el pretexto en el momento de subsumir la conducta en un tipo penal."

A lo anterior se sumaba el hecho de que, bajo el principio de legalidad, no se puede condenar a una persona si su conducta no está previamente definida como delito, de manera inequívoca, expresa y clara[6].

---

[5] Artículo ganador de "XV Concurso Nacional José Ignacio Márquez" sobre derecho económico, publicado en el libro Derecho de Internet y Telecomunicaciones". Universidad de los Andes. Editorial Legis 2003. Página 155.

[6] En relación con este tema, la Corte ha considerado que "*Es claro que en el artículo 29 el Constituyente de 1991 consagró de manera expresa el denominado principio de legalidad, "nullum crimen, nulla poena sine lege", principio tradicionalmente reconocido y aceptado como inherente al Estado democrático de derecho, sobre el cual se sustenta la estricta legalidad que se predica del derecho penal, característica con la que se garantiza la no aplicación de la analogía jurídica en materia penal, la libertad de quienes no infringen la norma, y la seguridad para quienes lo hacen de*

Por ello, destacamos de manera especial a los autores del proyecto de ley sobre delitos informáticos, los Honorables Congresistas Germán Varón Cotrino, Luis Humberto Gómez Gallo y Carlos Arturo Piedrahita, así como el acierto del Congreso al aprobar el texto de la 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."*

Esta ley constituye un gran paso para el país, ya que amplía la posibilidad de investigar y enjuiciar la ciberdelincuencia. La ley está compuesta de tres artículos; el primero adiciona al Código Penal, el Título VII BIS, denominado "*De la Protección de la información y de los datos*"; el segundo prevé una nueva circunstancia de agravación, relacionada con el uso de medios informáticos, electrónicos o telemáticos; y el tercero otorga a los jueces municipales la competencia para conocer de los nuevos delitos.

La ley establece tipos penales que buscan castigar los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. Así, se tipifican como delitos el acceso abusivo a un sistema informático[7]; la obstaculización ilegítima de sistema informático o red de telecomunicación[8]; la interceptación de datos informáticos[9]; el daño informático[10]; el uso de software malicioso[11]; la violación de datos personales[12]; el hurto por medios informáticos y semejantes[13] y la transferencia no consentida de activos[14].

Pero la ley no se queda en la tipificación de nuevos delitos. Establece una circunstancia de mayor punibilidad cuando para la realización de cualquier delito se

que la pena que se les imponga lo será por parte del juez competente, quien deberá aplicar aquella previamente definida en la ley." Sentencia C-739 de 2000.

[7] El que sin autorización o por fuera de lo acordado, acceda en todo o en aparte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de 48 a 96 meses, y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

[8] El que sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de 48 a 96 meses, y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, "siempre que la conducta no constituya delito sancionado con una pena mayor

[9] El que sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte, incurrirá en pena de prisión de 36 a 72 meses.

[10] 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 48 a 96 meses, y en multa de 100 a 1.000 salarios mínimos.

[11] El que sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, también incurrirá en pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos mensuales vigentes

[12] El que sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos.

[13] El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

[14] El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de 48 a 120 meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes.

utilicen medios informáticos, electrónicos o telemáticos[15].

Es de especial interés para la Asobancaria resaltar la importancia de esta disposición, que impone la aplicación de una pena mayor a aquellas personas que utilicen la tecnología para la comisión de conductas ilícitas. Por un lado, reconoce que su uso facilita consumar algunos delitos y, por otro, que el empleo de medios cibernéticos para fines criminales puede ocasionar efectos en masa e ilimitados.[16] [17]

Dentro de este contexto, el Ministro de Hacienda, en recientes declaraciones manifestó la importancia para el país, de disponer de herramientas adecuadas para adelantar investigaciones que permitan enfrentar rumores que circulan a través de correos electrónicos que pueden generar desconcierto entre la ciudadanía y que tratan de alterar el funcionamiento y la normalidad del sistema financiero.

Al respecto, el ministro destacó que el pánico económico constituye un delito que puede ser cometido mediante la circulación de correos electrónicos tanto por quienes originan las comunicaciones, como por quienes las retransmiten. Añadió que los organismos de seguridad tienen plena capacidad de adelantar las investigaciones necesarias para lograr individualizar a sus autores[18].

Consideraciones finales

La acelerada penetración de las tecnologías en la sociedad moderna presenta retos importantes en el manejo de la información, constituyéndose en elemento clave para el desarrollo económico de una sociedad digital incluyente.

Todos estos cambios generan una gran responsabilidad tanto para el Estado, como para la sociedad en general. Al respecto, las entidades bancarias han venido realizando importantes esfuerzos en la protección y seguridad en el manejo de su información y la de sus usuarios.

Sin embargo, constantemente se generan nuevos riesgos que deben mitigados de manera integral, no sólo desde un punto de vista técnico, sino también jurídico.

Es necesario que la legislación, la normatividad y las instituciones en general se adecúen rápidamente a los constantes cambios tecnológicos.

La Ley 1273 de 2009 constituye un gran avance en materia de seguridad informática, ya que mediante los nuevos tipos penales se facilitan las labores de judicialización y condena de los ciberdelincuentes.

Es importante resaltar que dicha ley, en la medida en que reconoce los perversos efectos masivos que puede ocasionar el empleo de la tecnología para fines criminales, dispuso de una nueva circunstancia de agravación de la pena.

Todos estos avances se tornan insuficientes si los ciudadanos no asumen el compromiso de dar un manejo responsable y cuidadoso a la información y a los instrumentos utilizados para la realización de transacciones electrónicas.

---

[15] "Artíiculo 2. Adiciónese al artículo 58 del Código Penal con un numeral 17, así: Artículo 58. *Circustancias de mayor punibilidad*. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera: (...)
17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos."

[16] Nelson Remolina. La obtención y comercialización ilegal de datos personales es un delito: Ley 1273 de 2009. Artículo publicado en www.eltiempo.com el 11 de enero de 2009.

[17] En este sentido, estudios como *Pew Internet and American Life* sugiere que el 92% de los usuarios de internet tienen, envían o leen correos electrónicos y el 56% lo hace cada día, lo que muestra la potencialidad de daño que puede generar.

[18] Declaraciones rueda de prensa sobre investigaciones por enviar falsos correos electrónicos sobre el sector financiero. Febrero 24 de 2009.