LA RESPONSABILIDAD CIVIL EN EL ÁMBITO DE LOS CIBERRIESGOS

JESÚS JIMENO MUÑOZ

V PREMIO JULIO SÁEZ DE INVESTIGACIÓN
EN GERENCIA DE RIESGOS Y SEGUROS

agers
Asociación Española
de Gerencia de
Riesgos y Seguros

Fundación
MAPFRE

LA RESPONSABILIDAD CIVIL EN EL ÁMBITO DE LOS CIBERRIESGOS

Jesús Jimeno Muñoz

V Premio Julio Sáez de Investigación
en Gerencia de Riesgos y Seguros

agers
Asociación Española
de Gerencia de
Riesgos y Seguros

Fundación
MAPFRE

Imagen de cubierta: ThinkStock
Maquetación e impresión: Arias Montano Comunicación
www.ariasmontano.com

Coordinación: Ana María Sojo
Edición: Miriam López Díaz

2017, Fundación MAPFRE
Paseo de Recoletos, 23
28004 Madrid
www.fundacionmapfre.org

ISBN: 978-84-9844-667-8
Depósito Legal: M-34449-2017

En 2015, y dentro de nuestro programa Ayudas a la Investigación en Seguros Ignacio Hernando de Larramendi, decidimos apoyar la propuesta que nos hizo llegar Jesús Jimeno para desarrollar un tema básico a día de hoy: la responsabilidad civil relacionada con el uso de tecnologías de la comunicación. Nos pareció una idea sugerente y novedosa, que encajaba muy bien con uno de nuestros fines fundacionales, la promoción y difusión del conocimiento del seguro y la previsión social. Los informes del tutor del trabajo, Josep Celaya, pusieron de manifiesto que nuestra decisión inicial había sido la adecuada. Por ello que un trabajo en el que confiamos desde el primer momento haya sido merecedor del V Premio Julio Sáez de Investigación en Gerencia de Riesgos, que con periodicidad bienal concede la Asociación Española de Gerencia de Riesgos (AGERS), nos produce una gran satisfacción.

La responsabilidad civil en el ámbito de los ciberriesgos constituye un completo análisis de cómo ciudadanos, instituciones y gobiernos enfrentan los desafíos que el uso cotidiano de las tecnologías de la información comporta. La existencia de un mundo virtual completamente interconectado supone un espacio de desarrollo social y económico que no está exento de riesgos, que se caracterizan por su alcance complejo y global. La correcta evaluación del riesgo y la contratación de seguros adecuados constituyen las herramientas básicas con las que la sociedad civil podrá enfrentar de manera adecuada las amenazas que puedan generarse en el ciberespacio, lo que al mismo tiempo servirá para mantener a este ámbito al margen de una regulación excesiva que, sin duda, redundaría en contra de su potencial desarrollo.

Nuestra felicitación a Jesús Jimeno por la publicación que el lector tiene entre sus manos, la primera de otras muchas que están por llegar y que ya estamos esperando, y nuestro a agradecimiento a AGERS, por el premio y por compartir con nosotros el reto que supone acercar a la sociedad la cultura del seguro y la previsión social.

Fundación MAPFRE

En 2006 la Junta Directiva de la Asociación Española de Gerencia de Riesgos y Seguros (AGERS) promovió la idea de crear el «Premio Internacional de Investigación en Gerencia de Riesgos Julio Sáez», en memoria de quien fuera su presidente desde 2003 hasta 2006. En este proyecto se cuenta con la generosa colaboración de El Corte Inglés, patrocinador del galardón, y el apoyo de la Fundación MAPFRE, que lleva a cabo la publicación del trabajo ganador.

En esta «V Edición del Premio Julio Sáez de Investigación en Gerencia de Riesgos» el Jurado ha estado presidido por José Luis Martínez Olivares, representante de El Corte Inglés, y compuesto por: Sergio Álvarez Camiña, director general de la Dirección General de Seguros y Fondos de Pensiones; Pilar González de Frutos, presidenta de UNESPA; Mercedes Sanz Septién, directora del área de Seguro y Previsión Social de Fundación MAPFRE; Juan Carlos López Porcel, presidente de AGERS y director de Riesgos y Seguros de ArcelorMittal España; Ignacio Martínez de Baroja, miembro de la Junta Directiva de AGERS y gerente de Riesgos de HISPASAT; M.ª Isabel Martínez Torre-Enciso, miembro de la Junta Directiva de AGERS, vicepresidenta de FERMA y vicepresidenta de la ACDP; Gonzalo Iturmendi Morales, secretario general de AGERS y administrador único del bufete G. Iturmendi y Asociados; y Pedro Tomey Gómez, director general de la Fundación Aon España.

El citado Jurado, por mayoría, ha determinado fallar a favor de la monografía de investigación titulada: *La responsabilidad civil en el ámbito de los ciberriesgos*, siendo su autor, Jesús Jimeno Muñoz, abogado especialista en Derecho de Seguros y Responsabilidad Civil.

Se trata de un trabajo innovador, dentro del ámbito de la Responsabilidad Civil y el Derecho de Seguros, que desarrolla las bases y principios aplicables a la responsabilidad civil procedente de las tecnologías de la información (IT), con especial atención a la gestión corporativa de las mismas y la responsabilidad de los CIO, CTO y CISO. Adicionalmente, profundiza en los elementos del contrato de seguro en relación con la cobertura de las amenazas cibernéticas y en los retos que el IoT (Internet of Things) y los ciberriesgos suponen para la industria aseguradora y reflexiona sobre las medidas de respuesta ante los mismos haciendo hincapié en los estándares de la Gerencia de Riesgos en busca de la excelencia.

Dicho lo anterior, en nombre de AGERS y en memoria de Julio Sáez, felicito al ganador de esta edición, así como al resto de trabajos presentados que han llamado enormemente nuestra atención.

Igualmente quiero agradecer a los miembros del Jurado su tiempo y dedicación, a la Fundación MAPFRE por su apoyo permanente y, de forma especial, a José Luis Martínez Olivares y El Corte Inglés por su destacada y altruista colaboración.

Finalmente, tengo la satisfacción de anunciar la convocatoria de la «VI Edición del Premio Julio Sáez de Investigación en Gerencia de Riesgos», deseando que el prestigio del mismo sirva para fomentar la investigación en la Gerencia de Riesgos y que esta disciplina continúe su evolución bajo el impulso de trabajos como el que ahora tiene en sus manos.

Juan Carlos López Porcel
Presidente de AGERS
Director de Riesgos y Seguros ArcelorMittal España

AGRADECIMIENTOS

De manera previa al desarrollo de la presente obra debo dar las gracias a todos los que han colaborado y han hecho posible su desempeño.

Inicialmente es oportuno agradecer a la Fundación MAPFRE y a las personas que la forman la continua confianza que vienen depositando en mi investigación, entre ellos a Ana Sojo y Josep Celaya, cuyo apoyo está siendo fundamental en el desarrollo de este proyecto. Y, en especial, a Eduardo Pavelek, sin cuya inestimable ayuda no hubiera sido posible la realización del presente estudio.

Y principalmente mi agradecimiento tiene que recaer sobre mis maestros, Jesús y Paco, a cuyo tiempo, esfuerzo y enseñanzas se debe cada palabra de las que contiene esta obra.

Quisiera extender mi agradecimiento a las personas, instituciones y empresas que de forma activa han querido participar en este estudio, muy especialmente a José Ignacio Rodríguez y a la UAH. También, a todos aquellos cuya investigación y trabajo ha sido inspirador de las ideas que aquí se han tratado. Y de forma especial tengo que agradecer al incansable apoyo de mi familia a la que se debe mi trabajo.

RESUMEN

El riesgo cibernético se ha definido como el riesgo asociado con el uso de las TI y está relacionado con la propiedad, la operatividad, la influencia, la participación y la implementación de las mismas. De tal manera, cualquier sistema tecnológico que se encuentre conectado a otro puede verse afectado por estos riesgos emergentes. Por ello, es posible considerar que el desarrollo progresivo de las TI ha dado lugar al aumento y evolución del riesgo cibernético. En efecto, desde la creación de los primeros ordenadores hasta el internet de las cosas, las TI se han ido aplicando a un número incontable de situaciones y elementos.

Los riesgos cibernéticos podrían afectar a un amplísimo panorama de intereses públicos y privados, por lo que resulta necesario estudiar las acciones que puedan concurrir al daño, y la distribución de la responsabilidad entre todos los agentes que participan del ciberespacio.

Así, el presente trabajo plantea un análisis pormenorizado de los elementos de la responsabilidad civil y el derecho de daños en el ciberespacio, con lo que pretendemos establecer las bases de la responsabilidad derivada de la utilización de sistemas tecnológicos y cibernéticos.

ABSTRACT

Cyber risk has been defined as the risk associated with the IT use, property, operativity, influence, participation and the implementation of IT systems. Therefore, every technology system connected to one another falls under this category. For this reason, it is possible to consider than the progressive development of IT systems has caused the increase and evolution of cyber risk. Indeed, since the creation of the first computers to the actual IoT (Internet of Things) IT has been applied for more number of the basics socioeconomic actions and daily routines. Therefore, cyber risk could affect the private lives of each individual citizen for either public or national interest.

There are an uncountable number of goods and rights possibly affected by the cyber events because the common characteristics of them is the connectivity between systems. For all of these reasons, It is appropriate to study the damaged concurrent actions and determine how to distribute the liability among every agents who take place at cyberspace.

There are some elements to determine the cyber risks liabilities: the action or the event generator of risks, as the cyber attack works and the cyber event effects. As mentioned, all of those are the liability essential elements and it would be necessary to analyze it forward to provide a cyber risk efficient transfer to the insurance industry. Furthermore, our study introduces the bases and the context of Cyber Tort and Liability, and afterwards we would be able to determine certain conclusions about controversial matters such as, cyber risk coverage, the applicability of insurance limts and cyber risk exclusions and the concurrence of insurance at cyber events.

ÍNDICE

1. LOS CIBERRIESGOS COMO AMENAZAS DEL MUNDO VIRTUAL

Las tecnologías de la información (IT por sus siglas en inglés) o tecnologías de la información y comunicación (ICT por sus siglas en inglés —TIC en español—) son las herramientas que permiten almacenar, recuperar, manipular y transmitir datos[1] conectando diversos dispositivos electrónicos entre sí.

El término *tecnología de la información* en su significado moderno se enunció en 1958 en un artículo publicado en la revista *Harvard Business Review* en el que sus autores Harold J. Leavitt y Thomas L. Whisler comentaron que «la nueva tecnología no tiene aún un nombre establecido. Deberíamos llamarla tecnología de la información (IT)».

En aquel momento se consideró que tal concepto compredía tres categorías: técnicas de procesamiento, la aplicación de métodos estadísticos y matemáticos para la toma de decisión, y la simulación del pensamiento de orden superior a través de programas computacionales[2].

Las IT han experimentado diversos cambios a lo largo de la historia[3], actualmente se asocian a herramientas que permiten compartir información por medio de redes y conexiones que forman el denominado ciberespacio y cuya evolución ha generado una red de información mundial.

Actualmente, el ciberespacio es un elemento fundamental del ámbito personal, empresarial y administrativo, y constituye el marco en el que se llevan a cabo actividades públicas y privadas que puedan tener algún componente digital. Este nuevo ámbito ha supuesto una oportunidad para el Estado, las empresas y la sociedad civil de compartir y participar de la información mutua, y tiene una capacidad de desarrollo ilimitada.

De esta forma, el ciberespacio se podría entender como un «nuevo mundo virtual» formado por conexiones individuales en el que los gobiernos e

1 John Daintith (ed.), «IT», *A Dictionary of Physics*, Oxford University Press, 2009.

2 Harold J. Leavitt y Thomas L. Whisler, «Management in the 1980s», *Harvard Business Review*, 1958, p. 11.

3 Jeremy G. Butler, «A History of Information Technology and Systems», University of Arizona.

instituciones públicas operan como un sujeto más y su control sobre el sistema global es muy limitado.

Los sujetos que interactúan en tal entorno están sometidos a los riesgos inherentes del mismo, y frente a ellos desarrollan un conjunto de actividades encaminadas a evitarlos que se denominan «acciones de ciberseguridad» o «ciberseguridad». Así, tal concepto se define como la situación de ausencia de amenazas realizadas por medio de, o dirigidas a, las tecnologías de la comunicación y de la información y de sus redes[4].

Las acciones de ciberseguridad están formadas por una serie de planes individuales de contingencia que presentan soluciones aisladas —*ad hoc*— a los problemas que puedan surgir en sistemas tecnológicos concretos. Por ello, se ha considerado que la ciberseguridad constituye un sistema de carácter amorfo[5], ya que inicialmente no prestaba atención a los riesgos sistémicos o globales. No obstante, frente al carácter global de las ciberamenazas, se ha ido prestando mayor atención de forma progresiva a la cooperación entre diversos sistemas y entidades, y al desarrollo de capacidades conjuntas[6].

La relevancia y extensión del ciberespacio ocasiona que las amenazas puedan ser de toda índole y afectar a cualquiera de los sujetos que interactúan en él. De tal manera, cuando las amenazas en el ciberespacio tienen carácter de acciones terroristas o militares, constituyen una amenaza para la seguridad nacional[7]. Y, además, pueden calificarse de amenaza para la seguridad nacional aquellas que afecten al orden público, a la población o a sistemas y estructuras de carácter estratégico que por su importancia y relevancia sean esenciales para el funcionamiento de la sociedad, como las infraestructuras críticas[8].

La creciente conciencia sobre las ciberamenazas y la constante presencia de los citados actores hostiles en la Red, bien sean gobiernos, empresas o delincuentes comunes, han obligado a la mayoría de los gobiernos a replantearse las posibles vulnerabilidades ante las actividades ilícitas en la red.

No obstante, el control del ciberespacio es un aspecto muy controvertido, como también lo son los límites de la regulación de las actividades llevadas

4 Emilio Sánchez Rojas, «¿Ciber… qué? La ciberseguridad», *Ejército*, vol. 837 (2010), p. 138.

5 Alexander W. Vacca, «Military Culture and Cyber Security», *Survival*, vol. 53, nº 6 (2012), p. 159.

6 Eneken Tikk, «Ten Rules for Cyber Security», *Survival*, vol. 53, nº 3 (2011), p. 119.

7 Emilio Sánchez Rojas, «¿Ciber… qué? La ciberseguridad», *Ejército*, vol. 837 (2010), p. 140.

8 Sebastián Koch Merino, Centro de Estudios Estratégicos, Academia General del Ejército de Chile, Revista de Ensayos Militares, vol. 1, nº 2 (2015), pp. 85-98, http://www.ceeag.cl/wp content/uploads/2016/05/libertad-en-el-ciberespacio.pdf

a cabo por el Estado para garantizar la seguridad del mismo. Así, la falta de límites claros hace que la distinción entre intereses públicos y privados sea una cuestión para la que aún no se ha alcanzado una solución de consenso global[9].

La discusión entre la libertad y la intervención se define como ciberdilema, que pretende comprender en qué situaciones se debe favorecer la libertad individual y en cuáles puede intervenir el Estado para procurar la seguridad del ciberespacio y de los sujetos que en él operan[10].

El ciberespacio tiene por característica una «realidad dual» en cuanto lo público y lo privado. Aunque, a diferencia de la realidad física, en el ciberespacio es difícil distinguir entre lo abierto y lo cerrado, lo privado y lo público[11].

Por ello, es importante estudiar los ciberriesgos desde una doble perspectiva: por un lado, en relación con el daño padecido por los sujetos individuales —en lo relativo al ámbito privado—; y por otro lado, la amenaza que suponen los ciberriesgos para el ámbito socioeconómico —desde el punto de vista del interés público—.

En lo relativo al daño y las amenazas que afectan a los derechos y libertades individuales John Stuart Mill entendía que, según el *principio del daño*, el único argumento válido para limitar la libertad de uno o de más individuos en una sociedad es evitar un daño a sus miembros. De tal manera, se pone el interés de la sociedad por encima de las preferencias, gustos, deseos e intereses individuales[12]. Este principio ha sido generalmente acogido y permite al Estado intervenir en caso de que por medio del ciberespacio se esté atentando contra los derechos de sujetos individuales. Pero, en la práctica, su aplicación puede verse dificultada por los medios tecnológicos de que se dispongan y por la competencia y autoridad territorial que siempre está delimitada por fronteras físicas.

La intervención del Estado en el ciberespacio con el fin de garantizar la seguridad, el cumplimiento de las leyes y someter la libertad individual en beneficio

9 Eguskiñe Lejarza Illaro, «Ciberguerra los escenarios de confrontación», *Instituto Español de Estudios Estratégicos*, nº 14 (febrero de 2014), pp. 2-4, http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO18-2014_Ciberguerra_EscenariosConfrontacion_EguskineLejarza.pdf

10 José María Molina Mateos, «Ciberdilema», *Instituto Español de Estudios Estratégicos*, nº 115 (noviembre de 2013), p. 1, http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO115-2013_Cyberdilemma_JM.MolinaMateos.pdf

11 Sebastián Koch Merino, «Libertad en el ciberespacio», *Revista de Ensayos Militares*, vol. 1, nº 2 (2015), p. 92.

12 John Stuart Mill, «On Liberty», *Bantam Classics*, New York, 2008, pp. 13-14.

del «bien común» es cada día mayor y excede de la simple aplicación del principio del daño. En la actualidad, según advirtió Jillian York (directora del departamento de Libertad de Expresión Internacional de Electronic Frontier Foundation) en la entrevista publicada el 14 de enero de 2014 por BBC.Com, la mayoría de los países tienen el control de la infraestructura con la que se accede al ciberespacio, lo que permite censurar cualquier contenido con facilidad. Y en ciertos casos, las autoridades exigen a los proveedores del servicio que implementen bloqueos. De cualquier forma, el resultado es el mismo: los habitantes de ese país pueden ver únicamente los sitios web permitidos por el gobierno[13].

De esta forma, diversas publicaciones de relevancia internacional como *Freedom on the Net reports*[14], *OpenNet Initiative*[15] *y Reporters Without Borders*[16] se han encargado de señalar los países que consideran «enemigos para la libertad en internet» por aplicar sistemas de censura e intervención sobre el contenido del ciberespacio al que tienen acceso sus ciudadanos.

Frente a la idea de intervenir y limitar el ciberespacio para exigir el cumplimiento de una regulación concreta, se ha postulado la doctrina y pensamiento liberal como se defiende en la Declaración de Independencia del Ciberespacio:

> *«En nombre del futuro, os pido en el pasado que nos dejéis en paz. No sois bienvenidos entre nosotros. No ejercéis ninguna soberanía sobre el lugar donde nos reunimos.*
>
> *No hemos elegido ningún gobierno, ni pretendemos tenerlo, así que me dirijo a vosotros sin más autoridad que aquella con la que la libertad siempre habla. Declaro el espacio social global que estamos construyendo independiente por naturaleza de las tiranías que estáis buscando imponernos. No tenéis ningún derecho moral a gobernarnos ni poseéis métodos para hacernos cumplir vuestra ley que debamos temer verdaderamente»*[17].

---

13 ¿Internet con fronteras electrónicas y límites geográficos?, *BBC Mundo*, 14 de enero de 2014, http://www.bbc.com/mundo/noticias/2014/01/140110_tecnologia_limites_internet_censura_kv

14 «Freedom on the Net 2015», *Freedom House*, octubre de 2015. Recuperado el 27 de diciembre de 2015.

15 Helmi Noman y Jillian C. York, «West Censoring East: The Use of Western Technologies by Middle East Censors, 2010-2011», *OpenNet Initiative* (marzo de 2011).

16 «Enemies of the Internet 2014: Entities at the heart of censorship and surveillance», *Reporters Without Borders* (París) (11 de marzo de 2014).

17 John Perry Barlow, *A Declaration of the Independence of Cyberspace*, Davos (Suiza) (8 de febrero de 1996), https://www.eff.org/es/cyberspace-independence

En este sentido, el ciberespacio comprende una realidad en la que se pone en evidencia la eficacia de la regulación e intervención del Estado. Y esto plantea la necesidad de que el Derecho Privado aborde los diferentes aspectos y conflictos que sobrevengan de este «nuevo mundo», cuya naturaleza la constituyen acuerdos y relaciones de carácter estrictamente privado.

Y, desde tal perspectiva, plantearemos la cohesión entre el ciberespacio y la ciberseguridad abordando con detenimiento las cuestiones relativas a la responsabilidad contractual y extracontractual que se ponen de manifiesto con ocasión de los ciberriesgos, así como los aspectos jurídicos del aseguramiento de las diferentes realidades existentes en el ciberespacio y los efectos de los seguros como instrumento de una sociedad liberal para el mantenimiento de la justicia y la paz social.

1.1. El concepto de ciberriesgos

Los ciberriesgos se pueden definir de forma general como riesgos informáticos, es decir, «el riesgo de negocio asociado al uso, propiedad, operación, participación, influencia y adopción de las IT dentro de una empresa» (ISACA IT Risk Framework)[18]; y es que comprenden no solo los daños causados a través de internet, sino los que sean consecuencia de sistemas internos, y en muchos casos ambas circunstancias deben ser tenidas en cuenta al mismo tiempo.

El National Institute of Standards and Technology (en adelante, NIST) determina que los riesgos que afectan a las IT se caracterizan por el nivel de impacto en las operaciones de una organización (misión, funciones, imagen y reputación), los activos de la misma y los sistemas de información; y esto determina el potencial de impacto de las amenazas y la probabilidad de ocurrencia. De esta forma, se definen como la probabilidad de que exista una amenaza accidental o intencionada como consecuencia de una vulnerabilidad particular o de un sistema de información[19]. La International Organization for Standardization (en adelante, ISO) califica los IT risk como la potencial amenaza ocasionada por una vulnerabilidad tecnológica de un activo o grupo de activos que pueden causar un daño a una organización[20].

---

18 COBIT 5 for Risk, ISACA (2013), http://www.isaca.org/COBIT/Documents/COBIT-5-for-Risk-Preview_res_eng_0913.pdf

19 Gary Stoneburner, Alice Goguen y Alexis Feringa Risk, *Management Guide for Information Technology Systems*, National Institute of Standards and Technology NIST SP 800-30 (julio de 2002), http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

20 ISO/IEC 27005:2011, Terms and definitions, ISO, *Online Browsing Platform (OBP)*, https://www.iso.org/obp/ui/#iso:std:56742:en

En la actualidad, dentro de la doctrina y el ordenamiento jurídico español no parece existir una definición clara de ciberriesgos; así, se consideran como riesgos diferenciados diversas circunstancias y causas relacionadas con las IT, y se tiende a prestar atención únicamente a la violación de datos personales (que en este sentido fue el primer aspecto que se reguló dentro del ordenamiento jurídico de EE. UU.). Sin embargo, y a la vista de los últimos acontecimientos a los que más adelante haremos referencia, se ha puesto de manifiesto que los posibles daños ocasionados por ciberriesgos son innumerables, y en ciertos casos exceden de la pérdida de datos o violación de la privacidad, llegando a producir daños físicos a terceros.

Los límites del actual concepto de ciberriesgos son muy amplios ya que cada informe y estudio que se publica aporta una nueva definición dependiendo del ámbito al que se dirige. No obstante, es necesario que aquí establezcamos la definición y características que entendemos que se adecúan con mayor certeza al concepto de ciberriesgos. Los aspectos relativos a la ciberseguridad han sido desarrollados de forma extensiva desde la perspectiva de la técnica informática, por lo que, como norma general, el concepto que encontramos en diversas publicaciones y estudios se refiere a un punto de vista práctico y funcional que por su naturaleza tiene un carácter amplio y ambiguo. Frente a tales definiciones técnicas, la presente investigación atiende al necesario rigor doctrinal propio del ordenamiento jurídico español y la utilidad pública de la investigación jurídica.

El profesor Juan Alberto Díez Ballesteros (2016) define «ciberriesgo» como cualquier situación en la que la utilización de internet, de las nuevas tecnologías o redes de la sociedad de la información puede implicar un eventual resultado dañoso para el usuario o un tercero, cualquiera que sea el medio o dispositivo utilizado (ordenador, tableta, teléfono, nube, etc.)[21], que, desde un punto de vista general, se denominan como riesgos operacionales para la información y los activos tecnológicos cuyas consecuencias pueden afectar a la confidencialidad, integridad y utilidad de los sistemas de datos o información[22].

El estudio *Cyber Risk*, publicado por The Institute of Risk Management, entiende por *cyber risk* cualquier riesgo o pérdida financiera, amenaza o daño para la reputación de una organización producido por cualquier fallo de seguridad en las IT[23].

---

21 Juan Alberto Díez Ballesteros, «Riesgos cibernéticos: daños propios, responsabilidad civil, pérdida de beneficio», XVIII Congreso de RC y Seguro, INESE (27 y 28 de junio de 2016).

22 Paul Kallenbach y Anthony Lloyd, «Perspectives on cyber risk», *MinterEllison* (enero de 2016), p. 2, http://www.minterellison.com/files/uploads/Documents/Publications/Reports%20Guides/RG_2016_Cyber-Report[150189].pdf

23 *Cyber Risk*, The Institute of Risk Management, CGI, IRM (2014), p. 8, https://www.theirm.org/media/883443/Final_IRM_Cyber-Risk_Exec-Summ_A5_low-res.pdf

En la ponencia «Insurance Cyber Risk de Tine Olsen», publicada por Willis en mayo de 2013, considera que los ciberriesgos se pueden definir como riesgos relacionados con la actividad *online*, las transacciones por internet, los sistemas electrónicos y herramientas tecnológicas y el almacenamiento de datos personales[24].

El New Zealand National Cyber Security Centre (NCSN) relaciona el concepto de ciberriesgos con el objeto del daño, estableciendo que cualquier activo electrónico es un objetivo potencial de un ciberataque contra toda la organización y sus socios[25]. En todo caso, los ciberriesgos ponen de manifiesto la preocupación por las amenazas que provienen del posible uso de las tecnologías y medios de información y comunicación con propósitos que perjudican e impiden la garantía de la seguridad y la estabilidad internacional tanto en el ámbito civil como el militar (conforme a lo establecido en el *Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security*, que se aprobó durante el 61.° plenary meeting el 2 de diciembre de 2008)[26].

Las definiciones que hasta aquí se han mencionado mantienen una serie de puntos básicos comunes aunque tengan circunstancias claramente diferenciadas, por lo que podemos destacar que se trata de aquella amenaza o posibilidad de que, como consecuencia del uso de las IT y por medio de una acción intencionada, o no, se ocasione un daño a los sistemas tecnológicos[27], la información almacenada en ellos o los sistemas que de ellos dependen, así como a los propios usuarios o terceros.

