Arcila & Sotomayor
DERECHO PENAL

DELITOS INFORMÁTICOS Y MEDIDAS DE PROTECCIÓN EN EL MARCO DE LA EMERGENCIA SANITARIA POR EL COVID-19

A raíz de la actual contingencia que atraviesa el país, producto de la pandemia ocasionada por el COVID-19, se pronostica un alarmante incremento en los delitos informáticos, pues los delincuentes informáticos se aprovechan de la intensificación de las conexiones remotas y el mundo virtual, tomando ventaja de la vulnerabilidad de la información y datos sensibles de los usuarios para cometer esta clase de delitos. Para ello se valen de malware, implantan virus espías, suplantan sitios web, entre otros, utilizando como atractivo temas relacionados con el COVID-19.

Delitos informáticos en Colombia

En Colombia, la regulación que tutela a la información y los datos como bien jurídico autónomo se encuentra consagrada en la Ley 1273 del 05 de enero de 2009, a través de la cual se adicionó al actual Código Penal [1] un título que regula las conductas lesivas de los sistemas informáticos, por considerar que todas ellas atentan contra un bien jurídico de naturaleza informática. De esa manera, se creó en nuestro ordenamiento el bien jurídico "de la información y los datos" [2].

Lo anterior implica que la vulneración de la información y los datos no solo puede ser el medio para la realización de otros hechos punibles atentatorios contra diferentes bienes jurídicos como el patrimonio económico, en el caso del hurto por medios informáticos, etc.) sino que también puede dar lugar a la comisión de los delitos descritos en el Título VII del Código Penal vigente, esto es: al acceso abusivo a un sistema informático (artículo 269A), a la obstaculización ilegítima de sistema informático o red de telecomunicación (artículo 269B), a la interceptación de datos informáticos (artículo 269C), al daño informático (artículo 269D), al uso de software malicioso (artículo 269E), a la violación de datos personales (269F), entre otros, que lesionan o ponen en peligro ilícitamente la seguridad de las funciones informáticas, sin perjuicio de que esto signifique la lesión o puesta en peligro de otros bienes jurídicos tutelados (como la intimidad personal, la libertad y formación sexual, los derechos patrimoniales y morales de autor, etc.).

Medidas de protección recomendadas

Las personas naturales o jurídicas que emplean sistemas automatizados de información pueden ser víctimas de estos delitos. Por ello, y teniendo en consideración los riesgos que ellos complican, y a la vez, la necesidad de utilizar estos sistemas de comunicación, realizamos las siguientes recomiendaciones:

[1] Ley 599 de 2000.
[1] Art. 1 de la Ley 1273 de 2009

Arcila & Sotomayor
DERECHO PENAL

- La búsqueda de información sobre la contingencia generada por el COVID-19, es utilizada por los delincuentes informáticos, por lo que se recomienda abrir únicamente los mensajes de fuentes de información oficiales [3]. Además, si estos contienen archivos adjuntos, se recomienda no descargarlos, salvo provengan de un sitio web o contacto de confianza.

- Implementar instrumentos de autenticación en dos pasos (móvil de usuario, token físico, etc.). Se trata de una verificación adicional que permite identificar que es realmente el usuario quien está intentando acceder al sistema de información y no un delincuente informático.

- Revisar con detalle las direcciones electrónicas desde donde se remiten comunicaciones a los usuarios para validar que se traten de sitios oficiales o conocidos. Evitar contestar mensajes, E-mails, o cualquier otro tipo de comunicación electrónica que provenga de una fuente desconocida o sospechosa, incluidos bancos o instituciones financieras.

- No compartir información personal y sensible (dirección, teléfono, claves, etc.) a través de llamadas telefónicas. Los bancos y las instituciones oficiales no solicitan este tipo de información.

- No compartir publicaciones en redes sociales donde se visualicen datos personales como direcciones, ubicaciones, placas de vehículos, etc.

- No realice transacciones electrónicas en redes de WiFi abiertas o desconocidas

- Muchos usuarios no actualizan la funcionalidades básicas de sus equipos (actualización de software en celulares y ordenadores), específicamente los sistemas operativos. Por ende, es recomendable mantener actualizado el software básico, así como actualizar su antivirus.

- Las modificaciones de archivos o registros, los cambios de permisos o su eliminación son una señal de riesgo. Por ello se recomienda implementar un software que permita monitorear cualquier actividad relacionada con archivos, carpetas y registros, y que generen alertas al detectar cualquier cambio o actividad sospechosa.

- En el caso de las organizaciones empresariales, es sumamente importante la divulgación de las posibles conductas ilícitas derivadas del uso indebido de las computadoras o sistemas de información, alertando a las potenciales víctimas para que tomen las medidas pertinentes con el objeto de prevenir la delincuencia informática.

- Así mismo, se recomienda a las empresas efectuar un análisis objetivo de las necesidades de protección y de las posibles fuentes de peligro que pueda tener cada organización empresarial. Una eficaz protección contra los delitos informáticos presupone que los usuarios de la red o sistemas computacionales conozcan las correspondientes formas de manipulación, así como las técnicas encubrimiento por parte de los delincuentes informáticos.

[3] Cuando se trate de sitios Web, se puede verificar el Certificado Digital, que se identifica al visualizar que la barra de direcciones de un buscador es de color verde o cuando aparece un ícono de un seguro a la izquierda.