PAAKAT: revista de tecnología y sociedad
ISSN: 2007-3607
Universidad de Guadalajara, Sistema de Universidad Virtual

López Jiménez, David
Recensión. Derecho de daños tecnológicos, ciberseguridad e Insurtech
PAAKAT: revista de tecnología y sociedad, núm. 19, e497, 2020
Universidad de Guadalajara, Sistema de Universidad Virtual

DOI: https://doi.org/10.32870/Pk.a10n19.497

Disponible en: https://www.redalyc.org/articulo.oa?id=499069742008

Paakat: Revista de Tecnología y Sociedad
e-ISSN: 2007-3607
Universidad de Guadalajara
Sistema de Universidad Virtual
México
paakat@udgvirtual.udg.mx

Año 10, número 19, septiembre 2020-febrero 2021

Recensión
Derecho de daños tecnológicos, ciberseguridad e Insurtech

David López Jiménez*
https://orcid.org/0000-0002-7013-9556
EAE Business School, España

Obra reseñada: Jimeno Muñoz, Jesús. (2019). *Derecho de daños tecnológicos, ciberseguridad e Insurtech.* Madrid, España: Dykinson.

[Recibido 29/01/2020. Aceptado para su publicación 27/05/2020]
DOI: http://dx.doi.org/10.32870/Pk.a10n19.497

Como la realidad cotidiana pone de manifiesto, estamos ante un proceso de transformación digital que hace fundamental que, en nuestro día a día, hagamos uso de las nuevas tecnologías tanto a nivel personal como profesional. En otras palabras, casi todos los escenarios de la vida social han evolucionado hacia lo que podría calificarse como *digital* por defecto. Debemos saber cómo utilizar las nuevas tecnologías (lo que incluye a las tecnologías emergentes) para poder usarlas en nuestro beneficio, las cuales evolucionan a un ritmo vertiginoso, lo que vuelve atrasadas y superadas a las que, hasta hace poco, eran las nuevas.

Sin las nuevas tecnologías, en ningún caso, podríamos referirnos a la era digital. Debemos ser conscientes y plenamente responsables del uso que hacemos de estas. Actualmente, se han producido importantes novedades y avances inimaginables en poco tiempo. Piénsese, a título de ejemplo, en el *big data*, los *Smart contract*, el *blockchain*, el *bitcoin*, las plataformas de economía colaborativa y un larguísimo etcétera.

El libro que es objeto de esta reseña presenta un contenido y una estructura sistemática muy acertados. Consta de tres capítulos que incluyen un amplio conocimiento técnico y jurídico para delimitar el ámbito del derecho de daños en el ámbito tecnológico; asimismo, analiza la relevancia de la ciberseguridad como un instrumento esencial para la gestión de los peligros tecnológicos y, además, su transferencia financiera en virtud de las novedades incluidas por el *Insurtech*. Este último y novedoso vocablo se refiere al sector que engloba a las compañías de seguros tradicionales, a las de índole tecnológico y a las recientes *startup* disruptivas que, por definición, recurren a las nuevas tecnologías.

Dentro de las nuevas tecnologías cabe considerar, entre otras muchas, la cadena de bloques, la computación en la nube y otras similares. Con todo esto, se crean dentro del sector de los seguros novedosas formas de ofertar los productos y servicios al cliente final. *A priori*, podría parecer que *Insurtech* es, por decirlo coloquialmente, una suerte de hermano pobre del *Fintech*, que se refiere a la tecnología financiera, el cual ha logrado una notable atención a nivel mundial. Las denominadas *Fintech*, como es sabido, presentan instrumentos de índole tecnológico que permiten la realización de diversos actos jurídicos vinculados con el dinero, en un sentido amplio.

El capítulo uno del libro alude a los ciberriesgos y su efecto en el desarrollo socioeconómico mundial. En primer término, se analizan los riesgos tecnológicos y cibernéticos, y se detiene en el concepto y evolución de los ciberriesgos a fin de centrarse en la historia y el funcionamiento de la Red. El aumento y el progreso del ciberespacio han posibilitado que las amenazas de los sistemas que lo forman puedan repercutir sobre una gran amplitud de situaciones, acciones y sujetos. De esta manera, podrían llegar a reputarse como amenazas para la seguridad nacional cuando constituyan un riesgo para el orden público, la población o los sistemas y estructuras de carácter estratégico que sean esenciales para el funcionamiento de la sociedad, como es el caso de las infraestructuras críticas.