El informe *A Taxonomy of Operational Cyber Security Risks*[28] establece unas pautas por las que podemos definir con claridad los ciberriesgos determinando que son acciones u omisiones humanas que pueden ser voluntarias o no, que producen **un fallo en los sistemas tecnológicos y en los procesos internos de seguridad, lo que ocasiona un daño o efecto externo.** Estas pautas comprenden todos los aspectos que hemos ido manifestando, por lo que deben ser acogidas por el presente estudio como la definición de riesgos tecnológicos. Y la única diferencia entre riesgo tecnológico o informático, y ciberriesgo es el

24 «Insurance Cyber Risk», *Tine Olsen*, Willis (18 de julio de 2013), p. 7, http://www.pwc.dk/da/arrangementer/assets/cyber-tineolsen.pdf

25 «Cyber Security and Risk Management», *NCSC*, 2013, p. 2, http://www.ncsc.govt.nz/assets/cyber-security-risk-management-Executive.pdf

26 Shanghai Cooperation Organization, NATO Corporative Cyber Defence Centre of Excellence (16 de junio de 2009), https://ccdcoe.org/sco.html

27 *Guía Terminológica de Ciberseguridad*, AGERS, Madrid, 2017, p. 14.

28 James J. Cebula y Lisa R. Young, *A Taxonomy of Operational Cyber Security Risks*, Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA (diciembre de 2010), http://bit.ly/1NEBcTU

ámbito en el que se producen, de tal manera que los ciberriesgos se ocasionan en o por medio del ciberespacio y han sido la consecuencia del desarrollo de las IT.

1.2. Características de los ciberriesgos

La taxonomía de los riesgos operacionales se puede determinar conforme a sus cuatro aspectos fundamentales: la necesidad de que se produzca una acción humana, de que ocasione un fallo en los sistemas tecnológicos, y en los procesos internos de seguridad, y como consecuencia de estos, se produzca una serie de efectos externos.

Tabla 1. Características de los riesgos operativos

Acciones humanas	• Acciones involuntarias: errores u omisiones. • Acciones intencionadas: fraude, sabotaje, robo y vandalismo. • Acciones no intencionadas: falta de habilidades, conocimientos o capacidad.
Fallo de los sistemas tecnológicos	• Hardware: capacidad, mantenimiento y obsolescencia. • Software: compatibilidad, gestión de la configuración, cambio de control, ajustes de seguridad, prácticas de codificación y control. • Sistemas: diseño, integración y complejidad.
Fallo en los procesos internos	• Procesos de diseño y ejecución: procesos de transmisión de información, documentación; procesos de asignación de roles y responsabilidades; procesos de notificación y alerta. • Procesos de control: monitorización y revisión periódica. • Procesos de soporte: dotación de personal, financiación, capacitación, desarrollo y adquisiciones.
Eventos externos	• Desastres naturales: eventos climáticos, incendios, inundaciones, terremotos, disturbios y pandemia. • Problemas legales: *compliance*, regulación y litigios. • Problemas del negocio: fallos del proveedor, condiciones del mercado y condiciones económicas. • Servicio de los que depende la actividad: servicios públicos, servicios de emergencia, combustible y transporte.

Elaboración propia desde la fuente *Taxonomy of Operational Risk*[29].

29 James J. Cebula y Lisa R. Young, *A Taxonomy of Operational Cyber Security Risks*, Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 15213, p. 1 (diciembre de 2010), http://bit.ly/1NEBcTU

a) Acciones humanas

Los ciberriesgos son los riesgos operativos ocasionados por acciones u omisiones realizadas por personas que forman o no parte de la institución afectada (insiders o outsiders) de forma voluntaria o involuntaria, conforme las siguientes características:

- **Acciones involuntarias** ejercitadas inintencionadamente como consecuencia de fallos, errores u omisiones generalmente ocasionados por quien padece el daño o forma parte de la institución afectada.

- **Acciones intencionadas** que se ejercitan de forma voluntaria y ocasionan un fraude, sabotaje, robo o vandalismo.

- **Omisiones** que pueden ser causa de la falta del conocimiento, los sistemas o las habilidades adecuadas para actuar.

Es importante destacar que en la investigación que aquí desarrollamos se plantea el concepto de ciberriesgos desde el punto de vista de la responsabilidad y el daño. Por ello, aunque se puede llegar a aceptar que los ciberriesgos provengan de acciones de la naturaleza (aunque sea de forma muy restrictiva ya que la acción del hombre es esencial para el funcionamiento de las IT), nos referiremos, para establecer un concepto amplio de ciberevento, a las situaciones causadas tanto por la acción humana como por la naturaleza.

b) Fallo de los sistemas tecnológicos

Los fallos en los sistemas tecnológicos se caracterizan por tratarse del riesgo de que surja un problema operacional anormal e inesperado en los activos tecnológicos funcionales (hardware, software y sistemas integrados).

- Los riesgos relativos al hardware son consecuencia de la capacidad, del rendimiento, del mantenimiento y de la obsolescencia de los equipos físicos.

- Los riesgos ocasionados por el software (aplicaciones, programas y sistemas operativos) se deben a la compatibilidad, configuración, cambio de control, herramientas de seguridad, políticas de contraseñas y examen del sistema.

- Los causados como consecuencia de sistemas integrados se producen por los elementos del diseño, las especificaciones, la integración y la complejidad.

c) Fallo en los procesos internos

El fallo en los sistemas internos implica que estos no funcionan como se necesita o se espera, tal fallo puede ocurrir en diversas etapas entre las que se encuentran los procesos de diseño, soporte, control y ejecución de tareas.

- Los elementos que pueden producir fallos de diseño y ejecución son el diseño de los flujos de proceso, la fase de documentación, la distribución de roles y responsabilidades, los procesos de notificación y alerta, el de flujo de información, la distribución de tareas, la falta de acuerdos y condiciones, y el rechazo de tareas —o asignación errónea de tareas—.

- Los fallos en los procesos de control producen un inadecuado examen de los procesos operativos, y se deben a fallos en la monitorización y revisión de los sistemas o en el proceso de gobierno y gestión de los mismos.

- Los fallos en los procesos de soporte son riesgos operativos causados por un fallo organizativo en el sistema de soporte formado por los miembros del personal.

d) Efectos externos

Aunque en el informe *A Taxonomy of Operational Cyber Security Risks* al que hacemos referencia se incluyen los elementos externos como circunstancias por las que se ocasionan o producen los ciberriesgos, estas circunstancias se han explicado en el primer apartado por lo que no será necesario reiterar el concepto.

En otro sentido, los ciberriesgos deben **afectar a ciertos elementos externos** al sistema dañado para constituir un verdadero riesgo. Tal circunstancia se pone de manifiesto conforme a los efectos que el ciberespacio presenta en la realidad material, para lo cual será necesario que un evento que acontece en el ciberespacio **produzca un daño real,** cuyos efectos se deben desarrollar en el ámbito material, social, personal, empresarial, político, juridico institucional o económico.

El ámbito del ciberespacio es una característica determinante para cumplir con los requisitos que enmarcan ciertas actividades dentro de los cyber risks, como también lo es que exista un riesgo cuya definición queda dispuesta en el diccionario de la RAE como contingencia o proximidad de un daño, y se caracteriza por tener un carácter incierto o aleatorio, posible, concreto, lícito, fortuito y de contenido económico, cuya forma de manifestarse está en constante evolución. Así, los avances científicos y el desarrollo de la sociedad han propiciado la aparición de una serie de nuevos riesgos derivados de la actividad individual, empresarial y social[30].

30 J. Castelo Matrán y A. Guardiola Lozano, *Diccionario MAPFRE de Seguros*, Ed. FME, Madrid, 1992.

2. CIBERSEGURIDAD

La historia de la seguridad internacional es al mismo tiempo la historia de las innovaciones tecnológicas[31], y a su vez la historia de la humanidad se ha definido por medio de las diferentes guerras acontecidas por quienes luchaban y por la forma con la que lo hacían[32]. Desde el punto de vista de la innovación y el desarrollo tecnológico, el momento actual se ha definido por diversos expertos[33] como la Cuarta Revolución Industrial, cuyo efecto principal en el ámbito de la seguridad mundial es la capacidad de afectar a la realidad física y virtual. La previa revolución industrial aportó numerosos avances técnicos para el desarrollo global, pero además produjo una violenta transferencia de poder. De tal manera, podemos predecir que las innovaciones tecnológicas pueden continuar influyendo en la forma de comenzar los conflictos, quién participa en ellos, cuándo y cómo se producen, y dónde tienen lugar.

Los potenciales usos dañinos de la tecnología no siempre resultan evidentes y hasta ahora, para producir daños de gran relevancia, era necesaria la utilización de equipos de tecnología muy sofisticada, como las armas nucleares, que solo se encontraban en poder de algunos Estados. No obstante, las innovaciones que forman parte de la Cuarta Revolución Industrial[34] permiten que estos grandes daños sean causados por pequeños grupos e incluso por individuos independientes desde un ordenador personal. Por ello, las herramientas existentes para prevenir el aumento de conflictos, como los tratados, convenciones o estrategias (entre las que podemos destacar la denominada «mutually assured destruction»), son de dudosa efectividad cuando la capacidad destructiva ya no se limita a un grupo de entidades con recursos, tácticas e intereses similares[35].

---

31 A. Kaspersen y A. Hagan, «8 emerging technologies transforming international security». Forum Agenda 8 September 2015, https://agenda.weforum.org/2015/09/8-technologies-transforming-international-security/

32 A. Kaspersen, «What will militaries of the future look like?», Forum Agenda 12 August 2015, https://agenda.weforum.org/2015/08/what-will-militaries-of-the-futurelook- like/

33 Klaus Schwab, «The Fourth Industrial Revolution», World Economic Forum (2016).

34 E. B. Eide y A. Kaspersen, «The dark side of the Fourth Industrial Revolution – and how to avoid it» (10 de noviembre de 2015), https://agenda.weforum.org/2015/11/thedark- side-of-the-digital-revolution-and-how-to-avoid-it/

35 E. B. Eide y A. Kaspersen, «Cyberspace: The new frontier in warfare» (24 de septiembre de 2015), https://agenda.weforum.org/2015/09/cyberspace-the-new-frontier-inwarfare/

En conclusión, los elementos que se han señalado hacen que sea más sencillo atacar que defender un sistema de las posibles amenazas tecnológicas. Esta dinámica tiene un carácter histórico ya que internet fue concebido como un sistema en el que se prima la flexibilidad antes que la seguridad. Y, además, la dinámica de la ciberseguridad hace que quien ataca únicamente necesite encontrar una vulnerabilidad en un momento determinado, mientras que para asegurar un sistema se debe defender en todo momento cada punto vulnerable en concreto[36]. Y en definitiva, **el ciberespacio ha abierto una nueva frontera para la producción de daños de cualquier escala,** ya que todo está conectado a la Red y todo lo que está conectado a la ella puede sufrir algún ataque[37].

2.1. El mercado de la ciberseguridad

Una de las características fundamentales de los riesgos globales y en especial de los ciberriesgos es la interconectividad, y tal circunstancia pone de manifiesto que este tipo de riesgos no pueden ser tratados de forma aislada[38]. Además, esto hace que sea muy difícil el seguimiento de las partidas presupuestarias y los gastos relacionados con la ciberseguridad debido a que se llevan a cabo desde muchas áreas de negocio (que abarcan desde el ámbito tecnológico e informático hasta los recursos humanos y la formación)[39]. No obstante, los riesgos tecnológicos han alcanzado tal notoriedad que el mercado de la seguridad informática se ha convertido en uno de los sectores con mayor crecimiento.

El mercado de la ciberseguridad es el sector que más rápido ha crecido dentro del ámbito tecnológico. Mientras que todos los demás sectores se impulsan en elementos tradicionales como la reducción de las ineficiencias y el aumento de la productividad, el gasto en seguridad cibernética se impulsa por el efecto negativo de los ciberataques. Por este motivo, resulta complicado estimar los futuros gastos en ciberseguridad ya que, como hemos visto en otros puntos, las ciberamenazas manifiestan una evolución constante sobre la que es muy difícil elaborar predicciones[40].

---

36 Global Risks Report 2014, p. 39.

37 E. B. Eide y A. Kaspersen, *op. cit.*, Forum Agenda (24 de septiembre de 2015), https://agenda.weforum.org/2015/09/cyberspace-the-new-frontier-inwarfare/

38 *Op. cit.*, World Economic Forum (2015), p. 22.

39 *The IT Security Spending Survey*, SANS Institute (febrero de 2016), https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697

40 Steven C. Morgan, «The Cybersecurity Market Report, Q3 2016», *Cybersecurity Ventures* (2016), http://cybersecurityventures.com/cybersecurity-market-report/

Las estimaciones que presentan las fuentes consultadas para el periodo comprendido entre los años 2017 y 2021 hacen prever que el gasto mundial en seguridad informática alcanzará 1 trillón de USD. En este mismo sentido, numerosas empresas han aumentado los presupuestos destinados a la seguridad cibernética: JP Morgan Chase & Co. duplicó su presupuesto anual de seguridad cibernética para el 2017 pasando de 250 millones a 500 millones USD; Bank of America ha asegurado tener un presupuesto ilimitado para la lucha contra la delincuencia informática. El Gobierno de Estados Unidos ha aumentado su presupuesto anual de seguridad cibernética en un 35 %, al pasar de 14.000 millones de USD presupuestados en 2016 a 19.000 millones de USD en 2017[41]. Las empresas que formaron parte del estudio *PwC Estado Mundial de la Encuesta de Seguridad de la Información 2016* aumentaron sus presupuestos de seguridad de la información en un 24 % en 2015[42].

La compañía de investigación de mercado Gartner estima que el gasto en seguridad de las IT alcanzará los 2,77 billones de USD, con lo que crecerá un 13,9 % con respecto a los 75,4 mil millones que se gastaron en 2015 (o un 25 % si se incluye el gasto de externalización de servicios). Asimismo, Gartner prevé que el mercado global de seguridad crezca con una tasa anual del 7,8 % hasta el 2019. No obstante, hasta el 2019 el gasto en ciberseguridad solo representará un 5 % del gasto total en IT, aunque otros estudios apuntan a que la cifra de gasto anual en seguridad pueda ser mayor[43]. En 2004, el valor del mercado mundial de seguridad cibernética era de 3,5 billones, y se estima que en el 2017 alcance los 120 billones de USD, y en 2020, 170 billones de USD[44].

Por sectores, el aeroespacial, defensa e inteligencia continúan siendo los ámbitos que más contribuyen al desarrollo de tecnología enfocada a la seguridad de las IT. Y por áreas geográficas, EE. UU., Canadá y Europa son los principales contribuyentes del gasto en ciberseguridad, y China e India[45]

41 Steven C. Morgan, «The Cybersecurity Market Report», Q3 2016, *Cybersecurity Ventures*, 2016, http://cybersecurityventures.com/cybersecurity-market-report/

42 *The Global State of Information Security Survey*, PWC, 2016, http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

43 «Why cybersecurity is so important», *BI Intelligence* (5 de abril de 2016), http://www.businesinsider.com/cybersecurity-report-threats-and-opportunities-2016-3

44 Cyber Security Market by Solutions, *marketsandmarkets.com* (julio de 2016), http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html

45 Steve Morgan, «Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020» (diciembre de 2015), http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#526a3f592191

constituyen un mercado potencial para los proveedores de servicios de ciberseguridad igual que el resto de países emergentes[46].

En cuanto al gasto público, durante los años 2006 y 2017 aumentó un 14,5 % anual en EE. UU., superando el aumento del gasto en adquisiciones de cualquier otro programa público. Y como propuesta para el año 2017, el Gobierno de EE. UU. anunció que invertirá más de 19 mil millones de USD, lo que conllevará un aumento del 35 % con respecto al año 2016 de los recursos públicos dedicados a la ciberseguridad en general[47]. La demanda de productos y servicios de ciberseguridad por parte del Gobierno Federal de Estados Unidos aumentará de 8,6 billones en el año 2015 a 11 billones de USD en 2020, lo que determina una tasa de crecimiento anual del 5,2 %, y se estima que alcanzará en 2020 el 10 % del presupuesto total destinado a la IT[48].

El mercado de la ciberseguridad es la industria con más crecimiento dentro del sector tecnológico de la Unión Europea y presenta grandes oportunidades de negocio. La Comisión Europea anunció el 5 de julio de 2016 la creción de un acuerdo público y privado (The contractual Public-Private Partnership —cPPP— on cybersecurity) para mejorar la ciberseguridad y la capacidad del mercado europeo, con los objetivos de fortalecer esta industria, generar oportunidades de negocio, reforzar la confianza de los ciudadanos en el ámbito digital y contribuir a los objetivos estratégicos del mercado digital común. Con este programa la Unión Europea prevé destinar 450 billones de euros de sus fondos de forma directa al sector de la ciberseguridad y estima que tal inversión generará 1,8 billones de euros[49].

Por otra parte, se pueden destacar los buenos resultados que aportan este tipo de servicios a las compañías del sector tecnológico para las que se trata de un mercado estratégico. Entre los mayores proveedores de servicios de ciberseguridad se encuentran las principales empresas de servicios tecnológicos a nivel mundial como IBM Corporations, Intel Corporation, Booz Allen Hamilton, CSC, Lockheed Martin, Northrop Grumman, Sophos, Symantec y Trend Micro[50]. IBM y Cisco han invertido 2.000 y 1.750 millones de dólares,

46 Steven C. Morgan, «The Cybersecurity Market Report, Q3 2016», *Cybersecurity Ventures* (2016), http://cybersecurityventures.com/cybersecurity-market-report/

47 *Cybersecurity National Action Plan*, The White House Office of the Press Secretary, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national action-plan

48 Federal Information Security Market 2015-2020, *Deltek*, http://more.deltek.com/Federal-Information-Security-Market-2015-2020

49 Cybersecurity industry, Digital Single Market Digital Economy & Society, European Commission (2016), https://ec.europa.eu/digital-single-market/en/cybersecurity-industry

50 Cyber Security Market, *marketsandmarkets.com* (2016), http://www.marketsandmarkets.com/PressReleases/cyber-security.asp

respectivamente, en la adquisición de empresas de seguridad cibernética y ambos están creciendo de manera constante (IBM Security creció un 20 % en el primer trimestre de 2016).

2.2. Características y protocolos de la ciberseguridad

La U.S. NIST Cybersecurity Framework establece que los principales elementos de la ciberseguridad son **identificación, protección, detección, respuesta y recuperación,** entre los que podemos destacar las siguientes características[51]:

a) Identificación

La identificación es el proceso a través del cual se desarrolla conocimiento sobre el sistema, datos, activos y capacidad. Puede realizarse mediante la gestión de activos, el estudio del ámbito del negocio, la evaluación de riesgos y la estrategia de gestión de riesgos.

Desde un punto de vista orgánico y estructural se pueden llevar a cabo ciertas acciones que permiten advertir los riesgos, priorizar y asignar recursos adecuadamente con mayor facilidad. Entre ellas podemos destacar:

- El desarrollo de una estructura de gobierno que permita atender a los problemas relacionados con los ciberriesgos integrando sistemas de *compliance* que se dirigen a la prevención, detección y respuesta ante los riesgos derivados del incumplimiento[52].

- La creación e implementación de la figura del Chief Information Security Officer (CISO).

Y, además, el acceso a la información sobre la naturaleza cambiante de los ciberriesgos es una herramienta esencial para identificar y preparar estrategias preventivas. Por este motivo han surgido diversos grupos y comunidades que recopilan y comparten esta información, como son en el sector financiero CHEF (within the Financial Services Information Sharing and Analysis Center —FSISAC—) y GLEX (within the World Federation of Exchanges).

---

51 NIST Cybersecurity Framework, Cyber Security in Securities Markets – An International Perspective, IOSCO, p. 25, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf

52 Alain Casanovas Ysla (coord.), *Libro blanco sobre la función del Compliance*, Asociación Española de Compliance, Madrid (marzo de 2017), p. 5.

b) Protección

Se desarrolla mediante la implementación de las medidas de seguridad adecuadas que normalmente tienen relación con el control de acceso, seguridad de datos, medidas de formación, concienciación e información sobre los procedimientos. Estas pueden ser de carácter organizacional o tecnológico, que a su vez se pueden clasificar según se traten de políticas de control y gestión tecnológica (como el *Compliance* tecnológico), controles de seguridad (como las políticas de seguridad de acceso a los sistemas, optimización de contraseñas, la monitorización del mail y de sistemas que albergan información sensible, o la utilización de test de vulnerabilidad) y tecnologías de protección (como los firewalls, antivirus y antimalware, los Intrusion Prevention System y los Intrusion Detection System, sistemas de defensa de DDoS, plan de prevención de la pérdida de datos o los filtros antispam)[53].

Algunas compañías utilizan los denominados «red team» o test de penetración («penetration testers») para tratar de vulnerar sus propios sistemas de seguridad con el objetivo de descubrir sus debilidades. Estos sistemas de seguridad preventiva surgieron en 1979 cuando ARPANet todavía no se había transformado en el internet moderno y los protocolos TCP/IP aún no eran estándar.

c) Detección

Conlleva el desarrollo e implementación de actividades que permitan identificar un posible evento que comprometa la ciberseguridad (como los procesos de detección y monitorización). Los sistemas internos y externos de monitorización son una herramienta eficaz para la temprana detección de ciberamenazas. En el caso de los ciberataques, es esencial la rápida detección e intervención, ya que el tiempo de reacción puede ser utilizado para acceder a los privilegios y controles de un sistema crítico e impedir la efectividad de la respuesta.

Además de los sistemas de monitorización existen otras herramientas cuya utilización es más común entre las organizaciones de cualquier índole, como los sistemas de recopilación de información, sistemas de detección de virus y malware, escáneres de vulnerabilidades y tests de penetración, y la creación de grupos o comunidades para compartir información y conocimiento sobre los ciberriesgos.

---

53 AMCC TF Report and AMCC WG, NIST Cybersecurity Framework, Cyber Security in Securities Markets – An International Perspective, IOSCO, p. 25, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf

d) Respuesta

Las actividades de respuesta ante las ciberamenazas se basan en el desarrollo o implementación de acciones que permitan tomar medidas una vez se detecta el evento. Entre ellos destacan los planes de comunicación, análisis, mitigación y mejora. No obstante, para que un plan de respuesta contra las ciberamenazas sea efectivo, es necesario que se adecúe a las particularidades de la organización y de su sector.

Por medio de los planes de comunicación se transmite información relevante sobre las circunstancias y efectos del ciberevento a los socios, proveedores, clientes, colaboradores y personal de la corporación que pueda resultar afectado. El análisis forense *(forensic analysis)* permite entender la anatomía de las ciberamenazas, detectar los efectos de las mismas y la extensión del daño, y determinar las responsabilidades.

La creación de bases de datos para recopilar los efectos y el funcionamiento de los ciberataques permite transmitir el conocimiento y la experiencia por toda la estructura de la organización. Y ello, junto con la realización de simulacros periódicos de actuación, permite optimizar los tiempos de reacción para eventos futuros.

Durante los últimos años se han creados diversos simulacros como el test de respuesta, coordinación y resolución de ciberincidentes Quantum Dawn del SIFMA para instituciones del sector financiero patrocinado por el U.S. Department of the Treasury, el IIROC del TSX (la principal sociedad de bolsa canadiense) y el CBEST en Reino Unido.

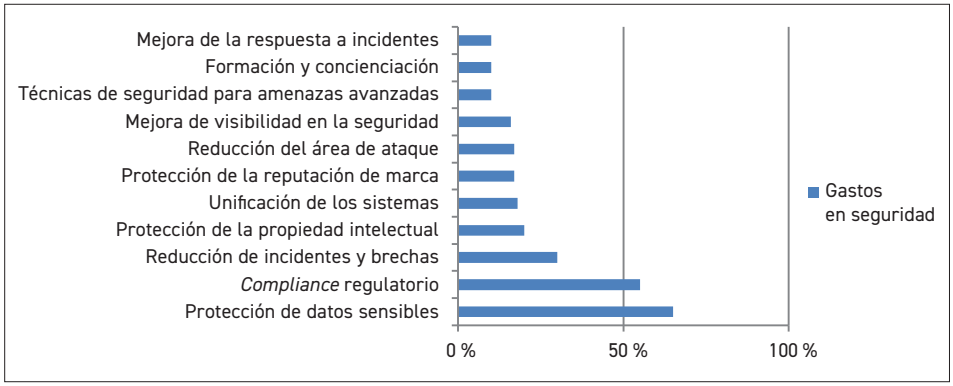
e) Recuperación

Por medio de estas acciones se trata de desarrollar e implementar planes de defensa y de restablecimiento de las funciones y servicios que hayan resultado dañados. En el plan de recuperación se define los denominados puntos objeto de recuperación RPO (Recovery Point Objective) sobre los que se actúa desde diversos ámbitos como el operacional, financiero, legal o reputacional.

Las acciones de seguridad que hasta aquí se han desarrollado (identificación, protección, detección y respuesta) implican uno de los gastos con mayor crecimiento dentro de las compañías y organizaciones de diversos sectores. Actualmente, el gasto se está focalizando en el desarrollo de sistemas de protección, en los sistemas de protección de datos y en los planes de *Compliance* regulatorio, seguidos por el entrenamiento y los programas de información interna que en 2016 comenzaron a formar parte de los principales gastos en seguridad con un importante impulso de la práctica

de análisis forenses para detectar vulnerabilidades y efectos de las ciberamenazas[54].

Gráfico 1. Gasto en seguridad



Elaboración propia desde la fuente *IT Security Spending Trends*, SANS Institute[55].

Como hemos mencionado, atendiendo a los datos de SANS Institute, los sistemas de *Compliance* y de protección de datos fueron las políticas de seguridad en las que más invirtieron las organizaciones[56].

Entre las compañías que más recursos dedicaron a estos planes de seguridad destacan las entidades financieras, bancos y aseguradoras, tanto por las particulares regulaciones a las que suelen estar sometidas, como por la importancia y sensibilidad de los datos con los que trabajan[57].

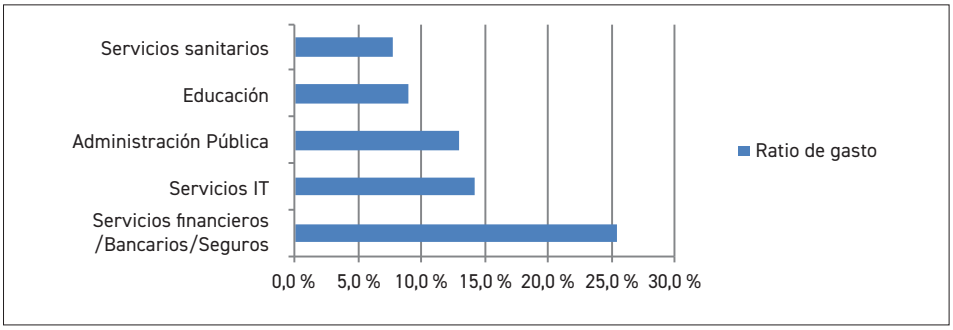
54 Barbara Filkins, *IT Security Spending Trends*, SANS Institute (febrero de 2016), p. 1, https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697

55 Barbara Filkins, *op. cit.*, SANS Institute (febrero de 2016), p. 4.

56 Barbara Filkins, *op. cit.*, SANS Institute (febrero de 2016), p. 4.

57 Barbara Filkins, *op. cit.*, SANS Institute (febrero de 2016), p. 4.

Gráfico 2. Cinco industrias principales



Elaboración propia desde la fuente *IT Security Spending Trends*, SANS Institute[58].

