El ciberseguro como elemento esencial del desarrollo de la economía digital

Francisco Pérez Bes

Of counsel de Derecho y Economía Digital de Gómez-Acebo & Pombo

El ciberseguro se ha convertido en un elemento fundamental en la gestión de riesgos empresariales, cuya contratación se viene considerando una de las medidas organizativas legalmente recomendables. Sin embargo, también plantea ciertas dificultades a la hora de definir su alcance —a la vista de la rápida evolución de las ciberamenazas— y su ámbito de aplicación en caso de siniestro, lo que requiere que las empresas cuenten con un asesoramiento legal especializado.

El 2017 será recordado como el año en que nos empezamos a concienciar de la ciberseguridad. En efecto, no había transcurrido un mes desde el impacto de WannaCry, que golpeaba Petya (y las variantes de éste), lo que ponía en jaque a toda la industria y revelaba una situación conocida por las empresas, aunque demasiadas veces ignorada: la infraestructura informática sobre la que se basa el negocio está expuesta a serias amenazas.

Valga como ejemplo el incidente sufrido por el bufete de abogados panameño Mossack Fonseca, que dio lugar al escándalo conocido como *los papeles de Panamá* y que ha llevado a la desaparición de dicho despacho como consecuencia del impacto que ha tenido la masiva fuga de información de sus sistemas, indebidamente protegidos.

El impacto económico de esta variante de programa maligno (*malware*) conocida como *programa de secuestro (ransomware)* fue más que considerable en algunas grandes multinacionales, las cuales se vieron afectadas por este virus. Aunque la responsabilidad de su

Advertencia legal: Este análisis sólo contiene información general y no se refiere a un supuesto en particular. Su contenido no se puede considerar en ningún caso recomendación o asesoramiento legal sobre cuestión alguna.

N. de la C.: En las citas literales se ha rectificado en lo posible —sin afectar al sentido— la grafía de ciertos elementos (acentos, mayúsculas, símbolos, abreviaturas, cursivas...) para adecuarlos a las normas tipográficas utilizadas en el resto del texto.

creación y distribución —a modo de ciberataque contra su vecina Ucrania— se atribuye a Rusia dentro del conflicto que ambos países mantenían, el virus se extendió también por empresas y organizaciones ajenas a dicha controversia. Por poner un par de ejemplos para ilustrar esta afirmación: la empresa Mondelez —considerada como la compañía fabricante de alimentos más grande Estados Unidos y la segunda del mundo— el 27 de junio del 2017 comunicó una incidencia en sus sistemas de información a nivel internacional; ese mismo día, la oficina del Reino Unido del despacho de abogados DLA Piper anunció la interrupción de su negocio como consecuencia de ese mismo incidente. Tanto una como otra se vieron afectadas por una serie de daños provocados por el mal funcionamiento de sus sistemas, lo que las obligó a interrumpir el normal desarrollo de sus actividades y les causó una serie de perjuicios valorados en millones de euros.

Ambas entidades reclamaron a sus respectivas compañías aseguradoras, las cuales consideraron que este tipo de incidentes quedaban excluidos de la cobertura de la póliza suscrita al interpretarse que se trataba de actos de guerra y, por lo tanto, no era aplicable la cobertura del siniestro. Tal circunstancia llevó a los afectados a demandar a sus aseguradoras, al efecto de dilucidar si tal interpretación era, o no, correcta.

Esta situación pone de manifiesto uno de los principales desafíos que conlleva la gestión de los ya comúnmente conocidos como *ciberriesgos*. Esto es, el de la correcta tipificación del riesgo objeto de cobertura dentro de la —relativamente— dinámica taxonomía de ciberincidentes de seguridad informática que, por ejemplo, hace pública ENISA de manera anual¹, así como la adecuación de la cobertura a aquéllos.

