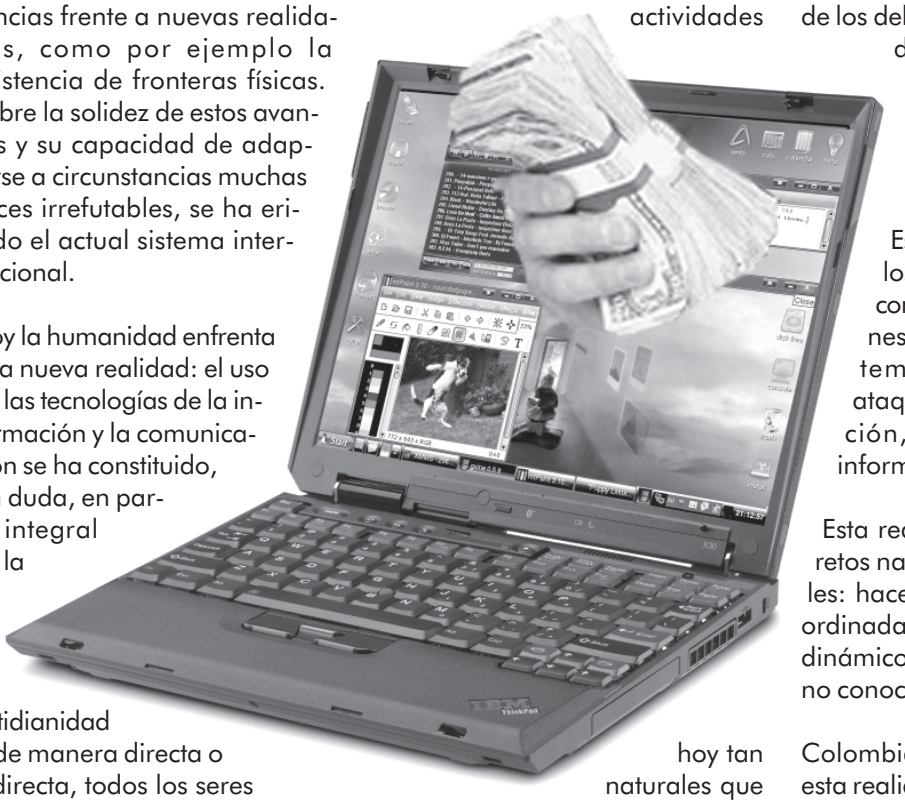
DELITO CIBERNÉTICO:
TEMA CLAVE DE SEGURIDAD EN LA AGENDA INTERNACIONAL

Por Daniel Andrés Cruz Cárdenas*

El derecho se ha desarrollado a través de la historia para brindarle herramientas a los seres humanos para dirimir sus diferencias frente a nuevas realidades, como por ejemplo la existencia de fronteras físicas. Sobre la solidez de estos avances y su capacidad de adaptarse a circunstancias muchas veces irrefutables, se ha erigido el actual sistema internacional.

Hoy la humanidad enfrenta una nueva realidad: el uso de las tecnologías de la información y la comunicación se ha constituido, sin duda, en parte integral de la cotidianidad y, de manera directa o indirecta, todos los seres humanos estamos relacionados con sistemas y datos informáticos. Recibir o enviar un correo electrónico, intercambiar información a través de cualquier medio de almacenamiento digital o efectuar una simple llamada telefónica, son actividades hoy tan naturales que no requieren mayor justificación.



Señalar el tipo de datos manejados por individuos y organizaciones sociales es una amplia labor: datos biográficos, fotografías, bases de datos oficiales, infraestructura crítica[1] para el funcionamiento de un país, entre muchos otros, son ejemplos de información con diferentes grados de sensibilidad en su uso.

Paradójicamente, los avances logrados por la humanidad en el campo técnico han ido de la mano del aumento de su uso por parte de los delincuentes, quienes día a día ingenian nuevas formas de cometer actos ilícitos en un entorno virtual de aparente anonimato e impunidad.

Es importante resaltar que los delitos cibernéticos son cometidos en tres dimensiones: a través del uso de sistemas informáticos, los ataques contra la información, o contra el sistema informático en sí.

Esta realidad plantea enormes retos nacionales e internacionales: hacer frente de manera coordinada a delitos pluriofensivos, dinámicos por naturaleza, y que no conocen barreras físicas.

Colombia no es un país ajeno a esta realidad: las autoridades nacionales enfrentan de manera cada vez más frecuente el acceso abusivo a sistemas informáticos, la suplantación de identidad con fines ilícitos, la estafa informática, la difusión de pornografía infantil a través de internet, seguido de un extenso etcétera.

En consecuencia, es de suma importancia avanzar en la consoli-

* Profesional en Gobierno y Relaciones Internacionales de la Universidad Externado de Colombia, candidato a Magíster en análisis de problemas políticos, económicos e internacionales contemporáneos del Instituto de Altos Estudios para el Desarrollo. Tercer Secretario de Relaciones Exteriores de la Carrera Diplomática y Consular de Colombia.