Además, el volumen de recursos que se dedican a los planes de ciberseguridad depende proporcionalmente del tamaño de la organización. De manera que las compañías de mayor tamaño aplican muchos más recursos en ciberseguridad que las compañías más pequeñas.

Tabla 2. Clasificación del gasto en ciberseguridad

Clasificación	% Presupuesto de seguridad		
	FY 2014	FY 2015	FY 2016
Grandes	4–6 %	4–6 %	7–9 %
Medianas	4–6 %	4–6 %	7–9 %
Pequeñas	3–4 %	4–6 %	6–7 %

Elaboración propia desde la fuente *IT Security Spending Trends*, SANS Institute[59].

La continua necesidad de mejora de las herramientas que facilitan la resolución de ciberevenos hace que las organizaciones busquen, en primer lugar, personal y herramientas para la detención y la respuesta; y después, las herramientas a las que más recursos se dedican son las de detección y análisis forense. Todo ello sin olvidar la inversión en formación y en la creación de equipos humanos con elevados conocimientos en la materia, lo que permite que la ciberseguridad se trate con la importancia debida.

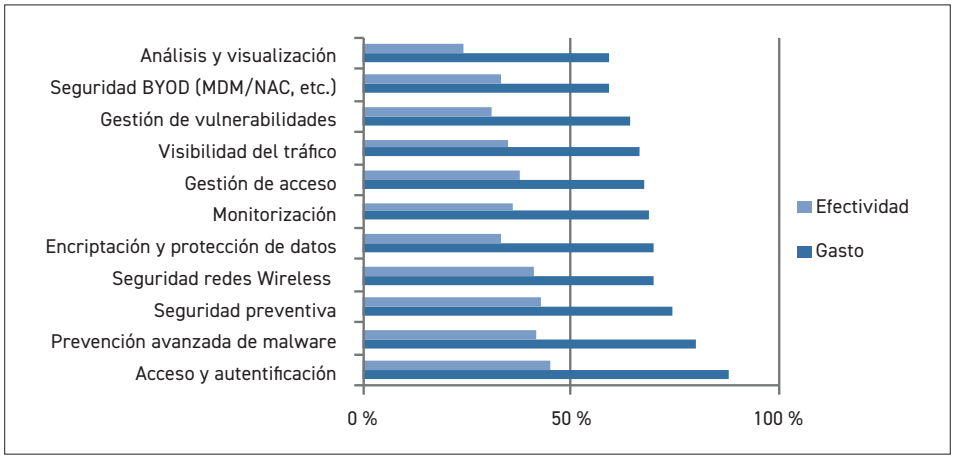
Las organizaciones están recurriendo principalmente a servicios externos de ciberseguridad para la capacitación del usuario final, la sensibilización y for-

58 Barbara Filkins, *op. cit.*, SANS Institute (febrero de 2016), p. 4.

59 Table 4. Median Budget and Percentage Allocated to Security by Year by Organization Size, Barbara Filkins, *op. cit.*, SANS Institute (febrero de 2016), p. 6.

mación del personal, la certificación, la obtención de experiencia en la materia, el *Compliance* y auditoría de sus sistemas. Entre los principales servicios de seguridad por el nivel de gasto y efectividad podemos clasificar:

Gráfico 3. Efectividad del gasto en tecnología



Elaboración propia desde la fuente *IT Security Spending Trends*, SANS Institute[60].

En términos generales, para definir los principales protocolos de seguridad podemos seguir la *Guide to Cyber Risk* publicada por Allianz en la que se recomiendan diez pasos para reforzar las medidas de seguridad:

1. La gestión de acceso e identidad que permiten la verificación y el control del acceso de los usuarios (*Identity and Access Management* —IAM—[61]).

2. La gestión de riesgos y *Compliance*, con el objetivo de asegurar que los actos de una organización sean acordes con la ética, los riesgos y las políticas internas previamente definidas. Y que todos ellos cumplan a su vez con la regulación aplicable al caso mediante la implementación de procedimientos, estrategias y medios de formación interno *(Risk and Compliance Management)*[62].

60 Table 9. Technology Spending and Effectiveness, *op. cit.*, SANS Institute (febrero de 2016), p. 6.

61 Definition «Identity Access Management (IAM) system», TechTarget, *SearchSecurity*, http://searchsecurity.techtarget.com/definition/identity-access-management-IAM-system.

62 Nicolas Racz, Edgar Weippl, Andreas Seufert, *A process model for integrated IT governance, risk, and compliance management*, TU Vienna, Institute for Software Technology and Interactive.

3. Los sistemas de encriptación de datos que protegen el contenido y la integridad de los datos confidenciales *(Encryption)*[63].

4. Los sistemas de prevención de pérdida de datos por medio de los que se establecen estrategias e implementan software que impiden la pérdida de datos sensibles y la gestión adecuada de los mismos (*Data Loss Prevention* —DLP—)[64], la gestión unificada de las amenazas que permite gestionar múltiples funciones de seguridad desde un mismo sistema o software *(Unified Threat Management)*.

5. Los cortafuegos que establecen una barrera entre las redes de confianza y el resto de redes, permitiendo que solo acceda el tráfico que cumpla con las políticas previamente definidas *(firewall)*[65].

6. El software antivirus y antimalware que permite identificar y expulsar las diferentes formas de software malicioso[66].

7. Los sistemas de detención de intrusiones son herramientas de control que actúan como un firewall analizando el tráfico de entrada y bloqueando los ataques a la Red, mientras que los sistemas de prevención de intrusiones es una herramienta de análisis que facilita la monitorización del tráfico de una red *(Intrusion Detection System —IDS—/Intrusion Prevention System —IPS—)*[67].

8. Los planes de gestión de vulnerabilidades comprenden el desarrollo de sistemas y procesos que permiten identificar y analizar puntos débiles tanto en el software como en el hardware que puedan exponer el sistema a ciberataques *(Security and vulnerability management)*[68].

9. Los planes de recuperación de desastres forman parte del área de seguridad que protege a la organización de los efectos de cualquier evento

---

63 Definition «encryption», TechTarget, *SearchSecurity,* http://searchsecurity.techtarget.com/definition/encryption

64 Definition «Data Loss Prevention (DLP)», *Whatls,* http://whatis.techtarget.com/definition/data loss-prevention-DLP

65 Definition «firewall», TechTarget, *SearchSecurity,* http://searchsecurity.techtarget.com/definition/firewall

66 Definition «antimalware», TechTarget, *SearchSecurity,* http://searchsecurity.techtarget.com/definition/antimalware

67 Do you need an IDS or IPS, or both?, TechTarget, *SearchSecurity,* http://searchsecurity.techtarget.com/Do-you-need-an-IDS-or-IPS-or-both

68 Definition «vulnerability management planning», *whatls.com,* http://whatis.techtarget.com/definition/vulnerability-management

negativo ya tengan relación con las IT o provengan de desastres naturales *(Disaster recovery)* [69].

10. Los sistemas de protección contra los ataques DDoS tratan de identificar y suprimir los paquetes de datos enviados de forma maliciosa permitiendo que el sistema siga funcionado durante el ataque mediante el control del tráfico de acceso. Los software de filtrado de web son aquellos programas que determinan si un sitio web o parte del contenido del mismo debe ser mostrado al usuario y permiten suprimir de forma automática aquellos contenidos que no estén permitidos por sus protocolos *(Web filtering)*[70].

Otro ámbito al que podemos hacer referencia por el potencial efecto que sobre él pueden tener los cibereventos es el sector industrial. Además, frente a los daños puramente patrimoniales propios del sector financiero, los cibereventos que afectan a los sistemas de control industrial pueden llegar a ocasionar otro tipo de daños como la interrupción del negocio o los daños materiales. Y la mayoría de los sistemas de control industrial utilizados actualmente fueron diseñados antes de que los ciberriesgos se convirtieran en una preocupación prioritaria, lo que dificulta la protección de estos sistemas. De esta forma, los sistemas de control industrial pueden ser vulnerables por causa de fallos técnicos y errores operativos, lo que aumenta la probabilidad de frecuencia con la que se producen. Y dentro de este ámbito, en 2014 en EE. UU., el sector energético y la industria manufacturera fueron los que más incidentes sufrieron[71].

El principal ejemplo de estos eventos ha sido el ciberataque que sufrió en 2010 la central nuclear de Natanz (Irán) atribuido al gusano informático Stuxnet creado por el ejército de Israel. Así, se puede advertir de las innumerables posibilidades de daño que podrían llegar a producir estos eventos como la interrupción durante horas o días de una planta energética o la introducción de un error en la fabricación de un producto[72].

---

69 Definition «disaster recovery», TechTarget, *SearchSecurity*, http://searchdisasterrecovery.techtarget.com/definition/disaster-recovery

70 Definition «Web filter», TechTarget, *SearchSecurity*, http://searchsecurity.techtarget.com/definition/Web-filter

71 Industrial Control Systems Cyber Emergency Response Team, US Department of Homeland Security, https://www.dhs.gov/sites/default/files/publications/DHS%20Federal%20Government_4.7.edIT__0.pdf

72 Allianz Global Corporate & Specialty, *A Guide to Cyber Risk*, p. 12, https://www.allianz.com/v_1441789023000 /media/press/document/other/Allianz_Global_Corporate_Specialty_Cyber_Guide_final.pdf

2.3. Clasificación y estadística de los principales riesgos

Los ciberriesgos provienen de diversas fuentes y se manifiestan de formas distintas. Existe una gran cantidad de circunstancias y acciones capaces de producir un daño por medio del ciberespacio. Como se ha visto, los diferentes aspectos del ámbito de las IT están en constante evolución y por ello cada día surgen nuevas formas a través de las cuales se pueden producir ataques, o vulnerabilidades, que a la postre ocasionan los daños a los que nos venimos refiriendo. Y, siguiendo el sistema AVOIDIT[73] (creado por el Department of Computer Science de la University of Memphis sobre la base del sistema VERDICT[74] y de los sistemas creados por Kjaerland[75] y Howard[76]) mediante el que se define la taxonomía de los riesgos potenciales para el ciberespacio, los ciberriesgos o cibereventos se pueden clasificar conforme a sus cinco características principales:

1. **Vector de ataque** («atack vector») que determina el medio o vulnerabilidad que permite la producción del daño, entre los que podemos destacar:

   - *Misconfiguration*, en este caso los atacantes se valen de un fallo de configuración para obtener acceso a los sistemas[77].

   - *Kernel Flaws*, consisten en la utilización de un defecto en el núcleo del sistema operativo para obtener ciertos privilegios de acceso que permiten explotar vulnerabilidades.

   - *Buffer Overflow*, el desbordamiento del buffer que se produce cuando parte del código no se revisa adecuadamente por tener una extensión o tamaño inapropiado lo que, a su vez, ocasiona un cúmulo de datos[78] que se reasignan de manera inadecuada.

---

73 Chris Simmons, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Qishi Wu, Department of Computer Science University of Memphis Memphis, TN, USA, http://ais.cs.memphis.edu/files/papers/CyberAttackTaxonomy_IEEE_Mag.pdf

74 Daniel Lough, *A Taxonomy of Computer Attacks with Applications to Wireless Networks*, PhD thesis, Virginia Polytechnic Institute and State University, 2001.

75 M. Kjaerland, «A taxonomy and comparison of computer securityincidents from the commercial and government sectors», *Computers and Security*, 25, pp. 522-538 (octubre de 2005).

76 John D. Howard y Thomas A. Longstaff, *A Common Language for Computer Security Incidents*, Technical report, Sandia National Laboratories, 1998.

77 K. Scarfone, M. Souppaya et al., «Technical Guide to Information Security Testing and Assessment». NIST (septiembre de 2008), http://web.nvd.nist.gov/view/vuln/detail?execution=e7s1

78 S. Hansman y R. Hunt, «A taxonomy of network and computer attacks», *Computer and Security* (2005).

- *Insufficient Input Validation*, el programa falla al validar las entradas de los usuarios[79], y esto permite explotar vulnerabilidades del sistema de valoración introduciendo código de forma arbitraria. Este sistema se aplica generalmente contra las aplicaciones web.

- *Symbolic Links*, se trata de explotar las vulnerabilidades que pueden existir entre los enlaces de un fichero y el programa que tiene derechos de escritura sobre él.

- *File Descriptor*, es un programa que utiliza los números del sistema en lugar de nombre de los archivos para llevar el seguimiento de los mismos[80]. Las vulnerabilidades de estos sistemas otorgan un acceso privilegiado a los archivos relacionados.

- *Race Condition*, se produce cuando un programa intenta ejecutar un proceso y el objeto cambia en el mismo momento a otra referencia que permite obtener privilegios elevados durante el tiempo en el que el programa concede privilegios de acceso[81].

- *Incorrect File/Directory Permission*, se produce cuando un programa concede permisos privilegiados al no asignar correctamente usuarios y procesos.

- *Social Engineering*, es el sistema que utiliza la interacción social para obtener información sobre la víctima o el sistema que, a su vez, permite acceder al mismo.

2. **Impacto operativo** («Operational Impact»), una vez producido el colapso o error del sistema se pueden ocasionar diversos efectos. En este apartado nos centraremos en los efectos operativos de los ciberataques, entre los que destacan:

   - *Misuse of Resources:* implica el uso no autorizado de los recursos de las IT[82] que requieren de ciertos privilegios y su utilización por parte del atacante para impedir el acceso a los usuarios.

---

79 K. Scarfone, M. Souppaya et al., «Technical Guide to Information Security Testing and Assessment», NIST (septiembre de 2008), http://web.nvd.nist.gov/view/vuln/detail?execution=e7s1

80 K. Scarfone, M. Souppaya *et al.*, *op. cit.* NIST (septiembre de 2008), http://web.nvd.nist.gov/view/vuln/detail?execution=e7s1

81 K. Scarfone, M. Souppaya, *op. cit.*, NIST (septiembre de 2008), http://web.nvd.nist.gov/view/vuln/detail?execution=e7s1

82 M. Kjaerland, *op. cit. Computers and Security* (octubre de 2005).

- *User Compromise:* comprende la obtención de los privilegios de acceso como usuario por parte de un sujeto no autorizado[83].

- *Root Compromise:* implica la obtención de los privilegios de acceso como administrador de sistema por parte de un usuario.

- *Web Compromise:* es la utilización de las vulnerabilidades de un programa web para facilitar un ataque contra otro sistema[84] (este ciberataque normalmente implica la utilización de *site scripting* o *SQL injection*).

- *Installed Malware:* es una de las formas más habituales de ciberataque, y requiere la instalación de programas de malware para explotar las vulnerabilidades de los sistemas afectados. Mediante estos programas se puede llegar a obtener el control del sistema, por lo que se han clasificado según las funciones que resultan afectadas en los siguientes grupos:

  a. *Virus:* es un código capaz de atacar al propio sistema por medio de archivos infectados que se reproducen por medio de la ejecución de un programa.

  b. *Spyware:* es un tipo de malware que se instala en un sistema para recopilar y enviar información sobre el mismo.

  c. *Trojan:* permite la creación de «una puerta trasera» que da acceso al sistema. Este tipo de malware permite ejecutar diversos ciberataques por medio del acceso obtenido.

  d. *Worms:* es un programa que se reproduce automáticamente sin necesidad de intervención, lo que permite ataques en masa.

  e. *Arbitrary Code Execution:* se ejecutan por medio de una vulnerabilidad que permite al atacante introducir su propio código en el sistema y así obtener acceso a este[85].

- *Denial of Service:* se ha convertido en una de las principales amenazas para el ciberespacio[86] cuyo objetivo es denegar el acceso a los usuarios a unos recursos o sistema en particular. Existen tres tipos de ataques DDoS:

83 M. Kjaerland, *op. cit. Computers and Security* (octubre de 2005).

84 M. Kjaerland, *op. cit. Computers and Security* (octubre de 2005).

85 C. Douligeris y A. Mitrokotsa, «DDoS Attacks and Defense Mechanisms: Classification and State-of-theart», *Comp. Networks*, vol. 44 (2004), pp. 643-666.

86 C. Douligeris y A. Mitrokotsa, *op. cit.*, *Comp. Networks*, vol. 44 (2004), pp. 643-666.

los *Host Based*, que se dirigen contra un sistema en concreto y tratan de consumir todos sus recursos[87]; los Network Based, que es el sistema de inundación por paquetes[88] que ataca a la conectividad y el ancho de banda de diversos ordenadores para impedir que ofrezcan un sistema apropiado[89]; y los *Distributed*, a través de los que en primer lugar se obtiene el control de varios sistemas mediante malware, que en segundo lugar permitirán ejecutar el ataque contra el objetivo, ya sea por medio de la utilización del ancho de banda de los sistemas controlados *(network-centric)* o a través de un ataque conjunto que sobrecargue el servicio *(application-layer)*[90].

3. **Impacto en la información** («Informational Impact»). Podemos clasificar las ciberamenazas conforme a los efectos que pueden producir con relación a la información confidencial y los datos de carácter privado.

   - *Distort:* produce un cambio o modificación en los archivos y datos afectados[91].
   - *Disrupt*, por el que se impide el acceso de los usuarios a un sistema concreto, normalmente por medio de la modificación de las claves o alteración del sistema de acceso.
   - *Destruct:* se trata de una de las ciberamenazas que más daños producen[92] y comporta la destrucción o inutilización de archivos y datos.
   - *Disclosure:* define en términos generales cualquier revelación de datos no autorizada.
   - *Discovery:* es la revelación de información oculta sobre el sistema que en algunas ocasiones permite detectar vulnerabilidades.

4. **Objetivo** («Target»): el objeto susceptible de ser dañado como objetivo de ciberataques, o por el efecto de daños involuntarios que procedan de un ciberriesgo de carácter no intencional o accidente puede clasificarse conforme a los siguientes apartados:

---

87 S. Hansman y R. Hunt, «A taxonomy of network and computer attacks», *Computer and Security* (2005).

88 S. Hansman y R. Hunt, *op. cit.*, *Computer and Security* (2005).

89 C. Douligeris y A. Mitrokotsa, «DDoS Attacks and Defense Mechanisms: Classification and State-of-theart», *Comp. Networks*, vol. 44 (2004), pp. 643-666.

90 «How to prepare for the emerging threats to your systems and data, essential guide, techtarget», http://searchsecurity.techtarget.com/essentialguide/How-to-prepare-for-the-emerging-threats-to-your-systems-and-data

91 M. Kjaerland, *op. cit*, *Computers and Security* (octubre de 2005).

92 M. Kjaerland, *op. cit. Computers and Security* (octubre de 2005).

- *Operating System:* daña el sistema operativo que es el responsable de la coordinación de actividades y distribución de recursos de una red o sistema concreto.
- *Network:* el objeto, una red formada por diferentes sistemas u ordenadores.
- *Local:* cuando el objeto es un sistema u ordenador concreto con independencia de los usuarios.
- *User:* el daño se produce sobre un usuario concreto.
- *Application:* en este caso el objeto es una aplicación o programa concreto que puede ser *client* (programa que permite a los usuarios realizar acciones comunes) o *server* (diseñado para servir como host).

5. **Defensa** («Defense»): frente a las ciberamenazas existen diversos tipos de defensa, que en términos generales se pueden clasificar según sean métodos preventivos o tengan por objeto dar solución a un daño padecido o vulnerabilidad existente.

   Los ciberriesgos tienen un efecto especialmente perjudicial en la industria financiera. Las instituciones financieras y demás compañías que operan en este ámbito padecen las ciberamenazas por su especial dependencia con la conectividad y la relevancia de los datos en sus operaciones.

   Estas dos características hacen que las compañías de trading sean especialmente vulnerables, por lo que asegurar la integridad de los datos con los que trabajan estas instituciones debería ser una de las principales prioridades del sector financiero, después de la capacidad del propio sistema.

   Los elementos esenciales de la vulnerabilidad de las operaciones de trading nos pueden servir de ejemplo para comprender los puntos en los que se deben aplicar con mayor empeño los protocolos de ciberseguridad[93]. Siguiendo la clasificación del informe *Cyber Security in Securities Markets* de IOSCO podemos distinguir siete operaciones dentro de un sistema de trading en las que se ponen de manifiesto unas vulnerabilidades en particular[94]:

---

93 «AP Twitter Feed Hacked; No Attack at White House», *USA Today* (23 de abril de 2013), http://www.usatoday.com/story/theoval/2013/04/23/obama-carney-associated-press-hackwhite house/2106757/

94 AMCC TF on Cyber Resilience and AMCC Working Group, *Cyber Security in Securities Markets An International Perspective*, IOSCO (abril de 2016), pp. 23 y 24, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf

a. *Pre-trade:* en este momento pueden producirse accesos no autorizados que permitan:

   - la utilización fraudulenta de los algoritmos de operación automáticos;
   - intervenir el sistema de gestión para activar órdenes falsas;
   - carga de virus o archivos corruptos durante la transmisión de datos;
   - manipular los índices de cálculo;
   - publicar mediante diferentes medios información falsa que desencadene operaciones.

b. *Execution:* durante esta fase los efectos que los ciberriesgos pueden causar al sistema de *trade* son:

   - la intervención en los motores de cambio («matching ingines») causando errores o la inhabilitación del sistema;
   - la interrupción o confusión de la información sobre el precio de cambio;
   - la manipulación de los protocolos Financial Information Exchange (FIX);
   - interrupción en las sesiones de los miembros de un sistema de trading;
   - la toma de control del sistema de *trade* por medio de *hacking*.

c. *Risk management:* en este momento del proceso de trading los principales riesgos son la modificación de los límites del pre-trading y el sistema de gestión de riesgos que pueden producir errores de cálculo del margen.

d. *Clearing and settlement:* se produce entre las operaciones de compensación y liquidación, en tal momento podrían producirse los siguientes episodios:

   - Las transferencias fraudulentas de fondos;
   - la mala utilización de los anticipos de pago;

- la carga de malware al sistema desde los miembros de liquidación;
- la manipulación de los post-trade systems para suprimir, modificar o corromper los registros de transacciones.

e. *Trade dissemination:* el apagado o corrupción de los sistemas que ocasione una difusión de datos comerciales puede producir la retirada de la liquidez del mercado o la interrupción de las negociaciones.

f. *Surveillance:* en este caso el principal riesgo es que el sistema de vigilancia y supervisión quede deshabilitado.

g. *Other services:* además los sistemas de *trade* suelen ofrecer otros servicios (web o mail) sobre los que también existen ciberamenazas.

6. Ejemplos del efecto según la **motivación:** en su mayor parte los eventos cibernéticos a los que nos hemos referido en los puntos anteriores pueden ser producidos por medio de actos intencionados, o desencadenarse como consecuencia de actos involuntarios, y ser la consecuencia indirecta de otros eventos o provenir del mal funcionamiento de los sistemas.

   Entre las amenazas de carácter intencionado podemos poner como ejemplo los ciberataques con mayor potencial de riesgo para el sector financiero, ya que este ámbito por sus características, importancia y vulnerabilidad es un reflejo de la gravedad de estos eventos, y entre ellos debemos destacar[95]:

   - *Hacktivists:* entre los diversos ataques que han sufrido las entidades financieras como consecuencia de estas actividades, podemos destacar que en 2011 la entidad reguladora de la Bolsa de Hong Kong se vio obligada a detener la cotización de varias empresas después de que un ataque al sitio web oficial de noticias de aquella bolsa interrumpiera el acceso de los inversores a la información corporativa que en él se publica.

     En 2012 se produjo una serie de continuos ataques DDoS dirigidos contra diversas entidades de EE. UU. entre las que destacan NYSE, NASDAQ y BATS[96]. Durante los años 2012 y 2014 se produjeron diversos ataques

95 *Cyber Security in Securities Markets*, IOSCO (abril de 2016), pp. 22 y 23, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf

96 «DDoS attacks against Global Markets» (febrero de 2014), http://www.prolexic.com/kcresources/whitepaper/global-market/DDoS_attacksagainst_Global_Markets_whitepaper_US_020314.pdf

a las entidades gestoras de diversas bolsas de Oriente Medio como la Bolsa de Tel Aviv y de Arabia Saudí[97]. En 2014 la Bolsa de Varsovia fue hackeada y se publicaron los datos de acceso de diversos corredores.

- *Cibercrimen:* en 2011 una brecha de seguridad en el mercado de carbón de la Unión Europea permitió robar 50 millones de euros en derechos de emisión, por lo que se tuvo que suspender la cotización durante una semana. En 2013 el ataque DDoS sufrido por la sociedad de intercambio de Bitcoins Mt. Gox produjo la pérdida de 350 millones de USD.

- Otros ataques, entre los que podemos poner como ejemplo el acontecido en 2011 cuando un ciberataque permitió la filtración de documentos confidenciales del grupo NASDAQ OMX, y el ataque sufrido en 2013 por el sistema de compensación (ClearPort) de Chicago Mercantile Exchange (CME) que provocó un daño de 16 millones de USD[98].

97 «Hacker targets Tel Aviv bourse and El Al», 16 de enero de 2012; «Hackers attack Arab stock markets», *Financial Times* (17 de enero de 2012).

98 Chicago Mercantile Exchange, CME Group Confirms Cyber Intrusion (15 de noviembre de 2013), http://investor.cmegroup.com/investor-relations/releasedetail.cfm?ReleaseID=807750

3. LOS EFECTOS DE LOS CIBERRIESGOS EN EL DESARROLLO SOCIOECONÓMICO MUNDIAL

3.1. Riesgo global[99]

El Foro Económico Internacional o World Economic Forum (en adelante, WEForum) define como riesgos globales aquellos acontecimientos que ocasionan efectos negativos significativos en muchos países e industrias durante un periodo mínimo de diez años. A su vez, se caracterizan por ser riesgos que tienen una naturaleza sistémica, es decir, tienen el potencial de afectar a un sistema entero y no, tan solo, a partes o componentes individuales del mismo. Y como define el Cambridge Dictionary, es la posibilidad de que suceda algo malo que afecte a todos los países de forma general[100]. En el informe que el WEForum publica de forma anual sobre riesgos globales se realiza una selección de 31 riesgos globales agrupados en cinco categorías: medioambientales, económicos, geopolíticos, sociales y tecnológicos.

Los ciberriesgos forman una parte fundamental de los riesgos tecnológicos y en la medida en la que se han desarrollado las IT se pueden considerar como el principal factor de los mismos. Así, el WEForum ha calificado los ciberriesgos como **uno de los principales peligros para el desarrollo económico mundial.** Y, en concreto, su informe de 3 de noviembre de 2007 bajo el título «Digital Ecosystem Convergence between IT, Telecoms, Media and Entertainment: Scenarios to 2015» es uno de los primeros estudios con carácter internacional en los que se alerta sobre la relevancia de estos riesgos.