Ante un escenario como el descrito, tanto el sector público como el privado han venido colaborando de manera intensa para lograr los objetivos de resiliencia que ha ido marcando el Gobierno de España en lo que a ciberseguridad se refiere, primero, en la Estrategia de Ciberseguridad Nacional del 2013 y, más recientemente, en la Estrategia Nacional de Ciberseguridad del 2019.

Asimismo, la normativa legal (y también la deontológica) va dirigiendo sus objetivos hacia la exigencia de nuevas obligaciones para las empresas, lo que está creando un entorno de cultura corporativa de ciberseguridad desconocido hasta ahora, pero bienvenido por necesario, aunque demasiado lento en su desarrollo.

En efecto, normas tales como el Reglamento General de Protección de Datos (RGPD) —y su posterior adaptación al ordenamiento jurídico español por medio de su nueva Ley Orgánica de Protección de Datos y Garantías de los Derechos Digitales— o la Directiva NIS (transpuesta en España por el Real Decreto Ley 12/2018) desarrollan este marco de obligaciones preventivas y reactivas, técnicas y organizativas imprescindibles para lograr un nivel aceptable y responsable de seguridad de la información.

¹ <https://etl.enisa.europa.eu/#>

Es precisamente dentro de este tipo de medidas organizativas donde se encuadra la contratación de una cobertura aseguradora con la que derivar el riesgo a un tercero, en este caso, una compañía aseguradora que ofrezca un producto de esta naturaleza.

Otras normas como, por citar algunas, la Ley de Secretos Empresariales o el Esquema Nacional de Seguridad complementan estas obligaciones, cuyo fin último es el de consolidar un auténtico ecosistema de diligencia y responsabilidad empresarial y cumplimiento normativo. Gracias a ello, España se encuentra en la séptima posición de los países mejor preparados para enfrentarse a ciberataques, según el informe sobre calidad de vida digital de la empresa Surfshark.

En lo que a la actividad aseguradora se refiere, podemos destacar la reciente publicación de la ISO/IEC 27102, sobre gestión de la seguridad de la información y guías para asegurar ciberriesgos (*Information security management-Guidelines for cyber-insurance*), o la referencia que el libro *La agenda 2030 y los ODS: nueva arquitectura para la seguridad* hace al coste de la contratación de un «ciberseguro» como estimación del coste del cibercrimen. Este tipo de menciones refuerzan la idea de que la adopción de medidas de ciberseguridad en la empresa —y en particular la contratación de ciberseguros— no sólo son meras obligaciones para el empresario, sino que van más allá: han pasado a convertirse en auténticas buenas prácticas empresariales que ayudan a las empresas a mejorar la confianza de sus clientes e inversores, a los que trasladan una imagen —cada vez más valorada— de seguridad en su actividad, diligencia en su gestión y responsabilidad en el mercado.

Este nuevo escenario ha revelado un notable incremento en la contratación de pólizas, que seguirá creciendo paralelamente al aumento del número y complejidad de los incidentes de ciberseguridad en empresas de todo tipo, tamaño y sector. Es precisamente esta complejidad la que también supone un reto para los aspectos regulatorios y legales derivados de la contratación de un ciberseguro, como también señala la Autoridad Europea de Seguros y Pensiones de Jubilación (EIOPA) en su informe del 2019 «Cyber risk for insurers – challenges and opportunities».

Por eso la línea de acción 3 dentro del objetivo II de la citada Estrategia Nacional de Ciberseguridad del 2019 ha querido destacar el papel del abogado dentro del desarrollo de la estrategia como elemento clave para el refuerzo de las capacidades de investigación y persecución de la criminalidad, pero también para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio. En este sentido, el Gobierno tiene claro que los abogados expertos en esta rama del derecho digital desempeñan un papel claro sobre el tablero de la ciberseguridad y pueden (y deben) ayudar al resto de los agentes en su labor de lograr una industria más segura.

La colaboración, así pues, con el sector asegurador va a ser clave para el mejor desarrollo de una sociedad conectada, pero segura.