Los fallos y las debilidades de las infraestructuras críticas son el ejemplo más significativo de ciberamenaza, que es susceptible de manifestarse en virtud de la hiperconectividad. Además, estos daños podrían eliminar los límites y las barreras y, así, propagarse por todo el sistema. Por estos motivos, la seguridad de cada sistema individual, que es una parte inherente del ecosistema digital, coadyuba a crear un ciberespacio robusto, lo que favorece el interés común de todos los sujetos que son parte.

El autor estudia los bienes y los derechos jurídicos que pueden resultar afectados por las situaciones y actividades que se suscitan en el ciberespacio para, posteriormente, ajustar y conceptualizar el derecho de daños en el ámbito cibernético. Igualmente, examina los aspectos jurídicos del aseguramiento de las diferentes realidades en el ciberespacio y los efectos de los seguros como herramienta de la que dispone la sociedad civil para el mantenimiento de la justicia. En segundo lugar, se estudian las repercusiones del mundo hiperconectado y, en concreto, el ciberespacio y los ecosistemas digitales.

El segundo capítulo refiere al daño en el ámbito de los ciberriesgos. En primer lugar analiza la manifestación del daño en el ciberespacio y su protección. Cabe mencionar que a finales de 2013, el representante de la Unión Europea para Asuntos Exteriores y Política de

Seguridad indicó que deben aplicarse las mismas normas, principios y valores que se emplean fuera del mundo virtual (lo que es extensible a la Unión Europea) para que el ciberespacio continúe siendo abierto y gratuito. Es necesario, por consiguiente, salvaguardar los derechos fundamentales, la democracia y la primacía del derecho en Internet. A este respecto, la Unión Europea está colaborando con sus socios internacionales, la sociedad civil y el sector privado para impulsar estos derechos desde una perspectiva global.

Además, se analizan diversas cuestiones vinculadas con la seguridad nacional, como el interés público del ciberespacio, el cibercrimen, y, por último, el ciberterrorismo. Dentro del concepto de cibercrimen, el autor se refiere al robo de identidad, las estafas *online*, el *scareware*, el fraude fiscal, el robo de negocios, la extorsión, el robo de datos de clientes, el espionaje industrial y el robo de propiedad intelectual. Se alude a que la normativa relativa a la ciberseguridad que se ha aprobado en España se centra, en gran medida, en la protección de datos personales y en la persecución de delitos cuya ejecución implica la utilización de medios informáticos.

Como se anticipó, la obra analiza, de manera amplia, el ciberterrorismo, que se puede conceptualizar como el uso de sistemas informáticos para atacar infraestructuras críticas o sistemas de la administración pública, o la coacción o intimidación capaz de afectar al sector público y a la sociedad civil.

El fin de los ciberterroristas es infundir terror, generando trastornos, caos y todos los daños posibles. Los ciberterroristas constituyen grupos criminales que, con independencia de su mejor o peor financiación, operan con suma destreza para atacar sus objetivos. Tienen la capacidad de infiltrarse en numerosos sitios y servicios de internet, entrar en múltiples sistemas para apropiarse de datos confidenciales y, posteriormente, venderlos o hacerlos públicos. Asimismo, roban a entidades financieras para hacer frente a sus actividades delictivas en toda su amplitud; en numerosas ocasiones, corrompen información e infraestructura para desestabilizar o simplemente destruir.

Dentro de los ataques a infraestructuras críticas podemos, entre muchos otros supuestos, referirnos a los dos casos en los que la red eléctrica de Ucrania se vio afectada por ciberterroristas. Otra de las mayores amenazas que imperan a nivel mundial son las plantas nucleares. Se suceden casos que no son supuestos aislados. A finales de 2019, India reconoció haber sufrido ataques de cibercriminales procedentes de Corea del Norte, en sus plantas nucleares. En este caso, se señaló que el virus informático con el que se afectó a la central nuclear guarda analogías con la campaña DarkSeoul, que es un programa de espionaje dirigido a entidades bancarias y medios de comunicación surcoreanos que se atribuye al Grupo Lazarus, vinculado con ciberterroristas procedentes de Corea del Norte.