El World Economic Forum es una de las instituciones con mayor reconocimiento internacional. Se trata de una fundación domiciliada en Cologny (Suiza) y reconocida por el gobierno suizo como una institución internacional cuyo objeto es «el compromiso por mejorar el Estado del mundo mediante la participación empresarial, política, académica, y otros líderes de la sociedad para determinar objetivos globales, regionales e industriales»[101].

---

99 R. S. Kaplan y A. Mikes, «Managing Risks: A New Framework», *Harvard Business Review* (2012).

100 Global Risk, *Cambridge Dictionary,* http://dictionary.cambridge.org/es/diccionario/ingles/global-risk

101 Abkommen zwischen dem Schweizerischen Bundesrat und der Stiftung World Economic Forum zur Festlegung des Status der Stiftung World Economic Forum in der Schweiz, Privilegien und Immunitäten. Abk mit der Stiftung, World Economic Forum (2015), http://www.news.admin.ch/NSBSubscriber/message/attachments/38059.pdf

En este sentido, su principal acción es la celebración de un foro anual en la ciudad de Davos en el que se reúnen los principales líderes mundiales para analizar y buscar soluciones a los principales riesgos del desarrollo mundial, fruto del cual todos los años se publica el informe denominado Global Risks Report (desde su primera edición en 2006), y en él se resume el previo Global Risk Network.

Las diferentes publicaciones del WEForum son una de las mejores perspectivas para estudiar los riesgos que afectan al desarrollo económico mundial, ya que esta institución ha ido elaborando durante años un sólido estudio sobre aquellos riesgos cuyos efectos se ponen de manifiesto en distintas partes del mundo. Y como resultado de tales estudios publica de forma anual diversos informes sobre el desarrollo y alcance de los riesgos globales.

Desde sus comienzos, estas publicaciones han sido patrocinadas por las principales compañías de la industria aseguradora, ya que el WEForum cuenta en este ámbito con numerosos socios con los que comparte conocimiento e información; y entre ellos, destacan compañías como Aon, Marsh, Allianz, Generali, Swiss Re Group, Willis Towers Watson, XL Group y Zurich Insurance Group.

Tales circunstancias hacen que las investigaciones publicadas por el WEForum sean idóneas para analizar el estado de la ciencia relativo a los efectos que producen los cyber risks en el desarrollo económico mundial.

El primer Global Risks Report fue publicado en 2006 gracias a la colaboración y el trabajo conjunto de World Economic Forum, MMC (Marsh & McLennan Companies, Inc.), Merrill Lynch y Swiss Re, junto con el Risk Management and Decision Processes Center del Wharton School de la University of Pennsylvania. Y sus principales objetivos fueron tratar de identificar los riesgos globales tanto actuales como emergentes, estudiar las relaciones entre ellos y mejorar la eficacia de los medios de mitigación.

En aquel momento ya se consideró que el número de riesgos potenciales era incierto, principalmente los asociados con las nuevas tecnologías que aún no suponían una amenaza global destacable, pero tenían un alto potencial de ser un riesgo muy destructivo en el futuro[102].

No obstante, en aquella edición del Global Risks Report no se consideró el alcance y objeto de los ciberriesgos en sí mismos, y dentro de la categoría de riesgos tecnológicos, se hacía referencia a supuestos como: *Convergence of technologies*, *Nanotechnology*, *Electromagnetic fields* y *Pervasive*

102 Global Risk Report, World Economic Forum (2006), p. 1.

computing[103]. Aunque se trataban de elementos completamente diferentes a los propios ciberriesgos, tal consideración ponía de manifiesto la influencia y dependencia global de las nuevas tecnologías. De esta forma, el estudio consideraba que ciertos eventos o situaciones que afectaban a las nuevas tecnologías podían suponer un riesgo para el ser humano y su entorno.

Entre los reseñados riesgos estimó que los riesgos provenientes del efecto de los campos electromagnéticos (radiación solar y tormentas solares) podrían llegar a producir unos efectos muy graves en el ser humano a largo plazo. Y sobre las tecnologías de localización o *pervasive computing* y las *Convergence of technologies*, el informe destacaba:

- el grave efecto que podía llegar a tener sobre la cohesión social la pérdida de privacidad individual;
- el posible aumento de la vulnerabilidad ante los riesgos emergentes;
- y la creación de herramientas que permitan monitorizar las acciones de un grupo de sujetos[104] (mecanismos que han sido denomindos en diversas publicaciones como «big brother»[105]).

El riesgo de que se produjeran ataques a las infraestructuras críticas se consideraba como parte de los riesgos globales económicos[106], advirtiendo de los efectos económicos que suponían las nuevas amenazas terroristas sobre las infraestructuras críticas[107]. Y, además, se hacía referencia a la importancia del componente geográfico en este tipo de riesgos, ya que el estado de los avances tecnológicos, la capacidad financiera y la priorización de las políticas locales determinan la rapidez y eficacia con la que se pueden reparar las infraestructuras críticas después de haber sufrido cualquier daño[108].

La amenaza sobre las infraestructuras críticas se definió como un riesgo con una probabilidad alta de ocurrencia cuyos efectos a corto y largo plazo podrían causar graves perjuicios, como se ponía de manifiesto en la siguiente tabla.

103 *Op. cit.*, World Economic Forum (2006), p. 14.

104 *Op. cit.*, World Economic Forum (2006), p. 17.

105 *Big brother:* a government or person in authority that tries to control people's behavior and thoughts, *Cambridge Dictionary*, http://dictionary.cambridge.org/us/dictionary/english/big-brother

106 *Op. cit.*, World Economic Forum (2006), p. 14.

107 *Op. cit.*, World Economic Forum (2006), p. 2.

108 *Op. cit.*, World Economic Forum (2006), p. 6.

Tabla 3. Riesgos económicos: infraestructuras críticas (CII)

Riesgos económicos: infraestructuras críticas (CII)		Probabilidad	Gravedad
Corto plazo	Corte del suministro eléctrico en Europa	3	2
Corto plazo (peor situación)	Bloqueo de la transmisión transatlántica de datos	1	3
Largo plazo	Ataque a las infraestructuras IT	3	1
Largo plazo (peor situación)	Ataque coordinado a las infraestructuras por medio de pulsos electromagnéticos	1	3

Elaboración propia desde la fuente Global Risks Report 2006[109].

El Global Risk Network Report publicado en 2007 introdujo los daños a las infraestructuras críticas dentro de la categoría de riesgos tecnológicos. De tal manera, centraba el estudio de esta categoría de riesgos globales en aquellas amenazas[110]. En él, se consideró que existía un equilibrio entre: el aumento de la vulnerabilidad que procede de la conectividad y la creciente conciencia de los problemas de seguridad de las infraestructuras críticas, y las inversiones en flexibilidad y capacidad disponible en algunas infraestructuras esenciales[111].

Dentro de los diversos elementos para la mitigación del riesgo el Global Risks Report 2007 atiende a cinco pasos o circunstancias fundamentales: *Improving insight*, *Enhancing information flow*, *Refocusing incentives*, *Improving investment* e *Implementing through institutions*. Entre ellas, atribuye a las amenazas contra las infraestructuras críticas (conforme al estado y conocimientos que existían en el 2007) el carácter de *Improving insight* y *Enhancing information flow*[112]. Estas dos citadas situaciones comprenden un aumento del conocimiento y del flujo de información que se tenía sobre este tipo de riesgos en relación con los años previos[113].

En general, el Global Risks Report 2008 mantuvo los riesgos ya señalados en el 2007 ahondando en la información y conocimiento de cada uno de ellos. En este nuevo informe se volvió a considerar la importancia del equilibrio entre la exposición del ser humano a la nanotecnología y las oportunidades de estos sistemas. Principalmente advirtió sobre el hecho

109 Critical Information Infrastructure (CII), *op. cit.*, World Economic Forum (2006), p. 15.

110 Global Risk, World Economic Forum (2007), p. 6.

111 *Op. cit.*, World Economic Forum (2007), p. 12.

112 *Op. cit.*, World Economic Forum (2007), p. 23.

113 *Op. cit.*, World Economic Forum (2007), p. 24 (tabla).

de que la constante interpelación de los ciberriesgos en las infraestructuras críticas hacía más predecibles los ataques específicos, y que, a su vez, tal aumento de las amenazas se debía a la carencia de medios dedicados a la ciberseguridad.

En otro sentido, y profundizando en el conocimiento sobre este tipo de riesgos, se concluía que el carácter global de las ciberamenazas a infraestructuras críticas se debe al posible efecto dominó que presumiblemente provocan estos daños. Este efecto en cadena podría interrumpir el funcionamiento de todos los sistemas dependientes de la infraestructura dañada (el sistema de distribución de agua y energía, el sistema bancario y financiero, o el sistema de gestión de emergencias)[114].

Para tal año (2008) se estimó que los daños en las infraestructuras críticas podrían causar pérdidas globales por valor de entre 250 billones y 1 trillón de USD, con una probabilidad de concurrencia cercana al 10 % (datos similares a los atribuidos a la inestabilidad de la economía china y de las relaciones políticas de Oriente Próximo, o el efecto del cambio climático en el tiempo atmosférico)[115].

Y, por otra parte, en relación con los daños humanos que podrían llegar a causar (expresado en el informe de referencia conforme al posible número de muertes) se estimó que este tipo de daños podría llegar a ocasionar en 2008 entre 1.600 y 8.000 muertes en todo el mundo, con una probabilidad del 10 % (tal estimación era, por tanto, similar al colapso de una crisis nuclear, o al crimen y corrupción internacional)[116]. Tales datos implicaban un aumento de la probabilidad de ocurrencia con respecto a las estimaciones de 2007 tanto en lo relativo a los daños económicos[117] como a la pérdida de vidas[118].

114 Global Risks Report, World Economic Forum (2008), p. 22.

115 *Op. cit.*, World Economic Forum (2008), p. 23 (tabla), Some risks were disaggregated for the purpose of assessment in Appendix 2 to the current report. For ease of visual representation they have been shown aggregated on the current graphics.

116 *Op. cit.*, World Economic Forum (2008), p. 24 (tabla), Note: Some risks were disaggregated for the purpose of assessment in Appendix 2 to the current report. For ease of visual representation they have been shown aggregated on the current graphics.

117 *Op. cit.*, World Economic Forum (2008), p. 48.

118 *Op. cit.*, World Economic Forum (2008), p. 51.

Tabla 4. Daños ocasionados por fallos de las infraestructuras críticas

2008			2007		
	Probabilidad*	Gravedad**		Probabilidad*	Gravedad**
Ataque o fallo en los sistemas CII crea un efecto dominó paralizando las aplicaciones dependientes de los sistemas IT (energía, agua, transporte, sistema bancario y financiero, y sistemas de emergencias)	3,5	1	Interrupción o fallo de las CII	3	1
Los estudios revelan un deterioro de la salud debido a la exposición a los sistemas en los que se utiliza nanotecnología (pintura, cosméticos y productos sanitarios)	2	1	Riesgos emergentes asociados a la nanotecnología	2	1

Elaboración propia desde la fuente World Economic Forum 2008[119].
* Probabilidad: 1, debajo del 1 %; 2, 1-5 %; 3, 5-10 %; 4, 10-20 %.
** Gravedad: 1, 600-8.000; 2, 8.000-40.000; 3, 40.000-200.000; 4, 200.000-1 millón.

En relación con el ya mencionado efecto en cadena debemos considerar que el Global Risks Report 2009 llamó la atención sobre los efectos económicos de la interconectividad de sistemas globalizados, y a tal circunstancia se le atribuyó el carácter global de los riesgos que se analizaban en el estudio[120]. En este sentido, el informe ofrecía la perspectiva de la interconexión desde cada uno de los cinco riesgos globales analizados, con lo que se lograba concluir

119 Risk assessments Lives lost, Technology, *Op. cit.*, World Economic Forum (2008), p. 51.

120 Global Risks Report, World Economic Forum (2009), p. 5.

que existe una gran equivalencia entre los riesgos relativos a la salud, economía, geopolítica y tecnología que afectaban a los países europeos entre sí[121].

El informe publicado en el año 2009 introdujo como nuevos riesgos, dentro del ámbito de las amenazas tecnológicas (en las que tradicionalmente se incluían los riesgos de colapso de las infraestructuras críticas y efecto de la nanotecnología), la pérdida y robo de datos. Y en cuanto a la vulnerabilidad de las infraestructuras críticas, consideró que mantenía en los mismos niveles que el año anterior; pues, aunque había aumentado la amenaza como consecuencia de la dependencia e interconectividad de los sistemas, los sistemas de seguridad para la prevención y gestión de los daños habían sido mejorados[122].

El aumento de la interconectividad pone de manifiesto el crecimiento de los riesgos sistemáticos de carácter global entre los que se encuentran las cybervulnerabilidades, cuya naturaleza y efectos cumplen con las características de este tipo de amenazas, y por tanto requieren de una eficiente gestión global[123]. Así, en el Global Risks Report 2010 se advertía del efecto perjudicial de la falta de inversión en infraestructura. Según estimaba el informe, tal circunstancia podía ser la causa de que se ocasionasen daños a las infraestructuras críticas con pérdidas de entre 250 billones y 1 trillón de USD, y entre 10 y 50 billones de USD por pérdida de datos; ambas con una probabilidad de ocurrencia entre el 10 y el 20 %[124].

La importancia de la inversión en infraestructuras tecnológicas se pone especialmente de manifiesto en las entidades y organizaciones públicas y privadas. En estas últimas, puede ser especialmente relevante, ya que a pesar de guiarse por intereses puramente privados, sus sistemas tecnológicos operan en un mundo interconectado, por lo que el daño debido a la falta de medidas de seguridad privadas puede ocasionar efectos en otros sistemas e incluso de carácter global.

Por ello, el informe de referencia consideraba necesario que se tomasen medidas regulatorias y de inspección, y que se mejorase la capacidad de reacción y la coordinación global ante este tipo de amenazas (como ya se hacía con otras amenazas de carácter global)[125].

En otro sentido, se considera que el crimen y la corrupción internacional podían ocasionar un aumento de la exposición global a las amenazas contra

121 *Op. cit.*, World Economic Forum (2009), p. 8.

122 *Op. cit.*, World Economic Forum (2009), p. 31.

123 Global Risks Report, World Economic Forum (2010), p. 5.

124 *Op. cit.*, Global Risks Report (2010), p. 18 (gráfico).

125 *Op. cit.*, Global Risks Report (2010), p. 23.

las infraestructuras críticas, y que la pérdida y el robo de datos tendrían unos efectos similares a la falta de inversión en infraestructura (a la que antes nos hemos referido)[126] y a los riesgos producidos por la interconectividad[127].

Atendiendo a las cibervulnerabilidades, en general, y a las infraestructuras de información crítica, en particular, en 2010 se consideró que la relación entre los sistemas tecnológicos abiertos y cerrados había generado ciertas vulnerabilidades de carácter desconocido. De esta forma, los resultados de la Global Risks Perception Survey 2010 muestran que la mayoría de expertos allí reunidos percibían que existía un riesgo bajo de daño y probabilidad tanto del colapso de las infraestructuras críticas, como del robo y pérdida de información. Y, además, fueron valorados como los riesgos globales con menores efectos relacionados con la interconectividad. No obstante, y como consideraba el Global Risks Report 2010, las cibervulnerabilidades deben entenderse como uno de los riesgos globales con mayor crecimiento cuyo desarrollo está ligado a la evolución de la tecnología y la interconectividad. Y es que el informe mantenía que el reconocimiento de la entidad de estos riesgos es el primer paso para reducir el aumento del cibercrimen, el robo y pérdida de datos, y los fallos de las infraestructuras tecnológicas.

Finalmente, se ponían de manifiesto cinco elementos relacionados con los ciberriesgos —siendo este el primer momento en el que se desarrollaron tales características en el informe anual de riesgos globales del World Economic Forum—, que son[128]:

1. **Visión:** en la medida en la que las TI se desarrollan e implementan en diversos ámbitos del sistema socioeconómico aumenta la potencial amenaza de los riesgos sistémicos.

2. **Información:** la falta de información lleva a que los desarrolladores de propiedad intelectual, distribuidores de plataformas de software y aplicaciones y demás operadores tecnológicos se atribuyan mutuamente la responsabilidad de los ciberriesgos, lo que en definitiva constituye una situación de desprotección a los consumidores y usuarios finales.

3. **Incentivos:** el referenciado informe considera que es necesaria la aplicación de un sistema de normas e incentivos que aseguren que los sistemas de seguridad tecnológica se implementen.

126 *Op. cit.*, Global Risks Report (2010), p. 28.

127 *Op. cit.*, Global Risks Report (2010), p. 30.

128 *Op. cit.*, Global Risks Report (2010), pp. 31 y 32.

4. **Inversión:** para la creación de un ordenamiento jurídico rápido, efectivo e internacional es necesaria la colaboración conjunta de medios públicos y privados.

5. **Instituciones:** el informe consideraba que es importante que en un futuro se crease un organismo que permitiera: publicar la información sobre los ciberdaños, establecer unos estándares generales de notificación de las vulnerabilidades y definir los conceptos básicos de este ámbito.

En conclusión, el Global Risks Report 2010 relacionaba las vulnerabilidades que afectan a las infraestructuras tecnológicas con una serie de efectos potenciales derivados de tales amenazas, entre los que se encuentran:

- El colapso de precios de mercado (con una probabilidad superior al 20 %, y capaz de ocasionar daños globales mayores a 1 trillón de USD).

- La volatibilidad del precio de los alimentos y el petróleo (con una probabilidad de entre el 10 y el 20 %, y capaz de ocasionar daños globales cercanos a 1 trillón de USD).

- El crimen y la corrupción internacional.

- El terrorismo internacional.

- La pérdida y el robo de datos (con una probabilidad de entre el 10 y el 20 %, y capaz de ocasionar daños globales entre 50 y 250 billones de USD)[129].

Del análisis de los datos sobre la evolución de los riesgos tecnológicos que ha ido aportando el Global Risks Report desde el informe publicado en 2006, podía extraerse, conforme al informe de 2010, dos circunstancias[130]:

- Que respecto a la posibilidad de que un daño a las infraestructuras críticas produjese, a su vez, un efecto dominó que afectase a sistemas básicos, se había producido un aumento de la probabilidad y del daño potencial.

- Y que de la misma manera había aumentado la probabilidad e intensidad del daño potencial de la pérdida y robo de datos, lo que había producido el aumento de la desconfianza en las IT y en las organizaciones que han sufrido estos daños. Tal aumento parecía estar motivado por la mayor penetración de internet en las actividades de los usuarios, lo que había facilitado la existencia de un mayor contenido de datos publicados.

129 *Op. cit.*, Global Risks Report (2010), p. 32.

130 *Op. cit.*, Global Risks Report (2010), apendix. 2.

La sexta edición de la publicación Global Risks (en 2011) fue la primera de esta serie de estudios en la que se incorporó el concepto de ciberseguridad. En esta edición se distinguía, dentro del ámbito de riesgos tecnológicos, tres categorías:

1. La posibilidad de colapso de las infraestructuras críticas (a la que se atribuía una probabilidad de ocurrencia media y una estimación de daños de entre 250 y 500 billones de USD).

2. La seguridad de los datos y la información confidencial (a la que se atribuía una probabilidad de ocurrencia media y una estimación de daños de entre 100 y 250 billones de USD).

3. Las amenazas que provienen de las nuevas tecnologías (a las que se atribuía una probabilidad de ocurrencia media y una estimación de daños de entre 100 y 250 billones de USD)[131].

En relación con la ciberseguridad en general se advirtió de algunos riesgos que debían ser observados y tenidos en cuenta *(risk to watch)* a los que se señalaba como riesgos potenciales que por sus circunstancias tenían un nivel muy alto de probabilidad de ocurrencia o de ocasionar daños cuantiosos. Así, la conciencia de que el mundo real es vulnerable ante las amenazas del ciberespacio ha aumentado entre los consumidores y usuarios. Y de tales preocupaciones surge el interés por la ciberseguridad que engloba: la seguridad de los datos y la información, las infraestructuras críticas y las amenazas que provienen de las nuevas tecnologías entre las que, a su vez, destaca los ***cyber theft, ciberespionaje, cyber war y cyber terrorism***[132].

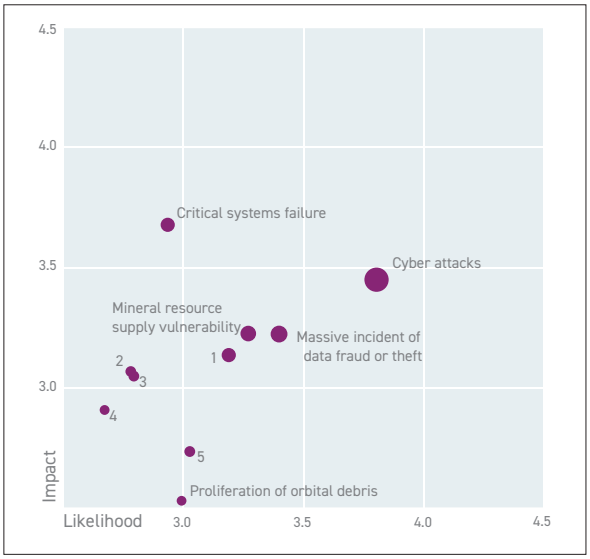
El panorama descrito ya empezaba a señalar como riesgos globales alguno de los elementos propios de los ciberriesgos o ciberamenazas, que fueron finalmente introducidos como tales conceptos en el Global Risks Report publicado en 2012. En esta publicación se incluyeron dentro del ámbito de los riesgos tecnológicos un gran número de categorías entre las que destaba: la desinformación digital, los incidentes masivos de fraude o robo de datos, el fallo de los sistemas críticos y principalmente los ciberataques[133]. A todos ellos los atribuyen las estimaciones de impacto y probabilidad de ocurrencia que se muestran en el siguiente gráfico.

131 Global Risks Report, World Economic Forum (2011), p. 5.

132 Global Risks Report, World Economic Forum (2011), p. 36.

133 Global Risks Report, World Economic Forum (2012), p. 4.

Gráfico 4. Riesgo tecnológico



Fuente: World Economic Forum (2012)[134].

Como se puede ver, los ciberataques se determinaron como los riesgos tecnológicos con mayor probabilidad de ocurrencia e impacto. Además, se consideró que representaban el cuarto riesgo con mayor grado de probabilidad de ocurrencia dentro de los 50 principales riesgos globales[135]. Y, dentro de esta clasificación se establecieron cinco categorías de riesgo que atendían a diferentes parámetros:

1. *Centres of Gravity*, que representaban los riesgos capaces de ocasionar efectos sistémicos, y que tenían una probabilidad de ocurrencia e impacto muy altos. Entre ellos destacan, en el ámbito de los riesgos tecnológicos, los fallos de sistemas críticos.

2. *Critical Connectors*, que relacionan riesgos clasificados como *Centres of Gravity*.

3. Los propios *global risks*, que suponen amenazas con efectos en diversos países y son capaces de ocasionar importantes daños en el sistema socioeconómico.

134 Technological Risk, Global Risk Report, World Economic Forum (2012), p. 4.

135 *Op. cit.*, World Economic Forum (2012), p. 11.

4. *Weak Signals*, que ponen de manifiesto diversas vulnerabilidades. Dentro de este ámbito, y en la categoría de riesgos tecnológicos, se mencionaba la proliferación de escombros espaciales y las consecuencias de la nanotecnología.

5. *X Factors*, que comprenden riesgos potenciales que ocasionan consecuencias desconocidas pero que aún no formaban parte de los riesgos globales analizados por los Risk Reports, sino que se trataban de los anteriormente calificados como «*risk to watch*». Entre ellos, tienen relación con el presente estudio dos aspectos que se enumeraban en el Global Risks Report como:

   a. La conectividad constante, que se definía como un elemento que podría hacer disminuir nuestra percepción del riesgo que comportan las IT;

   b. y, la desinformación, en relación con este concepto, se ponía en duda si los efectos de la liberalización de la información y la falta de medios que garanticen la misma perjudicarán o favorecerán a la veracidad y fiabilidad de la información.

En definitiva, el Global Risks Report publicado en 2012 planteaba que los mencionados riesgos podían ser la principal amenaza para las infraestructuras y los sistemas críticos. Y aunque los atribuía una probabilidad de ocurrencia baja, consideraba que en caso de producirse podrían llegar a ocasionar un impacto muy relevante[136].

En el 2012 el 35 % de la población mundial tenía acceso a internet, frente al 8 % en 2002[137]. Además, las formas de conexión también cambiaron, al final del año 2011 se habían vendido alrededor de 470 millones de *smartphones* en todo el mundo[138]. No obstante, el sistema que ha presentado una evolución más rápida es el «internet de las cosas»[139]. En 2012 existían 5.000 millones de dispositivos o «cosas» conectados a los que se podía acceder mediante internet (automóviles, hornos de cocina, fotocopiadoras, redes eléctricas, camas de hospital, sistemas de riego y bombas de extracción de agua, entre otros muchos). Y se espera que el número de dispositivos conectados a internet

136 *Op. cit.*, World Economic Forum (2012), p. 24.

137 World Telecommunication/ICT Indicators Database 2010, *International Telecommunication Union*, http://www.itu.int/ITU-D/ict/publications/world/world.html, 2011.

138 Nagamine, K. «Worldwide Smartphone Market Expected to Grow 55% in 2011 and Approach Shipments of One Billion in 2015». *International Data Corporation*, http://www.idc.com/getdoc.jsp?containerId=prUS22871611, 2011.

139 The Internet of Things Backgrounder, *Intel*, http://newsroom.intel.com/servlet/JiveServlet/download/2297-5 5895/The%20Internet%20of%20Things%20Backgrounder.pdf, 2011.

alcance 50.000 millones en 2020[140]. El aumento de la utilización de las IT comporta, por regla general, la obtención de numerosos beneficios y la disminución de costes, pero a medida que se conectan más sistemas a internet, se genera un canal de información y control susceptible de ser atacado[141].

El Global Risks Report 2012 trató con detenimiento el ámbito de las ciberamenazas poniendo una especial atención sobre los peligros y oportunidades del desarrollo de la conectividad. En él se introdujo por primera vez (en esta serie de estudios) el carácter de bien público para referirse a la ciberseguridad. En este sentido, se afirmaba que la seguridad online es un ejemplo de bien público, cuyos costes tienen un carácter privativo pero sus beneficios se comparten con todo el sistema. Por ejemplo, cuando una compañía contrata un software de seguridad protege sus sistemas, y al mismo tiempo impide que por medio de ellos lleguen ciberataques o spams a su red de contactos[142].

