JOSÉ DOMINGO MONFORTE Y SANDRA GARCÍA BARCOS

ABOGADOS EXPERTOS EN RC DE DOMINGO MONFORTE ABOGADOS ASOCIADOS

Ciberdelicuencia. Aseguramiento del riesgo digital

LAS NUEVAS TECNOLOGÍAS y su generalizada implantación han aportado múltiples ventajas y avances, pero también han generado un nuevo modelo de delinquir, la ciberdelicuencia, que plantea problemas tanto para la investigación, persecución y enjuiciamiento de este tipo de prácticas como también desde la perspectiva del aseguramiento del riesgo, es decir, la cobertura del daño que la conducta ocasione.

La intensidad con la que las nuevas Tecnologías de la Información y la Comunicación (TIC's), con diversos y distintos medios, sistemas y dispositivos informáticos, se han incorporado y forman parte ya de nuestras relaciones sociales y de nuestros medios y equipos de trabajo, relaciones jurídicas y negocios, ha propiciado que los delitos informáticos hayan experimentado un enorme incremento durante los últimos años en nuestro país, y un incremento muy notable de procesos judiciales para la persecución de este tipo de delitos de irrupción en sistemas aparentemente seguros.

Se hace necesario abordar el tratamiento jurídico y la regulación normativa de lo que ya se conoce como cibercriminalidad, para descender seguidamente al aseguramiento del riesgo digital.

No existe en nuestro Código Penal un concepto normativo ni ninguna definición normativa.

La primera definición de la "ciberdelincuencia" fue dada por la Comisión Europea en una Comunicación de 22 de mayo de 2007, conceptuándola como "las actividades delictivas realizadas con ayuda de redes de comunicaciones y sistemas de información electrónicos o contra las redes y sistemas, desglosadas en tres tipos de conductas: formas tradicionales a través del medio tecnológico, publicación de contenidos ilegales a través de medios de comunicación electrónicos, delitos específicos de las redes electrónicas, como los ataques contra los sistemas informáticos, la denegación del servicio y la piratería".

Con carácter general, la ciberdelincuencia puede definirse como toda conducta típica, antijurídica, culpable y punible para cuya comisión se ha utilizado, de alguna manera, las Tecnologías de la Información y la Comunicación (TIC's) e Internet, bien una red privada, pública o doméstica, con la finalidad de atentar la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de la información y datos que se procesan, almacenan o transmiten, así como el uso fraudulento de tales sistemas, redes y datos.

LEGISLACIÓN APLICABLE

El creciente uso de las TIC's para delinquir despertó al legislador la necesidad de abordar una reforma del Derecho Penal para dar tipicidad a las conductas que hasta ahora estaban impunes o con un deficiente tratamiento.

A través de la Ley Orgánica 1/2015, de 30 de marzo, de reforma del Código Penal, se introdujeron nuevos tipos y se adaptaron a la cibercriminalidad las conductas delictuales ya existentes, como por ejemplo: los delitos de descubrimiento y revelación de secretos mediante el apoderamiento y la difusión de datos reservados registrados en ficheros o soportes informáticos (arts. 197 y 197 bis), los delitos de descubrimiento, apoderamiento y revelación de secretos de empresa mediante soportes informáticos (arts. 278 y ss.), la interceptación de transmisiones no públicas de datos informáticos (art. 197.bis.2), la creación, adquisición o facilitación de dispositivos o programas informáticos para la comisión de estos delitos (art. 197 ter y 264 ter), los delitos de daños o sabotajes informáticos (arts. 264 y ss.), el acoso a través de medios de comunicación (art. 172 ter), los delitos contra la propiedad intelectual (art. 270), delitos de falsificación (art. 386 y ss.), delitos de estafa o fraudes informáticos (arts. 248 y 249), así como en los delitos contra la libertad realizados

> "AL IGUAL QUE LAS GRANDES CORPORACIONES, LA PEQUEÑA Y MEDIANA EMPRESA DEBE PRESTAR ESPECIAL ATENCIÓN PARA ALCANZAR Y MANTENER UN ELEVADO NIVEL DE SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN QUE UTILICE"

por cualquier medio de comunicación "amenazas (art. 169 y ss.), coacciones (arts. 172 y ss.) y acoso (art. 172 ter)" y los delitos contra la libertad "delitos de pornografía infantil (art. 189) o el acoso de menores (art. 183 ter)".

La Fiscalía General de Estado nos aporta un dato interesante en su Memoria Estadística al incluir, desde hace unos años, un apartado para la delincuencia informática a través del que se observa la evolución e incremento que este tipo de delitos se va produciendo en España. Así, según la última memoria publicada en 2016, durante 2015 se incoaron 22.575 procedimientos, un 9,93% más que en 2014 (20.534 procesos).

Las estafas informáticas, los delitos de daños informáticos y los delitos de intrusión informática e interceptación de las transmisiones informáticas vienen ocupando la primera posición en la lista de los delitos con más procedimientos judiciales incoados, por delante incluso de los casos contra la libertad sexual o la intimidad.

Son los fenómenos delictivos más comunes y también los que ocasionan a la víctima mayores y más relevantes consecuencias y perjuicios económicos, tanto por las pérdidas económicas sufridas como por la responsabilidad civil que le puede ser potencialmente exigible por un tercero, directa o indirectamente perjudicado por el hecho.