Sin perjuicio de que el autor después se refiere al Internet de las cosas, cabe hacer un inciso, a propósito de la ciberdelincuencia. En efecto, puede ser aprovechado por los piratas informáticos para fines ciertamente espurios. Con la fiebre desmedida por la conectividad, inherente al Internet de las cosas, cada día tenemos más aparatos conectados a la red; entre estos, podemos citar, sin ánimo agotador, los siguientes: webcam, cámaras

de videovigilancia, máquinas inteligentes de aspirar, frigoríficos, asistentes de voz, y un larguísimo etcétera.

Debemos partir del hecho de que estos instrumentos han sido diseñados y fabricados, al pensar, sobre todo, en su funcionalidad y no en la seguridad. Los dispositivos que se mencionan pueden convertirse en aparatos zombis para múltiples fines ajenos a sus funcionalidades de origen. Cabe hacer alusión al ataque de Mirai (octubre de 2016), en el que una red de millones de dispositivos acometió una agresión de denegación de servicio que afectó notablemente, entre otros, a Twitter, Github, Amazon y Spotify. Se aprovechó el punto débil de numerosos dispositivos y accesorios que estaban conectados a la red. Mirai actuaba con una licencia de software libre, por lo que era relativamente sencillo que cualquier persona pudiera hacer uso de la misma con el objetivo de efectuar ataques de denegación del servicio, lo que afectó impresoras, routers o web cam. Un número muy amplio de dispositivos y accesorios funcionan en virtud de un usuario y contraseña predeterminados. El malware aprovecha esto, los infecta y toma el control de los mismos.

Entidades de los Estados Unidos recomiendan a los usuarios de dispositivos (como los que comentamos) que lo más conveniente es que aíslen esos equipos en una red wifi secundaria, es decir, distinta de la que emplean para vincular sus dispositivos vitales como portátiles, ordenadores y smartphones. De esta forma, si es atacado, se impediría que, desde este dispositivo, se pueda entrar a los otros aparatos principales de los usuarios.

En continuidad, el autor estudia la incidencia de los datos en esta materia y, en concreto, la tutela de los bienes inmateriales y el espectro legislativo de la protección de datos de carácter personal. En este capítulo también son objeto de examen las infraestructuras críticas, el Internet de las cosas y los problemas que plantean los seguros, a propósito de los vehículos autónomos. En este último rubro, puede que el futuro aseguramiento de la conducción autónoma lleve a los productores y mantenedores de vehículos con motor a concurrir o participar en la suscripción de los seguros de circulación que, a la vista de las recomendaciones del Parlamento Europeo, parece que seguirán siendo preceptivos.

Algunos especialistas prevén que la facturación del sector caerá de manera notable; asimismo, indican que serán los fabricantes quienes estipulen las pólizas y que estas incluirán, entre otras cláusulas, el peligro de sufrir el ataque de un pirata informático. La responsabilidad legal, en el supuesto de que se produzca un accidente, no será del conductor, sino esencialmente del fabricante del vehículo; en otros términos, serán los fabricantes quienes aseguren el vehículo. Por otro lado, al hilo de cuanto se esboza, la búsqueda de la eficiencia energética provocará, sobre todo en las urbes más grandes, la puesta en marcha de empresas dedicadas a servicios de movilidad compartida, como las plataformas de alquiler de coches por cortos espacios de tiempo.

Es probable que, con los cambios que están sucediendo en la materia que comentamos, la contratación de las primas de seguro se reduzca en el escenario europeo. Esta última contracción podría cifrarse entre 10% y 30% hasta el año 2025, lo que podría generar un descenso en la facturación de hasta 35 000 millones de euros para estas

compañías. Un desplome del negocio que, sin duda, dará lugar a fusiones, e incluso a la clausura de las aseguradoras menos aptas para el cambio y adaptaciones a los nuevos tiempos y modelos imperantes.