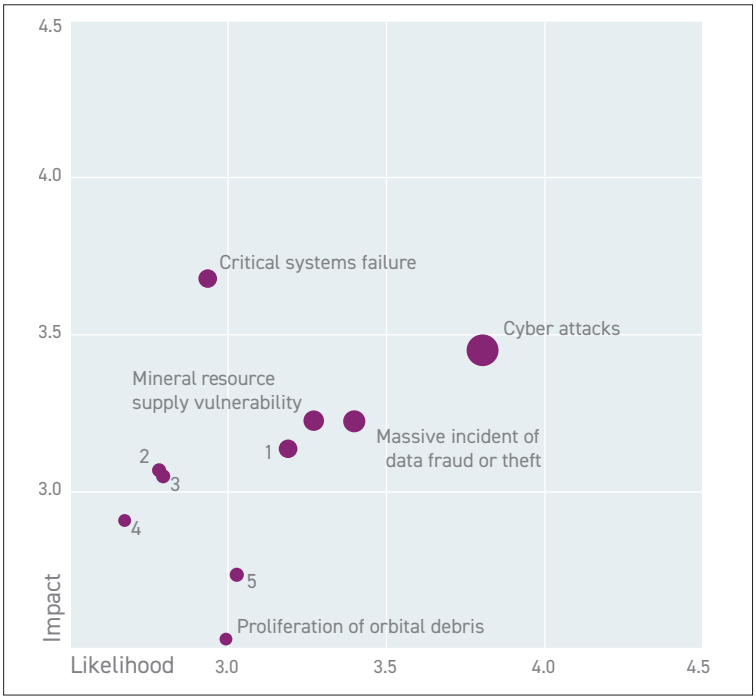
Los fallos de los sistemas críticos han sido señalados como *Centre of Gravity* por ser uno de los riesgos globales con mayor influencia. Este tipo de amenazas se pueden analizar desde las cinco categorías de riesgo global que el Global Risks Report propone, y guardan una especial relación con los ciberataques. En ambos casos, el WEForum estimó una probabilidad de ocurrencia e impacto superiores a los reconocidos para el resto de riesgos tecnológicos, según refleja el siguiente gráfico.

140 Dave Evans, «The Internet of Things», Cisco Internet Business Solutions Group (IBSG) (abril de 2011), http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

141 *Op. cit.,* World Economic Forum (2012), p. 26.

142 *Op. cit.,* World Economic Forum (2012), p. 27.

Gráfico 5. Fallos relacionados con las infraestructuras críticas



Fuente: World Economic Forum (2012)[143].

No obstante, la relación entre ambos riesgos proviene de la posibilidad de que un ciberataque produzca el colapso de alguna infraestructura crítica[144], como se muestra en el diagrama.

143 Figure 38: Technological Risk, *Op. cit.*, World Economic Forum (2012), p. 44.

144 *Op. cit.*, World Economic Forum (2012), p. 45.

Gráfico 6. Fallos en sistemas críticos

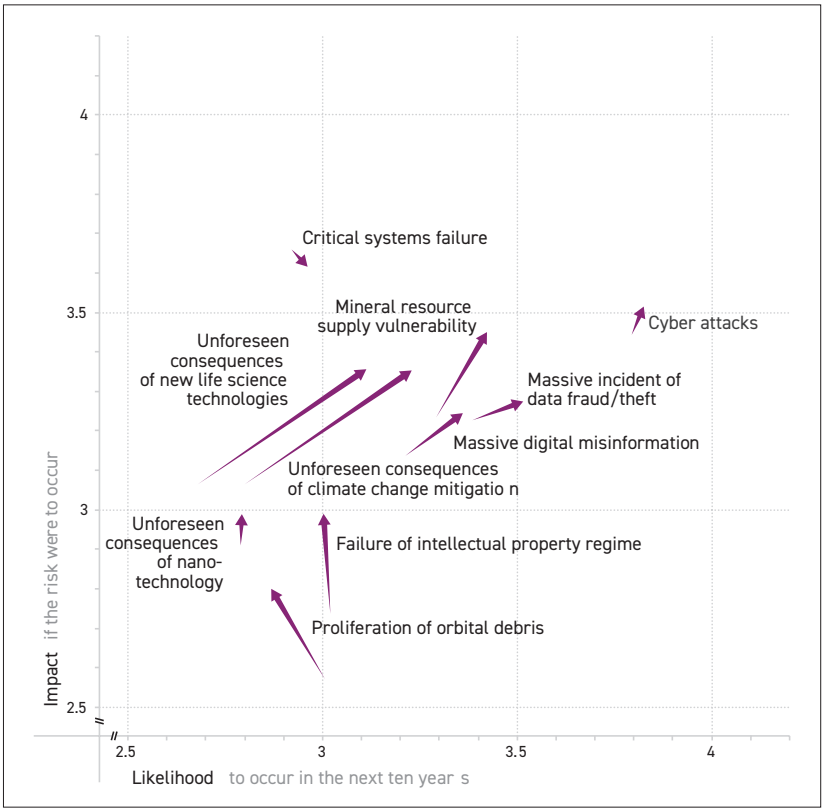
Fuente: World Economic Forum (2012)[145].

Las estimaciones publicadas en 2013 mostraban un leve descenso del impacto potencial de los fallos en las infraestructuras críticas y un aumento en el caso de los ciberataques. En tal sentido, estos últimos se volvieron a situar como uno de los riesgos con mayor probabilidad de ocurrencia dentro de los cincuenta riesgos globales analizados[146].

145 Figure 39: Critical Systems Failure is the Centre of Gravity in the Technological Category, *Op. cit.*, World Economic Forum (2012), p. 45.

146 Global Risks Report, World Economic Forum (2013), p. 4.

Gráfico 7. Comparación de la situación de los riesgos globales (2013-2012)



Fuente: Global Risks Report (2013)[147].

El Global Risks Report publicado en 2013 centró su atención en la amenaza de la desinformación, con relación a los efectos de los ciberataques y el ciberterrorismo. De esta forma, consideraba que tal circunstancia pone de manifiesto los efectos negativos de la hiperconectividad a los que haremos referencia posteriormente[148].

Los datos publicados por las diversas ediciones del Global Risks Report provienen de la opinión de grupos de expertos de cada uno de los cinco ámbitos que se estudian en estas publicaciones, que se reúnen cada año en torno a conferencias previas a cada publicación, y por los datos que proceden de

147 Figure 1: Global Risks Landscape 2013 versus 2012, Global Risks Report, World Economic Forum (2013), p. 4.

148 *Op. cit.*, Global Risks Report (2013), p. 23.

diversas encuestas realizadas periódicamente a profesionales de cada sector. Partiendo de tal información, el informe de 2013 concluyó que frente a los ciberriesgos destacaba:

- La preocupación puesta de manifiesto por los expertos procedentes de EE. UU. y China[149];
- y por aquellos que formaban parte del ámbito tecnológico que consideran que estos supuestos tienen una probabilidad de ocurrencia mayor (un 3,11 sobre 5) a la mantenida por expertos en otras materias (un 2,93 sobre 5)[150].

El Global Risks Report de 2014 estableció como objetivo principal estudiar los riesgos sistémicos cuyos efectos se ponen de manifiesto a largo plazo, entre los que destaca los referentes al ámbito del ciberespacio[151]. De tal forma, es importante tener en cuenta que aquella fue la primera vez en la que estos estudios se refirieron a los ciberriesgos como un problema que gira en torno al ciberespacio, con lo que extrajeron este concepto de su enmarcación tradicional dentro de los riesgos tecnológicos.

La edición publicada en 2014 diferenció, dentro del ámbito de los riesgos tecnológicos, tres categorías: el colapso de infraestructuras críticas, los ciberataques y el robo o pérdida de datos[152]. Además, introdujo el concepto de «*digital desintegration*», que se consideró como el principal riesgo para el ciberespacio, ya que plantea la posibilidad de aumentar el daño que ocasionan los ciberataques. Todo ello crea una situación en la que disminuye la confianza de los consumidores y usuarios en el ciberespacio, por lo que se concluyó que causaría un coste social y económico[153].

Dentro de los cincuenta riesgos globales analizados en 2014, se consideró que los ciberataques eran la quinta amenaza con mayor grado de probabilidad de ocurrencia, a la que se le atribuía un posible impacto de carácter muy alto[154].

La «*digital desintegration*» es un aumento gradual de la vulnerabilidad producido por el desarrollo de la hiperconectividad y la dependencia del ciberespacio (que es consecuencia de elementos como el Internet of Things). En atención a esta realidad, el Global Risks Report 2014 planteó bajo el título

149 *Op. cit.*, Global Risks Report (2013), p. 63.

150 *Op. cit.*, Global Risks Report (2013), p. 73.

151 Global Risks Report, World Economic Report (2014), p. 9.

152 *Op. cit.*, World Economic Forum (2014), pp. 12 y 13.

153 *Op. cit.*, World Economic Forum (2014), p. 11.

154 *Op. cit.*, World Economic Forum (2014), pp. 16-17.

Towards Measurement of Cyber risks que la dependencia de los factores socioeconómicos al desarrollo de sistemas interconectados requiere que se «normalicen» los ciberriesgos. Para ello, señaló diferentes niveles de seguridad que podrían permitir elaborar un sistema de gestión que atendiera a cada uno de ellos; de esta forma:

- el primer nivel estaría formado por las amenazas contra sistemas y organizaciones concretos que se podrían gestionar mediante la implantación y mantenimiento de sistemas de seguridad informática;

- y el segundo nivel se centraría en grandes riesgos, en tal caso consideró que se trataban de valores intangibles de seguridad que podría ser garantizada por medio de las compañías aseguradoras.

En otro sentido, el estudio anuncia que el WEForum ha empezado a investigar el impacto de los ciberriesgos a nivel macroeconómico, en relación con la competitividad y el desarrollo del GDP.

La capacidad de los diferentes países de mejorar su competitividad por medio de la tecnología ha sido documentada por el Forum Global Information Technology Report durante años, y a estos datos se sumaron los ofrecidos por otros estudios centrados en el efecto de la tecnología en el GDP. Como conclusión, se ha hecho hincapié en la relación que hay entre la capacidad de defensa contra los ciberataques y la amenaza que estos pueden suponer para el desarrollo económico por medio de las nuevas tecnologías.

En concreto, la preocupación por la seguridad de las transacciones puede producir un impacto negativo directo en las relaciones de comercio disminuyendo las estimaciones de ventas. Y en todo caso, se advertía de los efectos negativos de la fragmentación de las políticas de seguridad entre las diferentes áreas geográficas o «Balkamización de internet» («Balkanization of the Internet»), que producen una realidad muy heterogénea que a la postre perjudicará a la economía global[155].

El Global Risks Report 2015 advirtió que en algunos países no se mantenía adecuadamente las infraestructuras críticas, lo que dificultaba la prevención de los ciberataques, e impedía evitar que un siniestro llegase a causar un daño en cadena en todo el sistema[156]. La falta de políticas de ciberseguridad tiene unos efectos de carácter global, ya que no solo aumenta las amenazas a nivel nacional, sino que puede afectar a todo el ciberespacio. Esta circunstancia unida al inevitable aumento de los ciberriesgos durante la próxima

155 *Op. cit.*, World Economic Forum (2014), p. 41.

156 Global Risks Report, World Economic Forum (2015), p. 23.

década hace que las vulnerabilidades crezcan de forma irregular, de tal manera que podrán ocasionar sus principales efectos en las áreas geopolíticas más frágiles[157].

Por ello, en el ámbito del gobierno y la cooperación de internet se plantean dos elementos esenciales:

- El aspecto técnico relativo a la necesidad de mejorar la protección y seguridad de las infraestructuras críticas;

- y la protección de las circunstancias generales del ciberespacio, de la neutralidad de la red, la libertad y la privacidad, y la lucha contra el cibercrimen.

La mejora de las circunstancias técnicas es responsabilidad de diversas entidades como The Internet Engineering Task Force (IETF), The World Wide Web Consortium (W3C), the Regional Internet Registries (RIR), los «root servers operators» y The Internet Corporation for Assigned Names and Numbers (ICANN); además del resto de proveedores de servicios tecnológicos en general (conforme al ámbito en el que operen).

En cuanto a la protección de las circunstancias generales, el Cyber Risk Report considera que los gobiernos y entidades públicas se están viendo presionados para asumir esta responsabilidad dentro de las medidas de carácter nacional. Y por ello están empezando a tomar acuerdos con respecto a los datos y en materia de privacidad.

No obstante, mientras que la aplicación de la regulación que afecta a las infraestructuras es sencilla debido a su localización geográfica y su existencia material, las disposiciones relativas a los datos son de difícil aplicación y, en ciertos casos, producen el denominado «*data nationalism*»[158], que podría perjudicar a la transferencia de información y flexibilidad del ciberespacio.

En la publicación de 2015 se añadió, dentro del ámbito de los riesgos tecnológicos globales, la amenaza de la extensión del mal uso de las tecnologías, especialmente las relativas a impresión 3D, inteligencia artificial, geoingeniería y biología sintética. Pero se le atribuía un nivel de impacto y probabilidad de ocurrencia bajos. Además, se estimó un aumento de la probabilidad de ocurrencia e impacto de los principales riesgos tecnológicos (ciberataques y colapso de las infraestructuras críticas) que era consecuencia de la mayor sofisticación de los ciberataques y el desarrollo de la hiperconectividad.

157 *Op. cit.*, World Economic Forum (2015), p. 13.

158 *Op. cit.*, World Economic Forum (2015), p. 22.

En la medida en la que los **elementos del Internet of Things** (igual que los sistemas de las «*Smart cities*»[159]) **envían información, se comparten diversos datos personales que pueden ser susceptibles de sufrir un robo.** Esta circunstancia hace que **cada día existan más elementos que proteger,** y no solo en el plano de la seguridad de datos e información, sino del propio funcionamiento de los sistemas. Así, los smartphones, los coches o cualquier otro dispositivo conectado al ciberespacio pueden ser objeto del robo de la información de su GPS, con un claro detrimento de la privacidad. Además, los sistemas de control de estos elementos también pueden ser hackeados. Y, en ciertos casos, los efectos de la ciberamenaza se desplegarían contra la vida e integridad física de sus usuarios[160].

Tampoco puede olvidarse que el desarrollo de las IT ha venido influyendo en todas las realidades y circunstancias socioeconómicas en la medida en que los diferentes sistemas se han ido informatizando. El internet de las cosas podría ser un ejemplo de esta influencia global que ofrece cada día más oportunidades y, al mismo tiempo, implica que los riesgos de seguridad se intensifiquen y aumenten en la medida en que existen nuevas formas de ocasionar daños y más dispositivos que asegurar[161].

En conclusión, es esencial que **el desarrollo de las IT y su implantación en todos los aspectos de la sociedad se haga garantizando la seguridad del sistema y de los individuos que lo forman.**

Por ello, el World Economic Forum ha considerado como uno de sus principales objetivos asegurar el hecho de que internet siga siendo el motor del desarrollo mundial. Para lo que advierten en sus informes que será necesario concienciar a las organizaciones y usuarios de los ciberriesgos, y aplicar con mayor exigencia las medidas de prevención que se implantan[162].

En el Global Risks Report 2016 se ha determinado un nivel muy alto de probabilidad de ocurrencia e impacto de los ciberataques que, a su vez, se consideraron la principal amenaza global para Estados Unidos[163].

El mencionado informe concluye que los avances tecnológicos ofrecen un amplio panorama de oportunidades para el desarrollo socioeconómico al aportar soluciones a distintos problemas globales (acceso a la educación, creación de oportunidades de negocio y empleo, facilitar el intercambio comercial…),

159 *Op. cit.*, World Economic Forum (2015), p. 33.

160 *Op. cit.*, World Economic Forum (2015), p. 22.

161 *Op. cit.*, World Economic Forum (2015), p. 25.

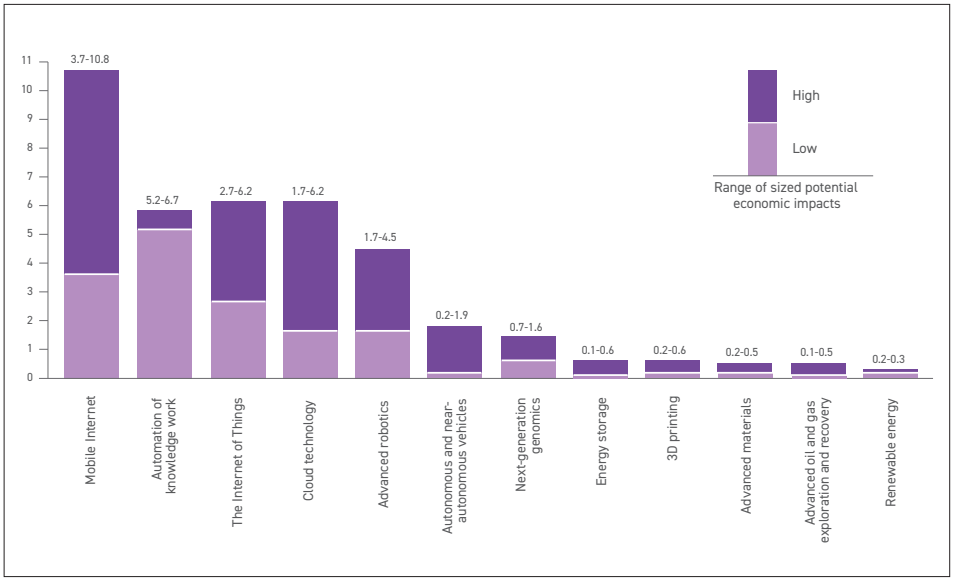
162 The Global Information Technology Report, ICTs for Inclusive Growth (2015).

163 Global Risks Report, World Economic Forum (2016).

pero al mismo tiempo aumenta la ciberdependencia, lo que provoca una mayor exposición a las ciberamenazas. Por ello, podemos considerar que la gestión de este paradigma es un aspecto crítico para la estabilidad del sistema (Klaus Schwab[164]).

Se estima que los países del entorno europeo que no sean capaces de desarrollar un sistema tecnológico apropiado pueden sufrir pérdidas de hasta 600 billones de EUR durante los próximos diez años. La estimación del potencial impacto económico de los riesgos tecnológicos ofrece los siguientes datos.

Gráfico 8. Estimación del potencial impacto económico de las tecnologías



Fuente: Global Risks Report (2016)[165].

Los ciberataques y los incidentes relacionados con los mismos han sido durante los dos últimos años los riesgos globales con mayor probabilidad de ocurrencia y potencial de impacto en EE. UU. y Canadá. Por lo que partiendo de esta situación, el Global Risks Report 2016 ha propuesto tres elementos a tener en cuenta sobre las perspectivas futuras de los ciberataques[166]:

164 *Op. cit.*, World Economic Forum (2016), p. 5.

165 Figure 1.4: Estimated Potential Economic Impact of Technologies, US$ trillion, anual, Global Risks Report, World Economic Forum (2016), p. 18.

166 *Op. cit.*, World Economic Forum (2016), pp. 18-20.

- El nivel de probabilidad de ocurrencia e impacto se mantendrá en la medida en la que se desarrolle la interconectividad e interdependencia, por lo que será conveniente atender a dos áreas que presentan un especial riesgo potencial: la tecnología de internet móvil y las conexiones entre sistemas informáticos *(machine to machine)*. El Global Risks Report considera que en este ámbito es esencial integrar programas de gestión física y cibernética para fortalecer el liderazgo y los procesos de negociación.

- Los datos se han denominado «*the oil of the 21 century*», pero diversos casos y estudios han puesto de manifiesto la incertidumbre legal que existe por la falta de regulación adaptada a los avances tecnológicos en áreas como: los flujos internacionales de datos o la impresión 3D, y en aspectos como la privacidad y la transparencia y control de la encriptación, además de la protección de la infraestructura tecnológica internacional de potenciales ataques terroristas.

- La incertidumbre sobre el impacto del desarrollo tecnológico en el mercado laboral (el US Bureau of Labor Statistics estima que en 2022 el 47 % de los trabajos en EE. UU. van a ser desempeñados por sistemas informáticos[167]).

- El acceso a la tecnología continúa siendo un aspecto que determina la desigualdad entre las diversas regiones del mundo (4 de los 7 billones de personas que viven en el planeta sigue sin tener acceso a internet).

De acuerdo con el análisis elaborado por EOS Data, la clasificación de los riesgos que producen un efecto mayor para la economía depende de las características de cada país. En todo caso, los riesgos tecnológicos, principalmente los producidos por ciberataques y robos de datos, afectan a la mayoría de países del mundo, pero tienen una especial relevancia en Estonia, Japón, EE. UU., Suiza, Malasia, Países Bajos, Singapur y Alemania, donde son la principal amenaza para la estabilidad socioeconómica[168]. En el conjunto de países del continente europeo, los ciberataques no forman parte de la lista de las principales amenazas salvo en Estonia, Alemania, Países Bajos y Suiza. Sin embargo, en Estados Unidos es una de las principales amenazas para la estabilidad, seguida por el robo de datos y el terrorismo. Y en China los ciberataques constituyen la tercera amenaza con mayor relevancia[169].

167 Carl Benedikt Frey y Michael A. Osborne, «The Future of Employment: How Susceptible are Jobs to Computerisation?», Oxford Martin School, University of Oxford (13 de septiembre de 2013), http://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf

168 *Op. cit.*, World Economic Forum (2016), p. 77.

169 *Op. cit.*, World Economic Forum (2016), p. 69.

3.2. Conectividad, hiperconectividad y ciberespacio

El desarrollo de las IT puede reducir la probabilidad de siniestros en muchos ámbitos gracias a los modernos sistemas de gestión y previsión del riesgo. Y de la misma manera, los daños derivados de los siniestros tradicionales pueden ser mitigados por medio de las nuevas tecnologías, especialmente gracias a la agilidad con la que se transmite y procesa la información.

En este sentido, el informe «Emerging Risks in the 21st Century an Agenda for Action», publicado por la OECD en 2003[170], hace referencia, en su apartado relativo a la tecnología, a dos aspectos esenciales con los que el desarrollo tecnológico puede generar notables riesgos para el desarrollo mundial que hasta este momento no existían:

- **La conectividad,** que es el elemento distintivo de las sociedades modernas (Castells, 1996)[171] que conlleva que el desarrollo de las IT en ámbitos como el transporte, el comercio y los sistemas de información haga que muchas actividades dependan de la interacción de una gran variedad de actores (a menudo en una escala global). Esta circunstancia es positiva con respecto al riesgo asegurador, en la medida en que se facilita la recogida y procesamiento de la información para la mejor gestión del siniestro. Pero la conectividad también multiplica los canales por los que las consecuencias negativas pueden ser propagadas.

- **La rapidez del desarrollo tecnológico y la vinculación o dependencia de los sistemas a la tecnología.** El ágil desarrollo del mercado tecnológico y el éxito con el que los nuevos productos son aceptados por los consumidores y reemplazan a los anteriores puede llevar, en algunas ocasiones, a que no se consideren todas las implicaciones futuras; máxime cuando los escenarios o posibles situaciones son ilimitadas y los efectos son impredecibles. Un ejemplo de esta falta de previsión fue el generalizado temor a los efectos del «*millennium bug*». Seguramente, esta situación fue imprevisible cuando se tomó la decisión acerca de la forma con la que debían de aparecer las fechas en los ordenadores.

Pues bien, lo dicho hasta aquí pone de manifiesto el carácter de los denominados nuevos riesgos que esencialmente derivan de las interconexiones de los sistemas, por lo que sus efectos potenciales pueden ser agravados como consecuencia de la dependencia de innumerables factores económicos y sociales a las IT.

---

170 «Emerging Risks in the 21st Century an Agenda for Action», OECD, 2003, p. 12, https://www.oecd.org/futures/globalprospects/37944611.pdf

171 M. Castells, *The Rise of the Network Society*, Oxford, Blackwell, 1996.

Por ello, los posibles fallos en los sistemas, los ciberataques y los delitos que se cometen por medio de las IT acentúan la necesidad de diseñar infraestructuras críticas cuidando de aspectos como la interdependencia; particularmente, en sectores relacionados con la energía, la información, las comunicaciones y el transporte, en los que un pequeño fallo puede llegar a ocasionar efectos catastróficos.

La omnipresencia de las IT y la importancia de las tecnologías relacionadas con elementos básicos para la sociedad hacen que cualquier interrupción o fallo tenga un alto impacto en la estabilidad económica y social a nivel mundial[172].

En este sentido, aunque históricamente eran necesarios muchos recursos para causar consecuencias devastadoras con transcendencia económica y política, actualmente es posible que individuos adecuadamente cualificados las causen de forma remota y anónima por medio de los sistemas informáticos. Tales circunstancias ponen de manifiesto el **traspaso de poder al mundo tecnológico y el paradigma de la necesidad de un espacio tecnológico sano**[173]. Además, desde esta perspectiva se deben considerar los denominados riesgos sistemáticos que al afectar a diversos aspectos del sistema toman un carácter global, cuya protección debe formar parte de las políticas y estrategias generales.

Desde el punto de vista de los beneficios que reporta la hiperconectividad, podemos mencionar que este efecto del desarrollo tecnológico facilita la creación del denominado ciberecosistema (con las particularidades sobre las que profundizaremos en este punto), que representan un interés que excede del ámbito exclusivamente particular, y ofrece una gran cantidad de beneficios al permitir y agilizar las diferentes relaciones sociales y económicas. En este sentido, destaca, por un parte, la creciente dependencia de la sociedad a las IT que se pone de manifiesto por medio de distintos elementos como infraestructuras críticas —de las que dependen diversos sistemas esenciales para la estructura socioeconómica global— o el denominado internet de las cosas —del que dependen los sistemas más cotidianos—, y por otra parte, la creación de estructuras complejas propicias al desarrollo de la hiperconectividad.

Todo ello produce una situación de desconfianza que reduce la agilidad del crecimiento de las IT y los mercados en general, y mantiene el temor que forma parte del denominado Cybergeddon[174].

---

172 *Op. cit.*, World Economic Forum (2011).

173 *Op. cit.*, World Economic Forum (2012), p. 24.

174 J. Healey, «The Five Futures of Cyber Conflict and Cooperation. Atlantic Council Issue Brief», 2011, http://www.atlanticcouncil.org/publications/issue-briefs/the-five-futures-of-cyber-conflict-and-cooperation

En efecto, el desarrollo de las IT y de la denominada conectividad ha facilitado la creación de un sistema mundial con fuertes vínculos económicos y sociales, lo que ha agilizado el proceso de globalización. Al mismo tiempo, tal proceso lleva consigo un aumento de la interdependencia que en el ámbito de los daños configura la principal particularidad de los siniestros en el siglo XXI. **De esta forma, se han creado los denominados «mega-risks», que tienen el potencial para causar importantes daños en los sistemas y en las infraestructuras de las que depende tanto nuestra sociedad como la economía global. Esta situación puede crear graves dificultades para las entidades tradicionales de gestión del riesgo y de riesgo compartido, como la industria de seguros[175].**

3.2.1. La teoría de los ecosistemas digitales

a) Concepto

La denominación «ecosistema digital» proviene de considerar que las IT producen continuas interacciones entre usuarios, empresas y gobiernos, y esto crea una comunidad digital que es, en cierta manera, independiente y autónoma; o por lo menos tiene unos hábitos y características culturales particulares[176] cuyo funcionamiento y sostenibilidad se puede comparar con los ecosistemas naturales.