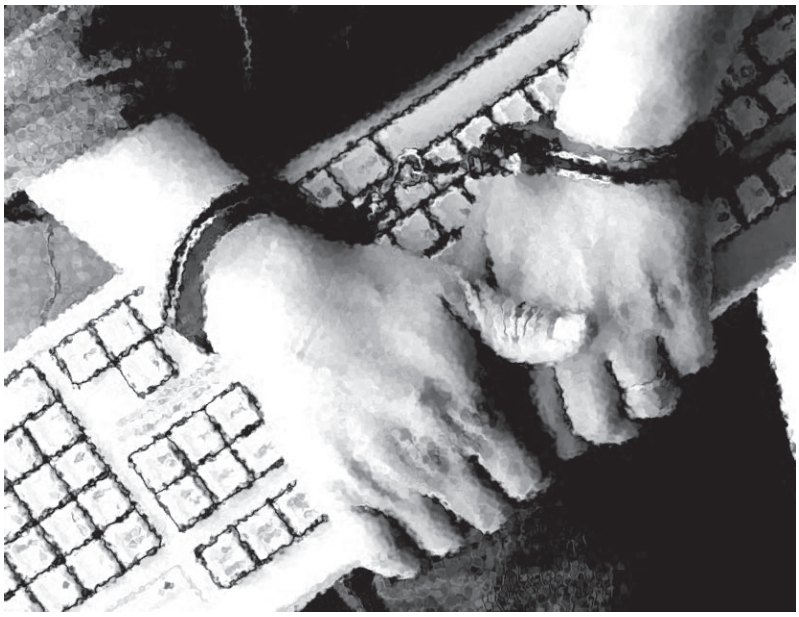
Paradójicamente, los avances logrados por la humanidad en el campo técnico han ido de la mano del aumento de su uso por parte de los delincuentes

dación de una política nacional contra la ciberdelincuencia acorde con las tendencias internacionales, atendiendo las necesidades del sector público, el sector privado y los aportes de la academia, y que gire en torno a la prevención, atención y judicialización del delito.

Esto implica generar una conciencia social sobre los riesgos potenciales del uso de sistemas informáticos sin las medidas de seguridad necesarias, continuar fortaleciendo las capacidades técnicas en la respuesta efectiva contra el delito, dotar las entidades públicas de sistemas confiables para el almacenamiento y manejo de información sensible, entre otros aspectos.

Sin duda uno de los principales retos es la adopción y adecuación de la legislación nacional en la materia, ardua labor que requiere considerar la seguridad en el ciberespacio en el lugar donde debe estar: un asunto de seguridad nacional. Basta con imaginar los efectos de un bloqueo al sistema financiero de un país o a cualquier servicio público para dimensionar la potencialidad de estos actos. No en vano en el escenario internacional el delito cibernético cobra espacios, y términos como "ciberterrorismo" son de uso más frecuente.

La Organización de Estados Americanos –OEA, mediante la adopción de la Estrategia Integral para Combatir las Amenazas a la Seguridad Cibernética en 2004, ha instado a los Estados del hemisferio a avanzar en tres dimensiones: el fortalecimiento de los instrumentos jurídicos necesarios para proteger a los usuarios de Internet y las redes de información



de los delincuentes y los grupos delictivos organizados que utilizan estos medios, la creación de una red de Equipos de Respuesta a Incidentes de Seguridad Informática, y la identificación y adopción de normas técnicas para una arquitectura segura de Internet.

Por su parte, la Asamblea General de la Organización de Naciones Unidas ha concentrado sus esfuerzos en la promoción del examen de las amenazas reales y potenciales en el ámbito de la seguridad de la información, y las posibles medidas de cooperación para enfrentarlas. Así mismo la Unión Internacional de Telecomunicaciones UIT, en el seno de Naciones Unidas, en desarrollo del Programa de acciones de Túnez para la sociedad de la información de 2005, emanado de la Cumbre mundial sobre la sociedad de la información, tiene como finalidad la construcción de un consenso en materia de ciberseguridad en el contexto de la cooperación internacional.

Los delitos cibernéticos son cometidos en tres dimensiones: a través del uso de sistemas informáticos, los ataques contra la información, o contra el sistema informático en sí.

Adicionalmente, el Consejo de Europa, ente creado el 5 de mayo de 1949, en el año 2001 adoptó el Convenio sobre Ciberdelincuencia[2], único instrumento internacional vinculante para las partes, que apunta a crear un cuerpo penal común contra el delito cibernético, establecer disposiciones comunes de derecho procesal, y allanar líneas de cooperación entre Estados. Este Convenio se ha constituido en el instrumento marco para el desarrollo de diferentes legislaciones nacionales, y ha sido suscrito por Estados Unidos y Japón, entre otros Estados no miembros del Consejo.

Establecido de manera sucinta el panorama nacional e internacional que enmarca el delito cibernético, cabe responderse una pregunta para claridad del lector: ¿cuál es la relevancia de este tema en una publicación sobre política exterior colombiana? La respuesta debe ser concreta: el delito cibernético se constituye en un tema clave dentro de la esfera de temas relativos a la seguridad en la agenda internacional, al ser una amenaza real para una sociedad cada vez más interconectada.

El delito cibernético se constituye en un tema clave dentro de la esfera de temas relativos a la seguridad en la agenda internacional, al ser una amenaza real para una sociedad cada vez más interconectada.

Es posible afirmar, a manera de conclusión, que quienes utilizan los sistemas informáticos con fines delictivos intercambian experiencias e información de manera rápida y eficiente, y están dispuestos a actuar en cualquier escenario desprovisto de las disposiciones legales y técnicas necesarias para una protección adecuada. En consecuencia, es labor del Estado dirigir sus esfuerzos hacia la lucha contra este delito, en el marco de la cooperación internacional.

Notas

1 De acuerdo con la Comisión Europea, las infraestructuras críticas son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados.

2 El Consejo de Europa adoptó en noviembre de 2001 el Convenio sobre Ciberdelincuencia, entrando en vigor desde el 1° de julio de 2004, y su Protocolo para la criminalización de actos de racismo y xenofobia cometidos a través de sistemas informáticos de 2003. Cabe resaltar que si bien el Convenio tuvo su origen en el ámbito regional europeo, es un instrumento abierto para su adhesión a todos los países del mundo.