El patrimonio es el bien jurídico protegido en el delito de estafa que es atacado con ánimo de lucro por su autor utilizando dispositivos y medios electrónicos e informáticos con engaño, generando un error en el sujeto pasivo de la acción (la víctima) que le lleva a la realización de un acto de disposición (generalmente pagos, transferencias bancarias, e incluso la facilitación de usuarios y contraseñas "phishing" o "spoofing-alterar un correo electrónico para que parezca enviado por otro, bancos, proveedores comerciales,...) evaluable a efectos económicos y que producen un menoscabo en el patrimonio de la víctima o de un tercero.

Daño o perjuicio económico que es la base necesaria para la consumación del delito, conforme el actual estado jurisprudencial.

El aseguramiento en España de este tipo de acciones se presenta complejo por cuanto se trata de riesgos sin garantía, fundamentalmente por la inexperiencia en la cobertura de este tipo de siniestros, que deben ser tratados globalmente, más cuando el año pasado se produjeron más de cien mil ciberataques y el 70% de ellos los han sufridos pequeñas y medianas empresas (pymes).

Sin embargo, en EEUU la cobertura de este tipo de siniestros está mucho más avanzada, al disponer datos históricos de delincuencia informática y de la envergadura de los daños que ocasiona para confeccionar este tipo de pólizas de aseguramiento digital.

RIESGOS A CUBRIR

El seguro cibernético es un contrato de seguro que tiene poca correlación con las pólizas del hogar, con las pólizas de vehículos a motor, o con las pólizas de vida o de salud y asistencia sanitaria, por la naturaleza del riesgo a cubrir que presenta ángulos y zonas oscuras que requiere el asesoramiento en la determinación del objeto del riesgo.

Las pólizas de cobertura de los delitos asociados al uso de las TIC's deben estar adecuadas a esta realidad social y al peligro digital, por lo que tendrán que cubrir una am-

plísima rama de riesgos que se pueden englobar en dos grandes grupos:

Daños propios: las consecuencias lesivas que el delito informático ocasiona sobre el patrimonio de la víctima, es decir, la pérdida de ingresos como resultado de la vulneración de la seguridad, de la intromisión en los sistemas informáticos: daños, deterioros y menoscabos de los dispositivos, pérdida y destrucción de documentos, programas y datos almacenados y las pérdidas económicas derivadas de los actos de disposición –pagos y transferencias bancarias no consentidas ni autorizadas efectuadas a través del phishing, es decir, previa obtención ilícita de usuarios y contraseñas- o spoofing alteración de correos para que parezcan enviados por terceros, bancos, proveedores comerciales,...

Daños para cuya restitución los contratos de seguros deben de completar como garantías los gastos de gestión y comunicación de las crisis, los gastos de investigación (herramientas informáticas y periciales para el análisis y la determinación de la infracción y del daño ocasionado, y para recuperar en la medida de lo posible los registros y datos todavía existentes), gastos de asistencia técnica, gastos de reposición de archivos reparando todos los desperfectos (borrado, destrucción, inutilización, alteración, etc.) generados en el software y en el hardware afectados, el coste de los programas de reparación, gastos de defensa y las pérdidas patrimoniales sufridas, entre otras, como daño emergente.

Y como lucro cesante, las cuotas del perjuicio en horas/dinero durante el cese del funcionamiento del servicio durante la acción criminal y su investigación.

Sin olvidar las multas y sanciones administrativas que resulten de las actuaciones administrativas iniciadas contra la víctima –generalmente compañías mercantiles- por la Agencia Española de Protección de Datos de Carácter Personal por no cumplir y seguir los principios y garantías de la LOPD y su Reglamento de desarrollo en la recopilación y almacenamiento de datos de terceros, cuando éstos también han sido sustraídos y vulnerados con ocasión del ataque informático.

Daños de terceros. Partida que integraría las coberturas de responsabilidad civil por la pérdida de datos de carácter personal consistente en el coste de las indemnizaciones individuales que la víctima del delito informático deba satisfacer a los terceros colaterales también perjudicados por el ciberdelito cuando además se haya vulnerado su confidencialidad, intimidad, honor o derechos de imagen y le sea imputable y exigible a la mercantil atacada una responsabilidad civil directa por un error de gestión y control interno en la obtención y almacenamiento de datos de carácter personal.

Así como también los gastos de defensa y protección frente a estas reclamaciones de terceros por incumplimiento en la custodia de datos, y los gastos de notificación de las vulneraciones de la privacidad a la AEPD, a los dueños de los registros, al encargado del tratamiento y al tercero afectado.

Motivos todos ellos por los que, al igual que las grandes corporaciones, la pequeña y mediana empresa debe prestar especial atención para alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información y comunicación que utilice para alcanzar un óptimo nivel de seguridad informática y disponer de capacidades técnicas y de organización adecuadas para poder adoptar medidas de prevención, detección, respuesta y mitigación de los incidentes y riesgos que afecten a las TIC's.

Nivel de seguridad que no sólo es exigible por la normativa nacional, sino también por la normativa comunitaria de preceptivo cumplimiento, como es la Directiva NIS (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. O

DOS EVIDENTES CONCLUSIONES

- También las pymes, como las grandes empresas y las multinacionales, deben contar con una cobertura aseguradora del riesgo digital que garantice las situaciones de crisis ante la criminalidad y cubra el gran impacto y las consecuencias económicas propias y de terceros que se deriven del sabotaje informático.
- Esta cobertura será el aseguramiento y la fuente de litigios más importante al que se enfrente la responsabilidad civil del tercer milenio.