Así, un ecosistema de vida natural se define como una comunidad biológica de organismos que interactúan y su entorno físico. De la misma manera, un ecosistema de negocios se puede considerar como «la red de compradores, proveedores y fabricantes de productos o servicios relacionados» y el entorno socioeconómico (en el que se incluye el marco institucional y normativo).

Por ello, un ecosistema digital es una infraestructura digital de autoorganización destinada a la creación de un entorno digital para las organizaciones en red que apoya la cooperación, el intercambio de conocimientos, el desarrollo de tecnologías abiertas y adaptables y modelos de negocio evolutivos.

El enfoque de ecosistema digital incorpora los conceptos al mundo digital, aplicando los mecanismos de los ecosistemas naturales. De igual manera que existen varios ecosistemas naturales que interactúan, pueden existir

175 «Emerging Risks in the 21st Century, the Secretary-General Emerging Risks», OECD, https://www.oecd.org/futures/globalprospects/37944611.pdf

176 Digital Ecosystem Community: Envisioning the future of the Digital Ecosystem, World Economic Forum (2007), http://www3.weforum.org/docs/WEF_DigitalEcosystem_Scenario2015_ExecutiveSummary_2010.pdf

varios ecosistemas digitales, debido a la diferenciación y el desarrollo de productos y servicios adaptados a las necesidades locales específicas[177].

En este sentido, se han pronunciado diversos estudios y modelos entre los que podemos destacar:

- Digital Ecosystems: Evolving service-oriented architectures[178].
- The digital ecosystems research vision: 2010 and beyond[179].
- Open Philosophies for Associative Autopoietic Digital Ecosystems (OPAALS)[180].
- The Vision of DEBI Institute: Digital Ecosystems and Business Intelligence[181].
- Digital Ecosystem Community: Envisioning the future of the Digital Ecosystem[182].

Una de las explicaciones con mayor relevancia del concepto es la aportada por *The Ecological Cognition Framework* publicado en 2007[183], que define tres niveles de comportamiento para comprender la interacción de los usuarios de las IT y el motivo que les instiga a formar parte del ciberecosistema[184]. En primer lugar, describe lo que impulsa a las personas a llevar a cabo acciones en las comunidades *online;* en segundo lugar, analiza las clases de

177 Digital Ecosystems, DG-Cnect of the European Commission, http://www.digital-ecosystems.org/

178 G. Briscoe y P. De Wilde, «Digital Ecosystems: Evolving service-oriented architectures». In Conference on Bio Inspired Models of Network, Information and Computing Systems. IEEE Press, 2006, https://arxiv.org/abs/0712.4102

179 P. Dini, N. Rathbone, M. Vidal, P. Hernández, P. Ferronato, G. Briscoe y S. Hendryx. «The digital ecosystems research vision: 2010 and beyond», European Commission (julio de 2005), http://www.digital-ecosystems.org/events/2005.05/de_position_paper_vf.pdf

180 Open Philosophies for Associative Autopoietic Digital Ecosystems (OPAALS), Information Society Technologies, http://www.lse.ac.uk/media@lse/research/OPAALS/D9.4.pdf

181 E. Chang, M. Quaddus y R. Ramaseshan, «The Vision of DEBI Institute: Digital Ecosystems and Business Intelligence», DEBII (2006).

182 «Digital Ecosystem Community: Envisioning the future of the Digital Ecosystem», World Economic Forum (2007), http://www3.weforum.org/docs/WEF_DigitalEcosystem_Scenario2015_ExecutiveSummary_2010.pdf

183 J. Bishop, «Increasing participation in online communities: A framework for human-computer interaction», *Computers in Human Behavior* (Elsevier Science Publishers) (2007), https://trac.v2.nl/export/7500/andres/Documentation/Behaviour%20modification/Increasing%20participation%20in%20online%20communities.pdf

184 V. Holzmann, S. Dubnov, «Understanding the Collaboration Enigm», *The International Journal of Knowledge, Culture, & Change Management* (julio de 2011), https://www.researchgate.net/publication/235872389_Understanding_the_Collaboration_Enigma

conocimientos que utilizan los usuarios para determinar si procede o no tener este tipo de acciones; y en tercer lugar, examinan los medios por los que pasan por llevar a cabo la acción en el entorno.

A su vez, la idea de ecosistema ha conseguido reunir a comunidades de investigación alrededor de todo el mundo, como la International Conference on Digital Ecosystems and Technologies (DEST), sobre los ecosistemas y tecnologías digitales, y la Conferencia ACM, sobre la gestión de los ecosistemas digitales emergentes (MEDES). En particular, esta idea surge de aplicar los modelos de autoorganización y evolución de la biología a los diferentes aspectos del software, basándose en el supuesto de que si se alcanza un cierto comportamiento «biológico» del software, se optimizará la función catalítica de las IT con relación al crecimiento socioeconómico y la innovación.

b) Características

El informe «Digital Ecosystem Convergence between IT, Telecoms, Media and Entertainment: Scenarios to 2015», publicado por el WEForum, plantea las IT como un ecosistema en evolución que se encuentra en su etapa más primitiva. Por lo que el informe considera que este emergente ecosistema digital genera muchos riesgos y desafíos para las políticas gubernamentales, y presenta nuevas oportunidades para la creación de valor social y económico. Además, al igual que cualquier ecosistema saludable, permite a las partes interesadas interactuar y crear relaciones que constituyan un beneficio para todos, permitiendo a sus participantes crear valor económico y proporcionar bienestar a la sociedad. No obstante, también pueden generar una serie de incertidumbres que afecten a la estructura del mercado, los derechos de propiedad intelectual, la seguridad y la privacidad[185].

En el marco de la Unión Europea este concepto fue acuñado en 2002 como «ecosistemas de negocios digitales»[186], destinados a aplicar los ambiciosos objetivos establecidos en el Consejo de Lisboa, que se centraban en promocionar mayor crecimiento económico, la creación de más y mejores puestos de trabajo, así como el desarrollo de programas de inclusión social, teniendo en cuenta las peculiaridades del desarrollo europeo, sobre todo basado en una red difusa de pymes y los sistemas locales de innovación. Desde este punto de vista, el desarrollo de los ecosistemas digitales se enmarcó en la

185 «Digital Ecosystem Convergence between IT, Telecoms, Media and Entertainment: Scenarios to 2015», WEForum (3 de noviembre de 2007), http://www3.weforum.org/docs/WEF_Digital Ecosystem_Scenario2015_ExecutiveSummary_2010.pdf

186 Francesco Nachira, «Towards a network of digital business ecosystems fostering the local development», European Comission DG INSFO, Bruselas (septiembre de 2002).

línea el uno de los objetivos contenidos en el «i2010, A European Information Society for growth and employment», cuya finalidad era definir las políticas de negocio con el objetivo de eliminar las barreras tecnológicas, organizativas y legales para la adopción de las TIC. Y, posteriormente, tal materia fue ampliamente abordada en el Séptimo Programa Marco (2007-2013) de la Comunidad Europea para Acciones de Investigación y Desarrollo Tecnológico.

Los estudios desarrollados por la DG-Cnect of the European Commission[187] en el marco de los ecosistemas digitales concluyen que la creación de una red de ecosistemas digitales ofrecerá una inmejorable oportunidad para que las pymes y las zonas de menor desarrollo participen en la economía global. Así, se considera que las nuevas formas de interacción dinámica permitidas por los ecosistemas digitales podrán fomentar el crecimiento económico local. De tal manera, esta tecnología puede contribuir a preservar el conocimiento, la cultura y la identidad local, y a reducir la brecha digital entre las diferentes comunidades.

En este sentido, se puede considerar que los principales retos tecnológicos en torno a los ecosistemas digitales están principalmente encaminados a apoyar el surgimiento y la sostenibilidad de los ecosistemas de negocio en red basados en el conocimiento. Principalmente, podemos señalar: el crecimiento de las zonas geográficas (o virtuales), la mejora de la innovación, la productividad y la inclusión social, a través de la utilización óptima de los recursos locales, y la interacción global autorizada por las TIC. El apoyo al intercambio de conocimientos, la creación de cadenas de valor en todo el mundo y la creación de redes de negocios transitoria promoverán la cooperación mundial y la creación de formas alternativas de desarrollo de software y de negocios.

Las tecnologías desarrolladas dentro del marco de los ecosistemas digitales tienen por objeto proporcionar una infraestructura de conocimiento orientada a la prestación de servicios que permitan una composición espontánea, la distribución, la evolución y la adaptación de los servicios basados en las IT. De tal manera, estas características son propias del *open source software* y de la industria del software SME, que son plataformas a través de las cuales se desarrollan y difunden de forma independiente los servicios y componentes del software que integran los ecosistemas digitales con la finalidad de formar soluciones complejas, evolutivas y que se adapten a las nuevas realidades. En especial, el software de código abierto (*open source software* —OSS—), que es el software cuyo código fuente y otros derechos que normalmente son exclusivos de quienes ostentan los derechos y propiedad sobre los mismos

187 «Growing a Digital Social Innovation Ecosystem for Europe DSI Final Report», DG-Cnect of the European Commission (2015), pp. 22-34, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=8907

son publicados bajo una licencia de software compatible con la Open Source Definition[188] o forman parte del dominio público (la OSS Watch utiliza esta lista aprobada por la OSI como medio para evitar debates sobre la interpretación de la definición de código abierto; así, se ha reconocido de forma mayoritaria al OSI como la autoridad final para determinar el software que forma parte del concepto de OSS). Estas tecnologías permiten el desarrollo espontáneo y la disposición cooperativa de servicios y soluciones sin la necesidad de ningún agente de coordinación o control central, de tal manera que se distribuye el conocimiento de forma libre y autónoma.

En los distritos industriales creados a mediados del siglo XX se reunieron diferentes industrias con características similares y complementarias, convirtiéndose de esta manera en los motores del crecimiento económico de diversas regiones a lo largo del mundo. Actualmente, el conocimiento y la experiencia se preservan y desarrollan en las empresas mediante las IT, lo que refuerza la conectividad y el intercambio de información, y proporciona un desarrollo social y económico equivalente al de aquellos distritos industriales.

Por ello, la capacidad de las IT por capturar, formalizar, retener y compartir el conocimiento a nivel sectorial y regional podría considerarse como un bien público que proporciona una infraestructura común. Y en concreto, los ciberecosistemas abiertos son un buen ejemplo para entender esta postura, ya que permiten establecer entornos que conservan y redistribuyen el conocimiento publicado por sus usuarios. De tal forma, se construye una red de conocimiento y experiencia en continuo desarrollo.

c) Efectos

La convergencia entre los sistemas, estructuras y agentes que forman los ecosistemas digitales lleva consigo un claro beneficio para los consumidores, que pueden acceder a una mayor variedad de productos y servicios de forma más rápida y personalizada, pero también produce dificultades regulatorias.

La complejidad de los mercados de los ecosistemas digitales aumenta la incertidumbre regulatoria, y el frenético ritmo de desarrollo y cambio hace que la regulación quede rápidamente obsoleta. Y tal necesidad ya se puso de manifiesto por la Comisión Europea en 1999 al considerar que la relación entre los sectores de telecomunicaciones, radiodifusión e IT estaba transformando el mercado de las comunicaciones; y en particular, con relación a la convergencia entre comunicaciones fijas, móviles, terrestres y por satélite, y los sistemas de localización y comunicación.

188 Open Source Definition, Open Source Iniciative, https://opensource.org/osd

Así, desde el punto de vista de las infraestructuras de comunicaciones y los servicios relacionados, la mencionada convergencia hace que la separación tradicional de las normas, que regulaban estos sectores, sea cada vez más inapropiada. Por ello, parece necesario el desarrollo de un régimen regulador coherente, y que comprenda estos medios de forma conjunta[189]. Además, la rapidez con la que se desarrolla el ámbito de los ciberecosistemas, debido a la creciente innovación y la rápida entrada en el mercado de las IT de nuevos competidores, puede aumentar el coste y la dificultad para regular este ámbito.

Las características de los ciberecosistemas plantean diversos problemas regulatorios que aquí se irán enunciando y que en términos generales se pueden englobar en torno a dos teorías, según se prime la libertad del sistema o el control y seguridad del mismo.

Como se ha visto, los ecosistemas requieren de la actuación libre y espontánea de los sujetos que actúan en ellos, y tal circunstancia produce un evidente beneficio para la agilidad de las transacciones, actividades y operaciones que se llevan a cabo por medio de las IT. En este sentido, se pueden enunciar dos teorías contrapuestas:

- La libertad como un bien público susceptible de protección en el que, además de la protección de las libertades individuales y colectivas, se garantice el fomento de los sistemas de código abierto y la limitación de las restricciones a la trasmisión y el alojamiento de datos.

- Comprender que el verdadero interés público lo representa la seguridad y los derechos de los sujetos que forman parte del ciberecosistema, y que son ellos junto a la integridad de las infraestructuras y sistemas de las IT el bien susceptible de protección.

No obstante, en cualquiera de los dos casos, si las políticas y las instituciones reguladoras no se adaptan a los cambios del mercado, se pondrían de manifiesto las vulnerabilidades del ecosistema digital. Y, en definitiva, esto sería un riesgo potencial para la libre competencia, se ralentizaría la innovación y en última instancia se podría privar a los consumidores de los beneficios del progreso tecnológico.

En todo caso se pueden identificar tres principios esenciales dentro de las normas que con relación a los ciberecosistemas se están aplicando en todo el mundo:

189 European Commission, «A New Framework for Electronic Communications Services COM», 539 final (10 de noviembre de 1999), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l24216

- Las normas deben centrarse en la funcionalidad en lugar de basarse en la estructura de la tecnología. Es decir, la regulación debe ser diseñada para lograr su objetivo de la manera más eficiente, sin tener en cuenta las tecnologías, las estructuras de la industria y los regímenes legales existentes. En efecto, la normativa y las instituciones diseñadas alrededor de definiciones obsoletas de los diversos productos y servicios del mercado tecnológico tienden a ser reemplazadas por enfoques más amplios que permitan comprender la realidad de los ecosistemas digitales en su conjunto.

- Los *digital ecosystem* son dinámicos y complejos, por ello su regulación debe ser flexible y dinámica, pues es necesario que se acomode rápidamente a los cambios tecnológicos y del mercado, y establezca un marco legal que garantice la confianza de los agentes que forman parte del ciberecosistema.

- Los cambios profundos y radicales que producen los ciberecosistemas implican que la regulación de los mismos deba plantearse desde el principio. En muchos casos, la intensa competencia que se produce en los mismos hace innecesaria su regulación, o al menos esta deberá ser muy limitada. En relación con algunos aspectos como la privacidad y los ciberriesgos, se nos plantean nuevos desafíos legislativos cuya regulación debe seguir los nuevos enfoques a los que aquí hacemos referencia.

3.2.2. Efectos de la hiperconectividad y riesgos sistémicos

Los ciberriesgos no son un problema aislado, sino que forman parte de una realidad mucho más amplia que abarca cada aspecto de la sociedad actual conforme a los efectos del desarrollo tecnológico y de las tecnologías de la información.

De esta forma, la naturaleza de las IT produce el aumento exponencial de la tasa de personas, procesos y cosas que se encuentran conectados a internet, lo que se ha denominado «hiperconectividad»[190].

Y como consecuencia de esta hiperconectividad, el informe «Risk and Responsibility in a Hyperconnected World», publicado en 2014 por el World Economic Forum, establece tres posibles escenarios en los que previsiblemente se situará el ciberecosistema en 2020[191]:

190 «Risk and Responsibility in a Hyperconnected World», World Economic Forum (febrero de 2014), p. 5, http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf

191 *Op. cit.*, World Economic Forum (febrero de 2014), p. 26, http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf

- **Escenario 1,** *Mudding into the Future:* en este escenario el nivel de amenazas aumenta, al mismo tiempo que avanza la sofisticación de las herramientas de ataque y defensa. No se establecen políticas homogéneas entre los diferentes gobiernos y organizaciones internacionales, sino que los controles de seguridad son establecidos por las instituciones individuales. Por ello, se advierte de que las soluciones de seguridad se fragmentarían, lo que produciría ineficiencias, pero aparecerían oportunidades para el desarrollo de empresas tecnológicas dedicadas a la ciberseguridad.

- **Escenario 2,** *Backlash Decelerates Digitization:* se considera la posibilidad de que aumenten las políticas públicas de protección contra los ciberataques y se establezcan planes internacionales de prevención, limitando y estableciendo barreras al tráfico de datos y la libertad del ecosistema digital. Por ello, se concluye que, en este escenario, el desarrollo de las IT y todo el ámbito relacionado con el ciberespacio se ralentizaría, lo que dificultaría la creación de medios de seguridad y facilitaría la generación de vulnerabilidades.

- **Escenario 3,** *Cyber Resilience Accelerates Digitization:* en este escenario se plantea la posibilidad de que tanto empresas como organismos públicos desarrollen políticas de ciberseguridad y planes de actuación conjuntos. De tal manera, se fomentaría la creación de organismos y acuerdos internacionales de colaboración entre instituciones públicas y privadas, y el desarrollo de sistemas de protección más sofisticados. Y todo ello permitirá que la información, las relaciones, las operaciones y las transacciones que tienen lugar en el ecosistema digital se produzcan con mayor facilidad, eficiencia y libertad.

Del análisis de las estimaciones que aporta el estudio «Risk and Responsibility in a Hyperconnected World» podemos extraer que en el tercer escenario podría llegar a generarse un valor de 3,72 trillones de USD.

En el primer escenario, el temor a las vulnerabilidades reduciría entre 130 y 470 billones de USD el potencial económico; y en el segundo escenario, la ralentización del desarrollo tecnológico no pemitiría la generación de 1,4 trillones de USD[192].

Con el título «El lado oscuro de la hiperconectividad» *(The Dark Side of Connectivity),* el informe Global Risks 2012 publicado por el World Economic Forum advierte que la hiperconectividad ha producido un aumento de la

192 «Risk and Responsibility in a Hyperconnected World», World Economic Forum (febrero de 2014), p. 30, http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf

dependencia de la vida diaria de las IT y los sistemas informáticos, lo que relaciona los riesgos del mundo físico con las amenazas del ciberespacio. Esta situación hace que un evento cibernético de escasa entidad o un ataque perpetrado con medios muy limitados produzcan daños de gran relevancia[193].

Los fallos de las infraestructuras críticas son el principal ejemplo de la potencial amenaza cibernética que se pone de manifiesto por medio de la hiperconectividad al eliminar los límites y barreras del alcance de los daños. Por estos motivos, la seguridad de cada uno de los sistemas individuales que forman el ecosistema digital contribuye a crear un espacio digital «sano», que puede constituir un beneficio para todos los sujetos que en él actúan. Y esto es más importante si consideramos, como se menciona en el referenciado informe, que para hacer frente al lado oscuro de la hiperconectividad, es necesario aceptar el hecho de que no hay sistemas completamente seguros, sino sistemas cuyas vulnerabilidades aún no se han descubierto[194].

Además, los fallos en las infraestructuras críticas son uno de los riesgos tecnológicos con mayor influencia, tanto en relación con los elementos del ciberespacio, como con los que son externos a este. Por ello, este tipo de amenazas se puede considerar como un centro de gravedad sobre el que gravitan el resto de riesgos, ya que mantiene una importante relación directa con las amenazas propias del ámbito económico, medioambiental y geopolítico[195].

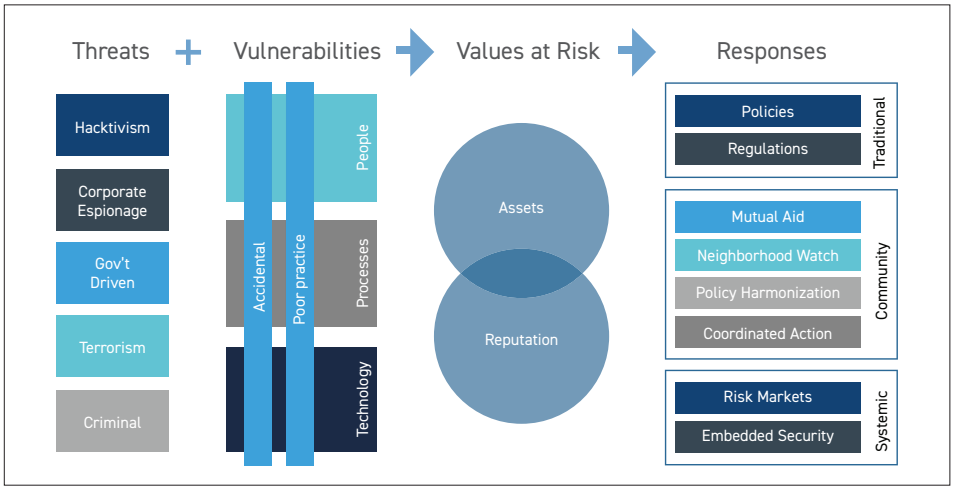
La hiperconectividad relaciona unos sistemas con otros entre los que se producen continuas conexiones e interacciones, y ello junto con el carácter impredecible de los cibereventos que dificulta el análisis de los elementos que entran en juego cuando se produce un evento cibernético. Estos elementos, que nos servirán para desarrollar el esquema de la responsabilidad, se pueden expresar conforme al siguiente esquema.

193 Global Risks 2012, World Economic Forum (2012), pp. 24-25.

194 *Op. cit.,* World Economic Forum (2012), p. 27.

195 *Op. cit.,* World Economic Forum (2012), p. 44.

Gráfico 9. La responsabilidad en un mundo hiperconectado



Fuente: World Economic Forum (2012)[196].

En la naturaleza son numerosos e impredecibles los riesgos sistémicos que se pueden poner de manifiesto, y tal concepto también se puede aplicar al ámbito de los riesgos que afectan al sistema financiero, a la economía global y ahora a los ciberriesgos. Así, esta consideración proviene del potencial impacto sistémico de los cibereventos en la seguridad y economía nacional[197]. En los informes publicados por la DTCC (Systemic Risk White Paper 2013), se considera que la naturaleza crítica y el efecto de la interconexión que causan los ciberriesgos hacen que estos constituyan la mayor amenaza sistémica que afecta no solo a los mercados financieros y a la industria, sino también a la estabilidad gubernativa y militar[198].

Tal perspectiva se confirmó con la encuesta DTCC's Systemic Risk Barometer survey (octubre de 2014) en la que el 84 % de los expertos preguntados situó las ciberamenazas dentro de uno de los cinco principales daños sistémicos[199],

196 Figure 41: Framework for Cyber Threats and Responses, *op. cit.*, World Economic Forum (2012), p. 46.

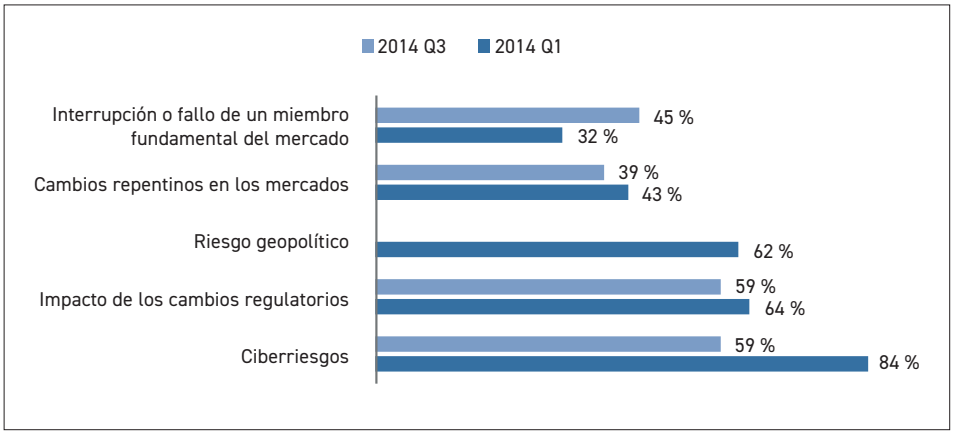
197 *Cyber Risk, a Global Systemic Threat*, A White Paper to the Industry on Systemic Risk, DTCC (octubre de 2014), Prólogo, https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjG7Ibqw-bPAhXCQBQKHUveB5UQFggcMAA&url=http%3A%2F%2Fwww.dtcc.com%2F~%2Fmedia%2FFiles%2FDownloads%2Fissues%2Frisk%2Fcyber-risk.pdf&usg=AFQjCNHaLHeWuZLVBLjiw_2JwBAUCh4xPA&sig2=QE0u1kerPcAwi_6NYsv-_w&bvm=bv.136499718,d.d24

198 *Op. cit.*, A White Paper to the Industry on Systemic Risk, DTCC (octubre de 2014), p. 1.

199 Systemic Risk Barometer, DTCC, 2014, http://www.dtcc.com/~/media/Files/Downloads/issues/risk/Systemic_Risk_Summary_Report.ashx

y la realizada en 2013 por International Organization of Securities Commissions, en la que un 89 % consideró que el riesgo potencial que implica el cibercrimen en los mercados era el principal riesgo sistémico.

Gráfico 10. Riesgo para la economía en su conjunto



Elaboración propia desde la fuente «Top 5 Risk Identified, Risk to Broader Economy»[200].

Por otra parte, la hiperconectividad no solo facilita que los daños se extiendan por todo el sistema produciendo una gran cantidad de efectos indirectos, sino que también permite que los propios ataques dañen de forma directa un gran número de sistemas. Así, la nueva generación de ataques también tiene carácter sistémico, ya que estos se identifican por la utilización de malware diseñado para infectar sistemas de forma masiva por medio de múltiples medios (web, mail, aplicaciones…)[201]. Los ataques sistémicos permiten obtener gran cantidad de datos e información de todo el ecosistema y establecer una red de sistemas infectados (Boths) que pueden ser utilizados como medio de otros ataques. El Cybergeddon representa una situación catastrófica que refleja los posibles perjuicios de la hiperconectividad, tal miedo en torno a la incertidumbre y las dudas que pueden existir acerca de los efectos potenciales de las ciberamenazas se fundamentan en el hecho de que las principales infraestructuras críticas (energía, agua, transportes…) se controlan por medio de sistemas conectados a internet, igual que el sistema financiero global, ya

200 «Top 5 Risk Identified, Risk to Broader Economy», Systemic Risk Barometer, *DTCC* (2014), p. 3 http://www.dtcc.com/~/media/Files/Downloads/issues/risk/Systemic_Risk_Summary_Report.ashx

201 Advanced Targeted Attacks: How to Protect Against the New Generation of Cyber Attacks, FireEye (2015), p. 4, http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-targeted-attacks.pdf

que el propio dinero es digital[202] (bitcoins, PeerCoin, Ripple, Litecoin, Dogecoin, etc.).