Una de las diversas ventajas de los coches autónomos estriba en que la tecnología permite suprimir el factor humano, al que se considera responsable de aproximadamente el 90% de los accidentes. Si bien es cierto que es probable que la tecnología dé lugar a un aumento de los montos de las indemnizaciones (tanto los vehículos como sus arreglos, en sus distintas variantes, se encarecerán), el importe total de estas disminuirá como consecuencia del mínimo número de accidentes. Es, desde otra perspectiva, una noticia negativa para las aseguradoras tradicionales que, dicho sea de paso, no pueden perder de vista otra novedad debido a que, con el cambio tecnológico, los expertos auguran la llegada de nuevos agentes al sector.

Finalmente, el capítulo se cierra con dos cuestiones muy significativas, que son el daño emergente y el lucro cesante, así como la pérdida de reputación y los daños generados al honor. A este último respecto, como señala el autor, existen perjuicios que suscitan un menoscabo de la reputación y del prestigio que es parte del derecho al honor de las personas físicas y jurídicas, y que tiene lugar por un ciberevento de cualquier clase.

Los ciberataques, individualizados o colectivos, suponen un riesgo importante para las empresas e instituciones, no solo desde el punto de vista económico, sino también a efectos de reputación. Actualmente, numerosas organizaciones no tienen protocolos de comunicación para hacer frente a estos ciberataques. Es esencial tener un seguro cibernético que, de producirse un incidente, haga frente al pago de los costes por la contratación de servicios de asesores en imagen y marca para atenuar la crisis que eventualmente haya podido desencadenarse.

El último de los capítulos trata sobre los ciberseguros y los efectos de los ciberriesgos en los seguros de responsabilidad civil. Los instrumentos de asistencia a la conducción, así como la conducción de vehículos autónomos limitan los riesgos humanos vinculados con la conducción, pero simultáneamente dan origen a una nueva generación de riesgos. En la actualidad, la industria automovilística discute acerca del alcance de la responsabilidad procedente de la conducción de vehículos a motor, pues el significado de conducción autónoma no es unánime. Esta disputa estriba en dilucidar si el sistema de conducción autónomo es de asistencia a la conducción (que necesita de la participación activa del conductor) o si, por el contrario, reemplaza plenamente al conductor.

Hay elementos como la conducción autónoma o asistida de vehículos, que reducen los riesgos humanos asociados a la conducción, si bien de forma simultánea, encajan una nueva generación de riesgos, en los que parece estar alterada la aplicación de los presupuestos de la responsabilidad civil de acuerdo con los supuestos tradicionales. Como determina más adelante el autor, en el ámbito de los ciberriesgos hay una serie de elementos de los que, con cierta seguridad, nacerán discusiones en cuanto a la aplicación del caso fortuito y la fuerza mayor.

La industria aseguradora debe adaptarse a las circunstancias que han introducido las tecnologías de la información en materia social, económica y empresarial. Así, la red genera un medio en virtud del que se crean nuevas relaciones y ofrecen nuevos servicios. Asimismo, admite la obtención de ventajas para las actividades y relaciones tradicionales. Nos referimos a que progresivamente más negocios integran sistemas tecnológicos para optimizar sus resultados, y, al mismo tiempo, se crean nuevos productos y servicios con un importante componente tecnológico.

Esta industria ha conseguido abaratar sus productos y servicios en virtud de la tecnología, la cual ha mejorado los procesos que implica. Además, los avances tecnológicos le han permitido estar a la altura y asegurar el bienestar que requiere el cliente. El daño más habitual y el que más peligro supone para una empresa es el que incide sobre los equipos informáticos y el tratamiento de datos. Dentro de la tipología de acciones indeseables que pueden acontecer, están los virus, el robo de datos, la extorsión o el fraude, que son los ciberriesgos más relevantes a los que se enfrentan las empresas. El valor medio de estas acciones para las empresas que lo sufren, en el caso concreto de España, es de unos 50 000 euros. Ahora bien, este no es el principal hándicap, ya que lo peor es que puede llegar a suponer el cierre para un lugar que no esté bien protegido (tanto desde la perspectiva tecnológica como económica).

