Ciberseguridad y responsabilidad civil, los riesgos de la 4ª revolución industrial

JESÚS JIMENO MUÑOZ
DSG Abogados

Durante los últimos años hemos sido testigos del continuo desarrollo de internet y de las tecnologías de la información. Así, sus efectos en el ámbito socioeconómico de nuestro tiempo configuran los nuevos retos del sector financiero y asegurador, y están siendo abordados por medio del Insurtech y Fintech.

La implementación de estos sistemas tecnológicos ha dado lugar a nuevas formas de causar, padecer y provocar daños; y con ello, a la toma en consideración de nuevos riesgos y preocupaciones en todos los ámbitos sociales, económicos, y empresariales. Tales circunstancias constituyen innumerables oportunidades para la Industria Aseguradora, y para que sean abordadas con éxito será necesario establecer bases y principios jurídicos sólidos.

El desarrollo de las Tecnologías de la Información ha generado un verdadero cambio socioeconómico global, al que el World Economic Forum[1] ha denominado 4ª Revolución Industrial, cuya principal característica es la creación del ciberespacio, como un entorno por medio del que se conectan entre sí sujetos e instituciones de diferente índole. Por ello, la adaptación del ordenamiento jurídico privado y en especial del Derecho de Seguro a estas nuevas realidades constituye reto esencial, y favorecerán el desarrollo de la Industria Aseguradora en este nuevo campo.

Así, el trabajo publicado recientemente bajo el título *"La responsabilidad civil en el ámbito de los ciberriesgos"*[2] constituye uno de los primeros estudios doctrinales en materia de responsabilidad civil en el ámbito tecnológico y cibernético. Y, en este sentido ha tenido por objeto contribuir a adaptar los principios del ordenamiento jurídico español a las nuevas realidades sociales y económicas. De tal forma, responde a la necesidad de abordar con detenimiento:

- La delimitación y relevancia del ciberespacio.
- La definición de conceptos jurídicos relativos a la ciberseguridad.
- El desarrollo del derecho de daños en el ámbito del ciberespacio.
- La adecuación de la doctrina de la responsabilidad civil a las relaciones que surgen en torno a estas realidades.

Todo ello, permitirá atribuir la responsabilidad individual derivada de las actuaciones que se llevan a cabo en el ciberespacio, y favorecerá el adecuado desarrollo del contrato de seguro como elemento esencial para garantizar la estabilidad social y económica de nuestro tiempo. Actualmente, la industria aseguradora se enfrenta al reto de adaptar las pólizas de responsabilidad civil a las estrategias tecnológicas de los clientes, de manera que permitan atender los nuevos daños que por medio de las tecnologías de la información pueden derivase a terceros. Y ello, favorecerá el mantenimiento un ciberespacio **saludable y responsable** capaz de garantizar la seguridad de los individuos y organizaciones que forman parte del mismo.

La incidencia de las Tecnologías de la Información (IT) sobre una cantidad ilimitada de actividades públicas y privadas, que se encuentran continuamente conectadas a internet, determina aquellos medios por los que se pueden ocasionar daños ilimitados. De tal forma, el desarrollo de esta hiperconectividad contribuye con la eficacia de innumerables acciones, pero, al mismo tiempo, permite que los cibereventos se propaguen por toda clase de sistemas, lo que puede llegar a producir **daños colectivos y los eleva a la categoría de riesgo global**.

El análisis de los estudios realizados por el World Economic Forum (entre los que destaca "Risk and Responsibility in a Hyperconnected World"[3]) nos permite llegar a la conclusión de que el carácter ilimitado y abierto del ci-

1 Klaus Schwab, The Fourth Industrial Revolution, World Economic Forum (2016).

2 JIMENO. J, La responsabilidad civil en el ámbito de los ciberriesgos, Fundación Mapfre, Premio Julio Sáez de Investigación en Gerencia de Riesgos y Seguros (2017).

3 Risk and Responsibility in a Hyperconnected World, World Economic Forum (febrero 2014), http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf

berespacio plantea tres cuestiones fundamentales, con las que podemos definir el alcance de los ciberriesgos:

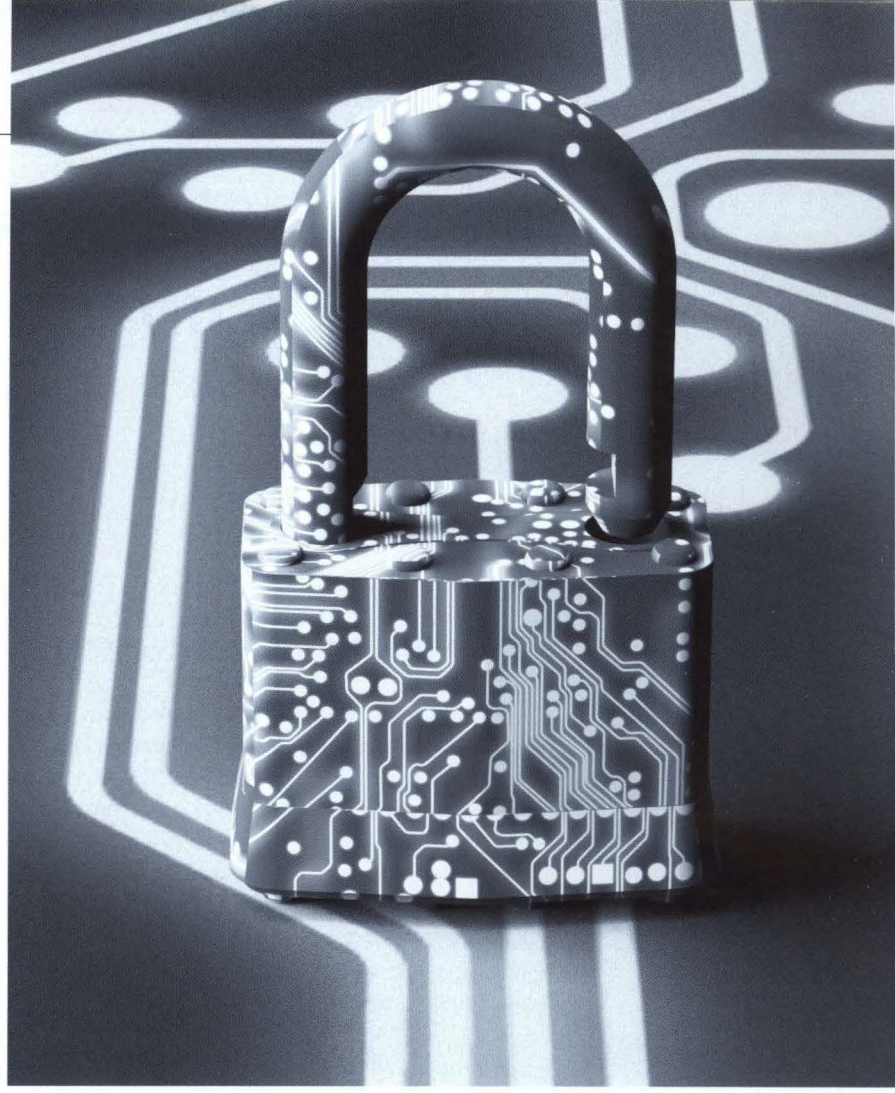
- Que, los ciberriesgos no son problemas aislados, sino, que afectan a todos los sistemas y procesos que se encuentren **interconectados**;
- que los ciberriesgos son **problemas complejos**, que se manifiesta de diversas formas;
- y que, los ciberriesgos representan un **problema socioeconómico global**, según lo definió Kaplan en su artículo Managing Risks: A New Framework[4] publicado en 2012 en Harvard Business Review.

En este sentido, el ciberespacio constituye una realidad múltiple compuesta por una serie de sistemas físicos formados por las infraestructuras de telecomunicaciones, y por todos los elementos y sistemas conectados a las mismas –como los que forman parte del IoT–. Y, además, constituye una realidad en la que los usuarios por medio de la transmisión de información y datos, interactúan y se desenvuelven en cualquier ámbito de su vida.

Todo ello, genera un nuevo medio al que se ha denominado ecosistema digital, desde el estudio que sobre esta materia realizó "The Directorate-General for Communications Networks, Content and Technology" de la Comisión Europea entre los años 2002 y 2005; y, en tal entorno pueden llegar a resultar amenazados e incluso sufrir algún daño, menoscabo o deterioro, toda índole de bienes y derechos.

Desde esta perspectiva, parece importante destacar que el fomento de la cultura de la ciberseguridad al que se refiere el considerando 44 de la Directiva 2016/1148 de 6 de julio constituye una materia esencial para evitar los efectos adversos de los cibereventos, tanto en el ámbito físico, como en el propio ciberespacio. Y, permite tratar de impedir que de una, u otra forma, se ponga en riesgo la integridad de un número ilimitado de bienes y derechos.

No obstante, en atención a los bienes susceptibles de padecer cualquier daño o detrimento, se observa que en la mayoría de casos las Tecnologías de la Información y el ciberespacio no introducen un nuevo bien o interés jurídico susceptible de protección sino un nuevo medio o ecosistema digital a través del que se puede producir un daño . De esta forma, los derechos y la propia integridad de los terceros ajenos a los asegurados (especialmente consumidores y usuarios) constituyen los elementos sobre los que recae de forma principal el riesgo cibernético.



iStock.com/the-lightwriter

En los últimos tiempos se han desarrollado diversas normas nacionales y europeas –GDPR y Directiva NIS– con el objeto de garantizar unas medidas mínimas de ciberseguridad, y algunas de ellas ya forman parte de nuestro día a día. Todas ellas, presentan **el elemento de la responsabilidad de los proveedores y titulares de sistemas como una circunstancia esencial de la naturaleza de las IT, lo que está permitiendo crear un régimen de responsabilidad civil propio para las actividades que se desarrollan en el ecosistema digital**. En este sentido, resultará esencial atender a ciertas características particulares, tales como: la elevación de la diligencia debida por medio de la responsabilidad proactiva; el desarrollo de la teoría de la atribución de la responsabilidad colaborativa; o, la responsabilidad derivada de los sistemas de inteligencia artificial e IoT.

El desarrollo y la adaptación del régimen de responsabilidad civil a las nuevas realidades tecnológicas, y el esfuerzo por la identificación y gestión de los riesgos cibernéticos permitirán garantizar un ecosistema digital seguro, saludable y responsable. Y, en este sentido, la adaptación de las pólizas de responsabilidad civil a las realidades tecnológicas de nuestro tiempo permitirá consolidar a la Industria Aseguradora como la una herramienta idónea para facilitar la gestión y transferencia del riesgo.

4 Kaplan, R.S., and Mikes, A. Managing Risks: A New Framework. En *Harvard Business Review*, 2012.