No obstante, podemos usar esta imagen como una advertencia de los efectos que a menor escala pueden ponen de manifiesto los ciberriesgos, y que pueden tratarse de verdaderos daños actuales. En efecto, el desarrollo de las IT y la estabilidad del mercado dependen de la confianza de la sociedad, y por este motivo una pérdida generalizada de la confianza o el aumento de los daños por consecuencia de ciberataques llevaría consigo una mayor intervención, lo que produciría la necesaria pérdida del carácter esencial de internet como sistema abierto y libre, y por ende la pérdida de su principal valor.

Por otra parte, esta situación puede afianzarse como consecuencia de la naturaleza cada vez más fragmentada de internet, lo que puede llegar a frustrar los intentos de lograr un acuerdo global sobre nuevas tecnologías y las normas de seguridad. En este caso, la cooperación internacional entre las naciones y organismos públicos y privados, y el desarrollo de sistemas de prevención, dejaría de producir efectos tanto por la pérdida de confianza, como por la existencia de ataques cada vez más sofisticados e implacables. Este escenario se ha denominado como «crecimiento inseguro»[203] para el caso en que el desarrollo de los ciberataques impida mantener el nivel de confianza de los consumidores y sea necesario plantear medios de defensa mucho más costosos.

3.2.3. Ciberespacio

Los *digital ecosystems*, como cualquier otro ecosistema, tienen su propio hábitat entendido por aquel lugar de condiciones apropiadas para la vida —actividad que desarrolla una persona o una comunidad— de un organismo, especie o comunidad animal o vegetal[204].

En efecto, tal hábitat se denomina *cyberspace* o ciberespacio, y es el medio ambiente en el que se producen las comunicaciones a través de redes de ordenadores[205].

202 Derek O'Halloran, «Tech utopia or cybergeddon?» (22 de enero de 2013), https://www.weforum.org/agenda/2013/01/tech-utopia-or-cybergeddon/

203 «The Evolving Internet: Driving Force, Uncertainties, and Four Scenarios to 2025» CISCO (2010) http://newsroom.cisco.com/dlls/2010/ekIT/Evolving_Internet_GBN_Cisco_2010_Aug_rev2.pdf

204 Vida, *Diccionario de la Lengua Española*, Edición del Tricentenario, RAE, http://dle.rae.es/?id=blw7uSa

205 Cyberspace, *Oxford Living Diccionaries*, Oxford University, http://www.oxforddictionaries.com/us/definition/american_english/cyberspace

Este concepto empezó a popularizarse después de que John Perry Barlow pronunciase el discurso «A Declaration of the Independence of Cyberspace» el 8 de febrero de 1996 en Davos (Suiza)[206]. Declaración mediante la que reivindicaba la libertad del *cyberespace*, y advertía a los gobiernos e instituciones públicas de que no ejercen ninguna soberanía sobre este medio en el que los ciudadanos viven en plena libertad sin que puedan ser objeto de discriminación alguna.

La RAE ha acogido el término ciberespacio como «ámbito artificial creado por medios informáticos»[207], no obstante parece que el concepto que determina el mismo tiene más vínculo con las relaciones sociales que con el sistema tecnológico que lo forma[208], aunque no hay una definición aceptada para este concepto[209]. La agencia estadounidense de telecomunicaciones (International Telecomunication Union —ITU—) considera que está formado por sistemas y servicios conectados directa, o indirectamente, por medio de internet, telecomunicaciones o red de ordenadores[210]. La *International Organization of Standardization* (ISO/IEC 27032:2012) define el *cyberspace* como el complejo medioambiental resultante de la interacción de personas, software y servicios de internet mediante dispositivos tecnológicos y redes informáticas que los conectan entre sí, los cuales no existen en forma física[211].

Y, finalmente, las definiciones más completas del *cyberspace* lo consideran como un dominio global y dinámico caracterizado porque combina el uso de sistemas electrónicos y electromagnéticos con el propósito de crear, almacenar, modificar, intercambiar y extraer información. Por lo tanto, el *cyberspace* está formado por: sistemas físicos y dispositivos tecnológicos que permiten la interconexión entre ordenadores (entendidos en el sentido amplio que incluye todos los dispositivos SCADA); un sistema de ordenadores (dispositivos SCADA) y software que garantiza la operatividad, funcionalidad y la conectividad de un dominio básico; una red entre sistemas de ordenadores (intranet); una

206 Jhon Perry Barlow, «A Declaration of the Independence of Cyberspace», Electronic Frontier Fundatio EFF (8 de febrero de 1996), https://www.eff.org/es/cyberspace-independence

207 Ciberespacio, *Diccionario de la Lengua Española*, Edición del Tricentenario, RAE, http://dle.rae.es/?id=98Wdd57

208 Chip Morningstar y F. Randall Farmer, *The Lessons of Lucasfilm's Habitat. The New Media Reader*, Ed. Wardrip-Fruin and Nick Montfort, The MIT Press, 2003.

209 «Cyberpower and National Security: Policy Recomendations for a Strategic Framework», en F. D. Kramer, S. Starr, L. K. Wentz (ed.), *Cyberpower and National Security*, National Defense University Press, Washington (DC), 2009.

210 Frederick Wamala, *The ITU National Cybersecurity Strategy Guide*, CISSP (septiembre de 2011).

211 ISO/IEC 27032:2012 Information Tecnology Security Techniques, Guidelines for Cybersecurity, ISO, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44375

red de redes que conecta diversos sistemas (internet); nodos de acceso y nodos de rutina intermediarios; y los datos alojados en todo el sistema.

Pues bien, una vez hemos concretado que el *cyberspace* es el hábitat en el que se desarrollan los *digital ecosistems*, deberemos atender a las dos realidades que forman el *cyberspace;* por un lado, la realidad física constituida por la estructura que permite el funcionamiento de internet; y, por otro lado, la realidad inmaterial formada por los datos que se almacenan, modifican, intercambian, crean y extraen por medio de estos sistemas.

En cuanto a la primera realidad o aspecto material del *cyberspace* al que haremos referencia en el próximo apartado, se puede considerar que la estructura primaria del *cyberspace* está formada por los *Backbone networks*, que conectan ordenadores en distintas localizaciones geográficas por medio de redes de fibra óptica o mediante satélite. Este sistema está configurado por una estructura internacional de cableado y red satélite que conecta unas ciudades con otras y se extiende por todo el mundo transportando paquetes de información de un punto a otro por medio de la Transmision Control Protocol/Internet Protocol (TCP/IT). Por su parte, cada proveedor de servicios de internet mantiene su propia *Backbone network* interconectada con varios *Internet exchange points* (IXP) alrededor de todo el mundo[212].

212 J. Tyson, «How Internet Infrastructure Works» (recuperado el 9 de febrero de 2011), p. 5.

4. CUESTIÓN DE INTERÉS Y SEGURIDAD NACIONAL

La seguridad del ámbito público es un elemento esencial de la ciberseguridad. Como hemos visto, las características del ciberespacio hacen que se forme una red internacional que conecta a individuos y organizaciones que forman el ecosistema digital. Por ello, los acontecimientos que se produzcan en este ámbito pueden afectar gravemente a una innumerable cantidad de elementos y sujetos, lo que pone de manifiesto la importancia de la ciberseguridad. Además, si comprendemos que el ciberespacio es el marco en el que interactúan diversos agentes de forma independiente y voluntaria, y que de tal forma se constituye un espacio diferenciado y distinto a la realidad física, podría ser lógico entender que la seguridad e integridad de este espacio forma parte de un interés colectivo.

En este sentido, podemos afirmar que ciertos aspectos del ciberespacio forman parte del interés colectivo o afectan necesariamente a los intereses públicos, lo que justifica la aplicación de la regulación administrativa en el ámbito de las IT y, en su caso, del Derecho Penal.

Tales disposiciones son especialmente relevantes en relación con la seguridad nacional y los derechos y libertades públicas que se ejercitan en el ciberespacio, por lo que el presente apartado se centrará en la aplicación de las normas de carácter penal y administrativo.

4.1. Interés público del ciberespacio

Las infraestructuras críticas que sostienen las acciones comunes de la vida diaria dependen cada día más de las IT y los sistemas hiperconectados. Por lo que, como hemos mencionado al definir el carácter de las ciberamenazas, históricamente eran necesarios muchos recursos para causar un daño que ocasionase consecuencias devastadoras, pero actualmente este tipo de daños pueden ser producidos por un individuo anónimo con un ordenador personal. Tal situación pone de manifiesto la importancia de establecer medidas que permitan garantizar un ciberecosistema saludable[213].

213 *Op. cit.*, World Economic Forum (2012), p. 24.

En este sentido, se puede considerar que la seguridad *online* foma parte del bien común, por lo que quedaría amparada dentro de la categoría del interés público, y esto conlleva que la inversión privada en este ámbito debe ser garantizada. Las acciones de guerra, el terrorismo, el cibercrimen y otros eventos susceptibles de ocasionar daños físicos son eventos que ya se tenían en cuenta por las políticas de seguridad tradicional; no obstante, y como hemos mencionado, el aumento del número de estas acciones en el ciberespacio crece de forma exponencial[214].

Además, la confianza es un factor esencial en el sistema socioeconómico actual en el que las expectativas y el potencial que ofrece un territorio son circunstancias que afectan directamente a su situación económica. Así, el colapso de una estructura crítica derivado de un ciberevento podría ocasionar la inmediata desconfianza y temor de la sociedad, lo que produciría un indudable daño económico.

No obstante, basta con el temor a que esta situación puede llegar a producirse para que se genere de forma progresiva una desconfianza generalizada entre los consumidores que lastre el desarrollo del ciberespacio. En este sentido, la primera consecuencia que producen los ciberriesgos es el daño psicológico, del que forma parte el temor de los consumidores, usuarios y demás agentes que actúan en el ciberespacio a los potenciales efectos de los mismos, que les puede llevar a tomar ciertas medidas de precaución (en el sentido de la reticencia a la utilización de ciertos medios y sistemas). Esta consecuencia de las IT en el marco económico hace que compañías de diversa índole centren sus preocupaciones en los ciberriesgos (en cuanto a la reputación e impacto en los precios del mercado), considerando este ámbito como un aspecto estratégico que requiere una política estratégica efectiva. Algunos países también han tomado medidas específicas para posicionarse como lugares seguros para hacer negocios en la era digital, al integrar la ciberseguridad entre sus capacidades principales[215].

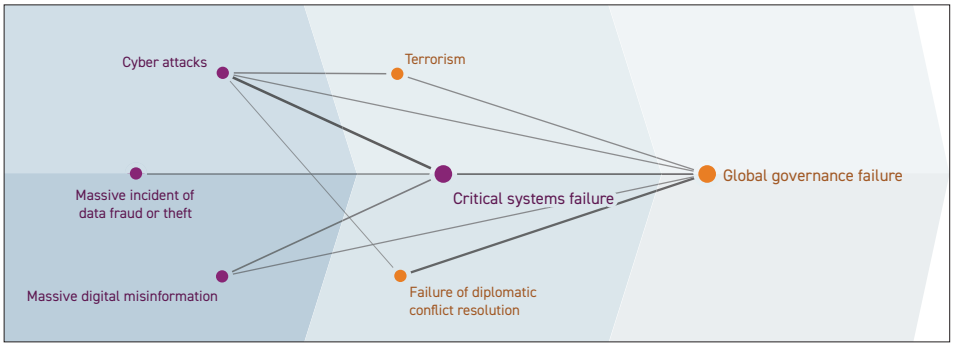
Los fallos de las infraestructuras críticas se han calificado como el centro de gravedad de los riesgos tecnológicos y, como se ha visto, como consecuencia de la hiperconectividad, cualquier daño que se manifieste sobre estos puede llegar a afectar a la estabilidad mundial (*global governance*)[216] que depende de ciertos sistemas como las infraestructuras críticas.

214 *Op. cit.*, World Economic Forum (2012), p. 24.

215 *Op. cit.*, World Economic Forum (2014), p. 41.

216 *Op. cit.*, World Economic Forum (2012), p. 24.

Gráfico 11: El lado oscuro de la conectividad



Fuente: Global Risk Report (2012)[217].

La ciberseguridad es un ejemplo de interés público aunque principalmente se desarrolla y financia por medio de organizaciones privadas y sujetos individuales, pero los beneficios que reporta se comparten con el resto del ecosistema[218]. En este sentido, cuando los usuarios y las entidades individuales implantan y desarrollan políticas y sistemas de seguridad, se beneficia: su propio sistema, el de sus clientes y proveedores, y el ciberecosistema en general.

Por ello, podemos mencionar tres niveles de interés que subyacen en el desarrollo de sistemas de ciberseguridad:

1. La protección de la integridad de los sistemas propios como reflejo del interés individual.

2. La protección de los clientes, proveedores y socios (evitando que por medio de los sistemas propios se derive un daño a estos por medio de malware, spam, robo de datos de terceros…) que responde a un interés contractual.

3. El interés colectivo de asegurar y preservar la eficiencia del mercado.

Para contribuir con este interés público, todas las partes interesadas deberían asegurar el mantenimiento de una efectiva capacidad de respuesta en caso de ciberincidente mediante diferentes medios, como el establecimiento de programas de intercambio de información y respuesta como CERT (Computer Emergency Readiness Team), y el desarrollo de programas de formación que mejoren las capacidades de los trabajadores en este ámbito. En particular,

217 Figure 17: The Dark Side of Connectivity Constellation, *op. cit.*, World Economic Forum (2012), p. 25.

218 *Op. cit.*, World Economic Forum (2012), p. 27.

el constante desarrollo de los *cyber attacks* requiere de unos medios de prevención en continua mejora y reciclaje, cuyo mantenimiento exige que se realicen inversiones en recursos tecnológicos, investigación y educación técnica que garantice la existencia de capital humano con amplios conocimientos en el ámbito de los ciberriesgos[219].

En el ciberecosistema la diferencia entre los intereses públicos y privados puede ser difusa[220], ya que como consecuencia de la hiperconectividad los daños que sufre un sistema concreto pueden llegar a afectar a un grupo muy amplio. Además, en algunos casos como en los ataques DDoS es necesaria la colaboración inconsciente de sistemas infectados (*boths*) para causar un determinado daño a un sistema. Así, podemos considerar que estos intereses forman parte del ámbito de la ciberseguridad nacional.

La seguridad nacional se ha definido tradicionalmente como un elemento garantista de la identidad e integridad de las naciones. No obstante, este concepto se ha ido generalizando en la medida en que se ha aplicado a otros riesgos que afectan a la sociedad civil y aspectos concretos de la integridad nacional[221]. Por ello, se podrá extender este ámbito al ciberespacio en la medida en que consideramos que se trata de un conjunto independiente de medios y relaciones que produce numerosos efectos sobre el mundo físico.

En definitiva, los sujetos pasivos de la falta de seguridad en el ciberespacio son todos los agentes que de una u otra manera forman parte del ecosistema digital (sociedad civil, individuos, empresas, intereses económicos, estados…) en cada una de sus relaciones (familiar, laboral, amistad, ocio, compras…). La estrategia de ciberseguridad nacional aprobada por España en diciembre de 2013 expone una lista de posibles riesgos y amenazas, así como agentes y factores responsables de los mismos, entre los que incluye causas deliberadas y naturales. En el informe presentado en 2014 el Consejo de Seguridad Nacional hace especial mención al ciberespionaje, ciberterrorismo y ciberdelincuencia como especiales riesgos para la seguridad nacional[222].

219 «Risk and Responsibility in a Hyperconnected World», World Economic Forum (31 de mayo de 2012), http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf

220 *Op. cit.*, World Economic Forum (2012), p. 27.

221 «Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio», *Cuadernos de Estrategia*, 149, Ministerio de Defensa (diciembre de 2010), pp. 50-51, https://www.cni.es/comun/recursos/descargas/Cuaderno_IEEE_149_Ciberseguridad.pdf

222 Luis de la Corte Ibáñez, José María Blanco Navarro, LID Editorial Empresarial (noviembre de 2014).

4.1.1. Conceptos relacionados con el interés nacional

La diferencia entre los conceptos que se desarrollan en este apartado es esencial y requiere el análisis de la aplicación de unas u otras circunstancias y el alcance de las mismas.

En el sentido al que vamos a hacer referencia en el presente apartado, los ciberataques se pueden definir como aquellas acciones que realiza una persona o grupo de personas intencionadamente mediante un sistema informático, para tratar de socavar o interrumpir el funcionamiento de otros sistemas informáticos con un objetivo político o de interés nacional. De esta forma, deberemos entender el interés nacional como la defensa de los intereses políticos, económicos, culturales y sociales[223], por lo que cualquier ataque que afecte al interés común formaría parte de este concepto (de tal manera los intereses globales se incorporan al concepto amplio del interés general[224]).

La extensión del concepto de interés general a la que nos hemos referido permite calificar como ciberataque a aquel que afecta a gran parte de los intereses de la sociedad ya sean públicos o privados; y esto hace que aumenten los casos que pueden encontrarse englobados en este ámbito que en algunas situaciones, además, constituyen cibercrímenes.

En general se considera que un cibercrimen es la realización de cualquier acción penada por la ley por medio de un sistema informático que facilita su comisión[225], cuya principal diferencia es que carecen de un interés político o no afectan a un interés nacional[226]. No obstante, tanto los ciberataques como los cibercrímenes suelen ser cometidos por personas o grupos individuales y no por países —cuyos ataques forman parte de categorías como *cyber warfare* o ciberterrorismo—, ya sean emprendedores individuales o auténticas compañías fantasma[227].

En ciertos casos un ciberataque puede ser considerado como cibercrimen —siempre que este tenga un objetivo político o de interés nacional e in-

223 Rubén Herrero de Castro, *Evolución del concepto de interés nacional*, Centro Superior de Estudios de Defensa Nacional, Monografías del CESEDEN (abril de 2010), p. 19, http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/115_EVOLUCION_DEL_CONCEPTO_DE_INTERES_NACIONAL.pdf

224 J. S. Jr. Nye, «The Paradox of American Power. Why the World's Only Superpower can't go it Alone». Cap. 5, *Redefining the Nacional Interest*, Oxford University Press, 2002.

225 Sarah Gordon y Richard Ford, «On the Definition and Classification of Cybercrime», *J. Computer Virology*, nº 1 (2006), p. 14.

226 Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel, *op. cit.*, 2012, p. 19.

227 Global Risks Report, World Economic Forum (2011), p. 36.

frinja alguna norma de carácter penal aplicable conforme a las reglas de competencia y jurisdicción—, por ejemplo, cuando una persona o grupo de personas hackean los servicios informáticos del U.S. Government's State Department —o de cualquier otro estado— bloqueando o impidiendo su funcionamiento[228].

El Gobierno de EE. UU. a través de The Congressional Research Service define la *cyber warfare* como aquella guerra que se libra en el ciberespacio que comprende actos de ataque y defensa contra la información y sistemas informáticos[229]. Y, por tanto, se trata del empleo de las operaciones de la red de ordenadores (CNO) con la intención de negar a sus adversarios el uso eficaz de sus ordenadores, sistemas de información y redes, garantizando al mismo tiempo el uso efectivo de nuestros propios ordenadores, sistemas de información y redes.

Estas operaciones incluyen la red de ordenadores Ataque (CNA), la red de ordenadores de Exploración (CNE) y la red de ordenadores de Defensa (CND)[230], y en ciertos casos pueden formar parte de una guerra psicológica o mediática que finalmente busque crear una reacción de guerra convencional[231]. Y, en todo caso, se caracteriza por tratarse de acciones ejercitadas por un país para penetrar en los sistemas informáticos de otro con el propósito de ocasionar un daño[232].

La relación de estas tres figuras es evidente y entre ellas podemos establecer unos puntos de conexión o circunstancias comunes; así, los ciberataques pueden ser producidos por sujetos individuales o por Estados, y se tratan de conductas intencionales cuyos objetivos tienen un carácter político o afectan a la seguridad nacional de otro Estado. Además, algunos ciberataques constituyen también un cibercrimen, pero no todos los cibercrímenes son ciberataques. Sin embargo, la *cyber warfare* siempre constituye un ciberataque, pero no todos los ciberataques son actos de ciberguerra; solo aquellos cuyos efectos equivalen a actos propios de un conflicto armado u ocurren en el contexto de un conflicto armado[233].

228 Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel, *op. cit.*, 2012, p. 21.

229 Steven A. Hildreth, «Cyberwarfare», *Congressional Research Service*, 16 (19 de junio de 2001).

230 Jeffrey Carr, Inside Cyber Warfare 176 (2010).

231 *Op. cit.*, World Economic Forum (2011), p. 36.

232 Richard A. Clarke y Robert K. Knake, *op. cit.*, 2010.

233 Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel, *op. cit.*, 2012, p. 21.

En este sentido, para que un ciberataque tenga el carácter bélico al que nos estamos refiriendo consideramos que será necesario que tenga los atributos a los que se refiere la Resolución 3314 de las Naciones Unidas sobre definición de la agresión, que fue aprobada a la luz del artículo 39 de la Carta de Naciones Unidas. Y, en particular, que tenga relación con el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de otro Estado, o en cualquier otra forma incompatible con la Carta de las Naciones Unidas.

Aunque en el caso de los ciberataques a priori parece difícil considerar como armas a las herramientas (sistemas tecnológicos) por medio de las que se perpetran, lo cierto es que, por lo general, se tratan de herramientas de software diseñadas específicamente para causar un daño concreto, y que un gran número de países (EE. UU., Israel, China, Irán, Corea del Norte…) han incorporado a sus Fuerzas Armadas equipos de expertos en *cyber warfare*.

El ciberterrorismo es el uso de sistemas informáticos para atacar infraestructuras críticas o sistemas del gobierno, o para coaccionar o intimidar a los organismos públicos y población civil[234]. Por tanto, se trata de un concepto claramente diferenciado de los actos de *cyber warfare*, aunque siempre constituye un ciberataque con carácter criminal conforme a la definición de terrorismo del diccionario de la RAE, en la que se establece que es una «actuación criminal de bandas organizadas, que, reiteradamente y por lo común de modo indiscriminado, pretende crear alarma social con fines políticos».

Además, existen otros conceptos que deberemos tener en cuenta, como el ciberespionaje o la ciberexplotación, que no pueden ser calificados propiamente como ciberataques porque ninguno de los dos conceptos requiere una alteración en los sistemas informáticos que afecte a sus funciones y adecuado funcionamiento[235]. En relación con la ciberexplotación, esta se caracteriza por la publicación de información personal y privada sin el consentimiento de aquellos a los que les afecte[236]. No obstante, tales circunstancias no obstan para que pueda ser considerado como un cibercrimen.

Como se ha dicho, el ciberataque requiere que el causante socave o interrumpa el funcionamiento de los sistemas que sufren el ataque; de tal manera que el

234 James Lewis, United States. *Center for Strategic and International Studies. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Washington, D.C., 2002.

235 Seymour M. Hersh, «The Online Threat: Should We Be Worried About a Cyber War?», *The New Yorker* (1 de noviembre de 2010), http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh?

236 Cyber Explotation-Law Enforcement FAQs, State of California Department of Justice, Office of the Attorney General, p. 1, https://oag.ca.gov/sites/all/files/agweb/pdfs/ce/cyber-exploitation-law-enforcement-faqs.pdf

atacante realiza más que una simple observación pasiva como en el caso del ciberespionaje —incluso cuando la información se obtiene de forma clandestina y el causante utiliza medios destinados directamente a conseguir tal acceso—[237].

En todo caso, los conceptos de cyber attack, cyber crime, cyber warfire y ciberterrorismo que hemos abordado hacen referencia a daños o amenazas que se desarrollan a través del ciberespacio, y que son consecuencia de una acción voluntaria cuyo principal objetivo es ocasionar un daño o beneficiarse de una acción no consentida por quien lo sufre.

4.1.2. Sistemas y estrategias de ciberseguridad nacional

La principal particularidad de los nuevos riesgos son los denominados riesgos globales que por su naturaleza no respetan las fronteras de los Estados (KLAUS SCHWAB, 2013[238]) entre los que sin duda se encuentran los riesgos tecnológicos, y que en la mayoría de casos producen efectos que por su complejidad van más allá del ámbito de gestión de un sujeto o empresa (es decir, son exógenos). Tal conclusión debe servir tanto para mejorar la estrategia, la planificación y la toma de decisiones, como para aumentar el interés del sector público y privado (LEE HOWELL, 2012[239]). En este sentido, debemos advertir sobre la importancia de los riesgos sistémicos que se pueden definir como aquel riesgo de que se produzca una avería que afecte a todo el sistema de las IT, y no solo a un componente o parte individual[240].

Existen diversas estrategias y protocolos que forman parte de la ciberseguridad nacional que principalmente ponen de manifiesto la militarización de este ámbito. El informe Global Risks Report publicado en 2014 mantenía que 30 países del mundo ya habían desarrollado doctrina y estrategias de ciberguerra aplicadas a la seguridad nacional, y de ellos 12 contaban con organizaciones dedicadas exclusivamente a velar por la ciberseguridad nacional[241].

En diciembre de 2013 el departamento de Seguridad Nacional publicó la *Estrategia de Ciberseguridad Nacional*[242], que fue redactado por iniciativa del

237 Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel, *op. cit.*, 2012, p. 14.

238 *Op. cit.*, World Economic Forum (2013), p. 8.

239 *Op. cit.*, World Economic Forum (2013), p. 9.

240 Note 1, G. G. Kaufman y K. E. Scott, «What Is Systemic Risk, and Do Bank Regulators Retard or Contribute to It?», *Independent Review*, 7 (2003), pp. 371-391.

241 Global Risks Report, World Economic Forum (2014), p. 39.

242 *Estrategia de Ciberseguridad Nacional*, Seguridad Nacional (diciembre de 2013), pp. 16-28, http://www.dsn.gob.es/es/file/146/download?token=K1839vHG

Consejo de Seguridad Nacional. Con este documento se dotó a España de un plan estratégico que recoge los elementos necesarios para proteger su ciberespacio. Y se creó una nueva estructura dirigida a mejorar la coordinación de la ciberseguridad a nivel nacional y apoyar la toma de decisiones del más alto nivel en esta materia: el Consejo Nacional de Ciberseguridad, el Comité especializado en la gestión de crisis y el Comité de Situación (junto con estos órganos debemos mencionar la importancia de la labor técnica del Centro Criptológico Nacional, que forma parte del CNI y fue regulado por el Real Decreto 421/2004, de 12 de marzo)[243]. La creación de este órgano forma parte del principio de liderazgo nacional y coordinación de esfuerzos sobre el que se basa el plan estratégico, y junto con este se establecen:

- **La responsabilidad compartida:** según el cual se considera a todos los agentes públicos y privados con responsabilidad en esta materia, por lo que incluye también a los propios ciudadanos que han de sentirse implicados con la ciberseguridad. En efecto, tal circunstancia participa del concepto difuso de interés público y privado de las circunstancias del ecosistema digital al que hemos hecho referencia. Y para ello, se hace precisa una intensa coordinación de los diferentes organismos de las Administraciones públicas y una adecuada cooperación público-privada capaz de compatibilizar iniciativas y propiciar el intercambio de información.