La defensa tecnológica pasa, en principio, por lo que se denomina en el argot popular como la ciberhigiene. Con esta expresión se busca amparar hábitos saludables o preventivos en temas de ciberseguridad, como contraseñas robustas, evadir descargas y sitios web no seguros, entre muchas otras acciones. Resulta indispensable tener las medidas técnicas adecuadas: deben considerarse antivirus, cortafuegos y actualizaciones permanentes.

Con todo, sean cuales sean los esfuerzos y la inversión, debemos tener claro que el riesgo cero no existe. Es significativo disponer también de protección económica; si bien los efectos malintencionados del ataque no pueden evitarse por completo, su huella puede reducirse al mínimo. Los seguros de ciberriesgo constituyen una suerte de última línea de defensa respecto a los asaltos, infracciones y robo de información de la empresa. Aportan un alto grado de seguridad, jurídica y económica, respecto a las responsabilidades derivadas. Con base en la magnitud del incidente, un ciberataque implicará gastos derivados de la gestión de la crisis, en un primer momento, responsabilidad civil, protección jurídica, merma de beneficios, perjuicios reputacionales y eventual abono de multas.

Respecto a las sanciones, uno de los elementos que mayor repercusión puede tener son los deberes que todas las empresas tienen respecto al tratamiento de datos personales de sus clientes, como consecuencia de las modificaciones al Reglamento Europeo de Protección de Datos, norma de aplicación directa que no precisa de transposición alguna a los países comunitarios.

Una sección del seguro donde las previsiones registran fuertes incrementos de las primas es el de las ciberpólizas, con las cuales las organizaciones buscan resguardarse de agresiones tecnológicas. La penetración de las nuevas tecnologías afecta a la industria aseguradora en dos áreas: en primer término, en tanto que compañías donde la

digitalización ha alborotado los procesos y se acumulan magnas bolsas de datos críticos, y como proveedores de defensa, que forman una nueva y prometedora área de actividad. Por todo esto, la ciberseguridad es más relevante en este que en ningún otro sector.

En la actualidad, imperan más de cien compañías de seguros en todo el mundo que ofertan servicios para hacer frente a los riesgos cibernéticos, además de que permiten absorber los peligros de los clientes cuando se produce un ataque. Para los integradores de sistemas de seguridad, también cabe la posibilidad de optimizar la seguridad cibernética al exponer este seguro como prueba para que sus clientes conozcan los férreos protocolos de seguridad. La existencia de amenazas de ciberseguridad aumentará con el crecimiento del Internet de las cosas.

Por estas razones, las compañías, incluidos los profesionales de los sistemas de seguridad, deben indagar acerca de las bondades de los seguros de responsabilidad cibernética. Como es conocido, el mayor beneficio de estos productos es disfrutar de la tranquilidad en el supuesto de que acontezca una violación de los datos o información corporativa, que es una experiencia traumática.

A partir de las revueltas geopolíticas y los vertiginosos cambios en la tecnología, numerosos analistas consideran que un ciberataque, a gran escala, podría suscitarse en cualquier momento. La ciberseguridad se encuentra a la delantera de las preocupaciones de los operadores económicos y del sector público; sin embargo, las coberturas únicamente serán efectivas si existen soluciones colectivas para enfrentar el riesgo de manera apropiada. A medida que los mercados de seguros cibernéticos maduren, se deberá empezar a valorar si estas pólizas habrán de ser imperativas –como son en España las de responsabilidad civil, adaptadas a los diferentes ámbitos–; esto facilitaría un grado complementario de seguridad para las compañías y los clientes.

CÓMO CITAR ESTE ARTÍCULO:

López Jiménez, D. (2020). Recensión. Blockchain: aspectos tecnológicos, empresariales y legales. *Paakat: Revista de Tecnología y Sociedad 10*(18). http://dx.doi.org/10.32870/Pk.a10n18.497

* Es doctor (con mención europea) por la Universidad de Sevilla y doctor por la Universidad Rey Juan Carlos, España. Full Professor en EAE Business School, España.