- **Proporcionalidad, racionalidad y eficacia:** conforme a la que se establece que es necesario gestionar los riesgos derivados del uso de la tecnología de forma dinámica, equilibrando oportunidades y amenazas, asegurando la proporcionalidad en las medidas de protección adoptadas.

- **Cooperación internacional:** el carácter transfronterizo de las amenazas hace que sea esencial promover la cooperación global, ya que muchas de las posibles medidas solo resultarán eficaces si se adoptan internacionalmente con la adecuada cooperación y coordinación entre los distintos países.

Y todo ello se establece para lograr que España haga un uso seguro de los sistemas de información y telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques. Con ese fin se crean cinco objetivos que giran en torno a contribuir a mejorar la ciberseguridad en el ámbito internacional como un interés público de carácter supranacional, que son:

1. Garantizar que los sistemas de información y telecomunicaciones que utilizan las Administraciones públicas poseen el adecuado nivel de ciberseguridad y resiliencia.

243 Mar López Gil, «Estrategia de Ciberseguridad Nacional», *astic*, boletic 73 (mayo de 2015), p. 1, http://www.astic.es/sites/default/files/articulosboletic/monografico2marialopezgil.pdf

2. Impulsar la seguridad y resiliencia de los sistemas de información y telecomunicaciones usados por el sector empresarial, en general, y los operadores de infraestructuras críticas, en particular.

3. Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio.

4. Sensibilizar a los ciudadanos, profesionales, empresas y Administraciones públicas españolas de los riesgos derivados del ciberespacio.

5. Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesite España para sustentar todos los objetivos de ciberseguridad.

El Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptográfico Nacional establece un mecanismo de actuación para los casos de amenazas contra la seguridad nacional al que dedica su Capítulo VII a la capacidad de respuesta a incidentes de seguridad. Así, en su artículo 36, el real decreto señala que el CCN «articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (Centro Criptológico Nacional-Computer Emergency Reaction Team), que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada Administración pública y de la función de coordinación a nivel nacional e internacional del CCN».

En relación con las infraestructuras críticas se creó en 2007 el Centro Nacional para la Protección de las Infraestructuras Críticas con el objetivo de coordinar la información y la normativa aplicable a este ámbito. Junto con esta institución se han creado numerosos planes y sistemas, así en 2008 el CCN-CERT empezó a aplicar un sistema de alerta temprana en la red SARA para detectar de manera proactiva las anomalías y ataques del tráfico que circula entre diferentes órganos públicos. Y en el ámbito privado, el Instituto Nacional de Tecnologías de la Comunicación es responsable de gestionar a través de su CERT la defensa del ciberespacio relacionado con las pymes españolas y los ciudadanos en su ámbito doméstico[244].

4.1.3. Legislación aplicable a la ciberseguridad nacional

En el ámbito de la defensa, la Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional menciona los conceptos de seguridad en su exposición de motivos: «El escenario estratégico ha visto desaparecer la política de bloques

244 «Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio», *Cuadernos de Estrategia*, nº 149, Ministerio de defensa (diciembre de 2010), pp. 62 y 63, https://www.cni.es/comun /recursos/descargas/Cuaderno_IEEE_149_Ciberseguridad.pdf

que protagonizó la guerra fría y emerger la globalización y un nuevo marco en las relaciones internacionales. Al mismo tiempo, junto a los riesgos y amenazas tradicionales para la paz, la estabilidad y la seguridad, surgen otros como el terrorismo transnacional con disposición y capacidad de infligir daño indiscriminadamente». La ley define aspectos como: las misiones de las Fuerzas Armadas, la contribución a la defensa, la preparación de recursos para contribuir a la defensa como son la Guardia Civil, el Centro Nacional de Inteligencia y el Cuerpo Nacional de Policía. A su vez, la Directiva de Defensa Nacional 1/2008, y ya anteriormente la de 2004, hace referencia a «un sistema de seguridad y defensa español, que debe enmarcarse dentro una Estrategia de Seguridad Nacional».

El Libro Blanco de la Defensa publicado en el año 2000 definía en su capítulo I («El escenario estratégico») el «panorama de riesgos» en cuanto al que menciona la globalización del escenario estratégico: «Los prodigiosos avances registrados en los campos de las comunicaciones y de los sistemas de información, los flujos de capitales e inversiones y las relaciones comerciales de extensión mundial han favorecido la integración de los mercados financieros y estimulado la circulación de ideas, personas y bienes. El mundo se ha hecho más pequeño y el proceso de globalización parece irreversible». Y en la Revisión Estratégica de la Defensa publicada en 2003, en su Planteamiento General, establece los intereses nacionales y riesgos para la seguridad. Entre los que menciona los ciberataques al considerar que:

> *«La economía mundial, fuertemente globalizada, depende del intercambio amplio de información, cuya interrupción provocaría problemas comparables a los ocasionados por la alteración del flujo de los recursos básicos.*
>
> *La vulnerabilidad estratégica que supone este tipo de amenazas comprende especialmente dos campos. Por un lado, los ataques contra los sistemas que regulan infraestructuras básicas para el funcionamiento de un país —como el sabotaje de los servicios públicos, la paralización de la red de transporte ferroviario o la interrupción de la energía eléctrica a una gran ciudad— suponen un serio quebranto para la normalidad y la seguridad de una sociedad avanzada.*
>
> *En consecuencia, todas las infraestructuras básicas deben dotarse de elementos de protección suficientes para poder neutralizar este tipo de agresiones cuando su funcionamiento depende de complejos sistemas informáticos y de comunicaciones.*
>
> *Por otro lado, la penetración en la red de comunicación, mando y control de las Fuerzas Armadas, en el sistema nacional de gestión de crisis o en las bases de datos de los servicios de inteligencia puede suponer*

una amenaza directa a la seguridad nacional. Por tanto, las Fuerzas Armadas deben dotarse de las capacidades necesarias para impedir cualquier tipo de agresión cibernética que pueda amenazar la seguridad nacional»[245].

En el ámbito de la Unión Europea durante los últimos años se han publicado diversas normas y estrategias enfocadas a paliar los efectos de los ciberataques, entre las que se puede citar la COM (2001) 209 «Seguridad de las redes y de la información. Propuesta para una política europea»; en el año 2006 COM (2006) 251 «Estrategia para una sociedad de información segura»; de 2009, una Decisión del Consejo 2009/C 321.01 «De un enfoque europeo común sobre la seguridad de la información y de las redes»; de 2010, COM (2010) 245 «Una agenda digital para Europa».

Durante años la Unión Europea ha fijado como objetivo estratégico la protección de infraestructuras críticas según se puso de manifiesto en la conferencia de ministros en Tallín (2009)[246]; y siguiendo este objetivo se ha desarrollado una amplia regulación entre cuyas principales normas destaca el «Programa Europeo de Protección de Infraestructuras Críticas (EPCIP)», COM (2006) 786; la Directiva (2008) 114/UE, la Comunicación y el Plan de Acción COM (2009) 149; y en 2011, la Comunicación «Resultados y siguientes pasos. El camino para la seguridad global de la red» COM (2011) 163.

En cuanto a las condiciones particulares del tráfico digital se establecen una serie de elementos específicos en el Reglamento 611/2013 de junio de 2013[247] como la obligación de notificación de los casos de violación de datos personales dirigido a las redes de comunicaciones electrónicas públicas. En este punto, consideramos que analizar cada uno de los documentos mencionados no parece muy útil porque los elementos que introducían se han ido recogiendo en otras decisiones y documentos más recientes que están todavía por mencionar —la Estrategia de Ciberseguridad de la Unión Europea y la Directiva NIS—.

---

245 «Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio», *Cuadernos de Estrategia*, nº 149, Ministerio de Defensa (diciembre de 2010), pp. 59 y 60, https://www.cni.es/comun/recursos/descargas/Cuaderno_IEEE_149_Ciberseguridad.pdf

246 EU ministerial conference in Estonia initialized «Tallinn process» to secure critical information infrastructure, Republic of Estonia Ministerio of Economic Affairs and Comunications (29 de abril de 2009), https://www.mkm.ee/en/news/eu-ministerial-conference-estonia-initialized-tallinn-process-securecritical-information

247 Reglamento (UE) 611/2013 de la Comisión de 24 de junio de 2013 relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas http://eur-ex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:ES:PDF

Finalmente, el 6 de julio de 2016 se aprobó la Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, con el objetivo de mejorar el funcionamiento del mercado interior mediante los siguientes medios:

> *«a) establece obligaciones para todos los Estados miembros de adoptar una estrategia nacional de seguridad de las redes y sistemas de información;*
>
> *b) crea un grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos;*
>
> *c) crea una red de equipos de respuesta a incidentes de seguridad informática (en lo sucesivo, «red de CSIRT», por sus siglas en inglés de «computer security incident response teams»), con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz;*
>
> *d) establece requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales;*
>
> *e) establece obligaciones para que los Estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y CSIRT con funciones relacionadas con la seguridad de las redes y sistemas de información».*

Desde un punto de vista práctico, en 2004 se creó la Agencia Europea para la Seguridad de las Redes y de la Información (ENISA) por el Reglamento 460/2004, cuyas competencias e importancia experimentaron en 2010 un notable incremento bajo la COM (2010) 521[248]—con efectos en 2013 (el Reglamento 580/2011 amplió su vigencia inicial hasta septiembre de 2013)—. Los campos de actividad de ENISA en la protección y el seguimiento de la política de ciberseguridad de la UE que desarrolla en colaboración con las autoridades de seguridad de los Estados miembros son notables[249]. Al comienzo de 2013 se creó el Centro Europeo de Lucha contra la Ciberdelincuencia (EC3), que parte de la policía europea EUROPOL, como punto central para el tratamiento de los ciberataques; y un CERT de ámbito europeo, el CERT-EU, que colabora

248 COM (2010) 521 final 2010/0275 (COD), Concerning the European Network and Information Security Agency (ENISA) (30 de septiembre de 2010), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0521:FIN:EN:PDF

249 http://www.enisa.europa.eu/

con los CERT nacionales de los Estados miembros, cuya creación fue exigida desde la Agenda Digital de la Unión Europea[250].

4.2. El cibercrimen

Los individuos, empresas, organismos y Estados dependen cada vez con más de los datos y sistemas tecnológicos; así, conforme a los datos de 2012, el 35 % de la población mundial utilizaba internet[251], y a finales del año 2011, alrededor de 470 millones de smartphones se vendieron en todo el mundo y se estimaba que tal cifra se duplicase en 2015[252].

Por todo ello, se empezaron a crear los indicadores del efecto financiero de los ciberriesgos como el del Ponemon Institute[253], que ya estimó que el coste del cibercrimen para las principales empresas de EE. UU. crecería un 44 % entre los años 2010 y 2011[254].

El cibercrimen se puede clasificar como la categoría de ciberataque con mayor frecuencia, de tal modo que es la circunstancia que más afecta a los usuarios en el día a día. Por ello, el UK National Security Council lo ha calificado dentro del primer nivel de la seguridad nacional, al mismo tiempo que el terrorismo y los conflictos internacionales[255].

Pues bien, el cibercrimen se puede definir con el estudio *The Cost of Cyber Crime* (publicado por DETICA en colaboración con Cybersecurity and Information Assurance, que forma parte del Cabinet Office) como las actividades ilegales llevadas a cabo por los delincuentes para obtener un beneficio económico, que se realizan aprovechando las vulnerabilidades en el uso de internet y otros sistemas electrónicos para acceder ilícitamente y/o información y servicios utilizados por los ciudadanos, empresas y gobiernos. Así, el mencionado objetivo económico constituye la principal diferencia entre el

250 Henning Wegener, «La ciberseguridad en la Unión Europea», ieee.es (14 de julio de 2014), pp. 4-7, http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO77bis2014_CiberseguridadProteccionInformacion_H.Wegener.pdf

251 World Telecommunication/ICT Indicators Database 2010. International Telecommunication Union, 2011, http://www.itu.int/ITU-D/ict/publications/world/world.html

252 K. Nagamine, «Worldwide Smartphone Market Expected to Grow 55 % in 2011 and Approach Shipments of One Billion in 2015», *International Data Corporation*, 2011, http://www.idc.com/getdoc.jsp?containerId=prUS22871611

253 *First Annual Cost of Cyber Crime Study*, Ponemon Institute; Second Annual Cost of Cyber Crime Study (agosto de 2011).

254 *Op. cit.*, World Economic Forum (2012), p. 26.

255 Sam Jones, «UK prime cyber attack target of Europe and Middle East», *Financial Times* (16 de octubre de 2014).

cibercrimen y otras formas de ciberataques (como el ciberterrorismo o *cyber warfare*). Y dentro del propio concepto se pueden distinguir diversas formas de delincuencia, entre las que destacan[256]:

1. **El robo de identidad,** que se lleva a cabo mediante la obtención de los datos personales para explotarlos en internet, abriendo cuentas o contratando servicios no deseados.

2. **Estafas *online*,** que se realizan mediante la obtención de contraseñas y claves de acceso por medio de diversas técnicas como *phishing*, *spear phishing*, *spoofing* o *pharming*.

3. ***Scareware:*** el engaño a los usuarios para que descarguen un software falso con apariencia familiar, pero que en realidad oculta algún tipo de virus[257].

4. **Fraude fiscal:** la utilización de herramientas online para realizar este tipo de actividades fraudulentas depende de las particularidades de cada régimen fiscal. En Reino Unido se ha dado casos como la retención de impuestos debidos o la reclamación de cantidades por atacar a los sistemas oficiales *online* utilizados por la Hacienda pública[258].

5. **Robo de negocio,** mediante el acceso a las cuentas o reservas de una organización.

6. **Extorsión,** por la que se reclama una cuantía a un particular o una organización mediante el uso de *denial of service*[259], introduciendo malware en los servidores o manipulando el website oficial.

7. **Robo de datos de clientes.**

8. **Espionaje industrial y robo de propiedad intelectual.**

---

256 *The Cost of Cyber Crime*, DETICA y the Office of Cybersecurity and Information Assurance in the Cabinet Office (enero de 2011), p. 7, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

257 «Organised gangs deceive web users into downloading malicious anti-virus software», *Get Safe Online* (15 de noviembre de 2010), https://www.helpnetsecurity.com/2010/11/16/web-users-deceived-into-downloading-malicious-anti-virus-software/

258 «Man arrested for £1m online tax fraud», *The Register* (4 de septiembre de 2009), http://www.theregister.co.uk/2009/09/04/pceu_hmrc/

259 Kelly O'Connell, «Online Casinos Will Experience Cyber-Extortion During SuperBowl Betting», *Internet Business Law* (28 de enero de 2008), http://www.ibls.com/internet_law_news_portal_view.aspx?id=1967&s=latestnews

9. **Blanqueo de capitales:** en la actualidad las organizaciones criminales utilizan sistemas y medios *online* para ocultar sus ganancias en otras actividades ilícitas[260].

4.2.1. El coste de los cibercrímenes para el desarrollo económico

El estudio publicado por McAfee en julio de 2013 con el título *The Economic Impact of Cyber Crime and Cyber Spionage* tiene por objeto advertir de los efectos y la importancia del cibercrimen. En este sentido, compara las pérdidas estimadas por efecto del cibercrimen con los efectos ocasionados por otros daños de reconocida importancia como los accidentes de circulación, la piratería, los robos, el crimen organizado y el tráfico de drogas.

Así, para concluir que el ciberriesgo produce los mismos efectos perjudiciales en la sociedad, el referenciado informe estima que los daños producidos se encuentran entre 300 billones y 1 trillón de USD, que a su vez representa del 0,4 al 1,4 % del GDP global (que representa entre el 15 y el 20 % del valor generado por internet[261]).

Este dato pone de manifiesto la importancia del cibercrimen en 2013, aunque sus efectos aún se encontraban lejos de otros negocios ilícitos como el tráfico de drogas, cuyo daño económico se estima en un 5 % del GDP mundial. Además, como punto de partida se recoge el resultado de otros estudios previos de los que se deducen diversas conclusiones[262]. Entre ellas se advierte que en 2010 se estimó, por la Asociación de Seguridad Corporativa Alemana, que las pérdidas de propiedad intelectual causaban un coste mínimo anual para las empresas del país de 24 billones de USD, la mayor parte producida por ciberespionaje[263].

Por tanto, partiendo de que el GDP de Estados Unidos es cinco veces mayor que el de Alemania, la extrapolación de este dato nos llevaría a considerar adecuada la estimación de 120 billones de USD como límite para las pérdidas de Estados Unidos. Otro de los estudios mencionados estimó en 27 billones de USD el coste de las pérdidas de propiedad intelectual para las empresas

260 «Money laundering in cyberspace», *BBC* (2 de febrero de 2001), http://news.bbc.co.uk/2/hi/business/1149984.stm

261 *The Economic Impact of Cyber Crime and Cyber Spionage*, McAfee, 2014, p. 7.

262 *Op. cit.*, McAfee, 2013, p. 7.

263 «The Dangers of Germany's Dependence on China», *Spiegel online*, http://www.spiegel.de/international/world/0,1518,713478-6,00.html

de Reino Unido[264]. Tal cuantía representa el 2 % del GDP de Reino Unido, lo que aplicado a los datos de Estados Unidos produciría unas pérdidas de 280 billones de USD. No obstante, debemos advertir que tres cuartas partes de las referenciadas cuantías se atribuyen a estimaciones basadas en diferentes métodos de predicción y no a datos reales, por lo que han sido puestos en duda[265].

No obstante, los efectos del cibercrimen ponen de manifiesto una realidad global muy heterogénea, de tal manera que si comparamos la proporción que el cibercrimen representa en el GDP de los principales países, conforme a los datos publicados en 2014 por *The Economic Impact of Cyber Crime and Cyber Spionage* (McAfee), debe advertirse que los países que sufren un mayor perjuicio son Alemania y Holanda, en los que las pérdidas representan un 1,6 y 1,5% de GDP, respectivamente, seguidos por Estados Unidos y China, cuyas pérdidas se estiman en un 0,64 y 0,63% de GDP, respectivamente.

El estudio elaborado por Ponemon Institute se centra en los ciberataques como cualquier actividad criminal realizada por medio de internet, con independencia del objeto o los efectos, entre los que menciona el robo de propiedad intelectual, la sustracción de datos bancarios, la creación y distribución de virus, la obtención de información confidencial y los daños a las infraestructuras críticas. Así, parece que el cálculo del coste real del cibercrimen es complejo, y es que no incide únicamente sobre quien sufre el daño, sino que indirectamente produce un coste residual en los mercados y la sociedad.

En este sentido, el estudio *The Economic Impact of Cyber Crime and Cyber Spionage*, McAfee (2013), diferencia entre ciberataques que afectan a la seguridad nacional y el cibercrimen que afecta a cada ciudadano de manera individual.

Los robos de identidad son los cibercrímenes que aportan mayor beneficio a los delincuentes, que pueden llegar a alcanzar en términos globales 1 billón de USD al año[266]. El estudio UNODC estima que el coste de los robos de identidad, por medio de las IT, alcanzó durante el 2008 en Estados Unidos los 780 millones de USD.

---

264 Ross Anderson, «Measuring the Cost of Cybercrime», 2012, http://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf

265 Joscha Weber, «Industrial espionage threatens German companies and Jobs», *DW.com* (29 de junio 2016), http://www.dw-world.de/dw/article/05645869,00.html; y Joseph FITanakis, «German security group sees rise in industrial, commercial spying», *Intelnews.org* (26 de mayo de 2009), http://intelnews.org/tag/berthold-stoppelkamp/

266 «Cybercrime», *UNODC*, https://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf

No obstante, resulta verdaderamente complejo conocer el número exacto de siniestros en función de las distintas pérdidas de datos, ya que no se puede disponer de las estadísticas de robo de datos bancarios. Aunque el estudio de referencia estima que este tipo de cibercrimen produce unas pérdidas, en Estados Unidos, de entre 300 y 500 millones de USD al año. En todo caso, la cuantía de estas pérdidas es muy elevada, lo que sin duda producen un efecto importante en la economía de las instituciones financieras. Aunque en gran parte de los casos se asumen dentro de unos parámetros habituales como el coste de los negocios *online*[267].

Como ya hemos adelantado en el apartado anterior, las particularidades de los daños provocados por ciberataques ocasionan un coste remanente cuyo alcance es difícil de predecir, así deberá cuantificarse teniendo en cuenta diversos extremos como el coste de detección, recuperación, investigación y gestión, además de los costes adicionales para el negocio, la pérdida de clientes y el daño moral o psicológico.

El cibercrimen afecta a todos los sectores e individuos, provocando un especial daño cuando incide en los servicios públicos, educación, sanidad y demás aspectos básicos para la sociedad, donde la sensibilidad de los datos y la intensidad del daño son mayores.

En efecto, el cibercrimen se trata de una amenaza real y directa para todos los individuos que supera los límites de las infraestructuras críticas y de los sistemas de las grandes compañías, para afectar al día a día de todos los ciudadanos; máxime si consideramos que los ciberdelincuentes pueden formar parte de nuestra misma compañía u organización. En este sentido, advierte el Ponemon Institute Research Report que los cibercrímenes que mayor daño económico produce son: en primer lugar, los DDoS; en segundo lugar, los ocasionados por el propio personal; y en tercer lugar, *los web-based attacks*. Estos tres tipos de ataques ocasionan el 49 % del coste anual del cibercrimen. Las operaciones para mitigar y evitar este tipo de ataques requieren implantar tecnología SIEM (*sintrusion prevention systems*), y aplicaciones especializadas en auditorías de seguridad y las soluciones GRC[268].

Conforme a los datos aportados por el Ponemon Institute, el coste del cibercrimen depende del tamaño de la organización afectada, y concluye que las de menor tamaño tuvieron un coste per cápita en 2015 de 1.014 libras, mientras

267 Fred Bailard, Brian Busony y Gene Lilienthal, «Call the FED Cybercrime», *FRBSF* (14 de marzo de 2013), http://www.frbsf.org/banking/audioconf/031413/Call-the-Fed-Cybercrime-3-14-13.pdf

268 *2015 Cost of Cyber Crime Study: United Kingdom*, Ponemon Institute (octubre de 2015), pp. 4 y 5.

que el coste per cápita en las de mayor tamaño fue de 232 libras; además, se estimó que el coste global del cibercrimen en Reuno Unido durante 2015 creció un 14 % respecto al año anterior, y un 64 % con relación a 2012. Las organizaciones de menor tamaño han sufrido el mayor aumento de coste al pasar de 399 libras per cápita en 2012 a 1.014 libras en 2015.

Todo ello pone de manifiesto que el principal problema no está en la sofisticación de los ataques, sino en la vulnerabilidad de los sistemas; así, las pequeñas organizaciones habitualmente sufren un mayor coste por los *web-based attacks*, *virus*, *worms* y *trojans*; mientras que las organizaciones de mayor tamaño padecen los daños con mayor coste como consecuencia de *stolen devices*, *malicious code*, *phishing & social engineering* y daños ocasionados por empleados.

Las mencionadas circunstancias son comunes a las pequeñas organizaciones y usuarios particulares, que padecen daños de menor alcance pero con mayor frecuencia. En efecto, el estudio de referencia advierte que los ataques menos sofisticados se parecen con mayor frecuencia que aquellos que requieren mayor planificación. En este sentido, afirma que todas las organizaciones encuestadas habían sufrido en 2015 virus, gusanos o troyanos, y malware el 97 %; mientras que solo el 26 % sufrieron *phising*, y el 23 % fueron atacadas por sujetos de la propia organización[269].

Así, para calcular el coste de los ciberataques se deben tener en cuenta tanto la intensidad del daño como la frecuencia. Por tanto, se concluye que el 43 % de las pérdidas debidas a ciberataques fue ocasionado por: DDoS, ataques internos y *web-based attacks*[270].

Cada ciberataque produce unos efectos radicalmente distintos con unas consecuencias diferentes. La paralización del negocio, aunque conlleve un gran coste de gestión y recuperación, no ocasiona un daño directo importante, así como los ataques mediante DDoS o la encriptación de datos personales. Se tratan, por tanto, de daños con efectos intangibles (como la pérdida de reputación o de daño moral) que generalmente se desarrollan en el ámbito personal.

El estudio de Cambridge University, *Survey of phishing estimated*, concluye, sobre la base de las estadísticas de *Gartner Report*, que en EE. UU. el coste medio del robo de identidad es de 572 USD por persona, y que el coste total

269 *Op. cit.*, Figure 8. Types of cyber attacks experienced by 39 benchmarked companies, Ponemon Institute (octubre de 2015), p. 11

270 *Op. cit.*, Figure 10. Average annualised cyber crime cost weighted by attack frequency, Ponemon Institute (octubre de 2015), p. 13.

del robo de identidad (por medio de *phishing*) en Estados Unidos es de 350 millones de USD al año. Por otra parte, en el mencionado informe *Gartner Report* se estima que la cuantía global de pérdidas anuales que ocasiona este tipo de cibercrimen es de 2 billones de USD[271]. No obstante, parece que menos del 1 % de las víctimas de *phishing* sufren una pérdida económica directa[272].

En todo caso, las pérdidas ocasionadas por los ciberataques se pueden diferenciar conforme a los siguientes niveles:

- **El daño directo** ocasionado por: el robo y pérdida de datos sensibles y de propiedad intelectual o industrial; los daños en los sistemas de infraestructura tecnológica; y la manipulación de datos.

- *El coste de recuperación*, dentro del que podemos diferenciar: el coste directo de las actuaciones necesarias para detectar y reparra el daño; el coste indirecto del tiempo y esfuerzo que supone para la estructura de una organización; y el coste de oportunidad, cuya principal causa es la paralización del negocio.

Además, **los ciberataques producen daños de carácter psicológico que afectan a la imagen corporativa y dañan la confianza que los clientes y la sociedad ponen en las IT**. En este nivel, el cibercrimen es la principal amenaza para el dasarrollo social y económico relacionado con las nuevas tecnologías. Como mantiene *The Economic Impact of Cyber Crime and Cyber Spionage*, McAfee (2013), que afirma que el cibercrimen produce un grave coste social y, en especial, ciertos supuestos como las webs de pornografía infantil o las utilizadas por los grupos terroristas para hacer apología de sus crímenes[273].

El Congressional Budget Office estima que el coste de aprobar e implementar una ley para la lucha contra la pornografía infantil en internet es de 30 millones de USD al año[274]. Y a ello se debe sumar el coste humano que estos crímenes producen, que en la mayoría de supuestos el daño tiene efectos puramente psicológicos. En estos casos, los costes intangibles están representados por el daño moral de las víctimas y sus familiares, y el daño indirecto que esto puede suponer para la imagen de cualquier proveedor tecnológico, utilizado como medio o herramienta del cibercrimen.

---

271 *An Empirical Analysis of the Current State of Phishing Attack and Defence*; http://www.cl.cam.ac.uk/~rnc1/weis07-phishing.pdf, p. 16.

272 Dancho Danchev, «How many people fall victim to phishing attacks?» (4 de diciembre de 2009), http://www.zdnet.com/blog/security/how-many-people-fall-victim-tophishing-attacks/5084

273 *Op. cit.*, McAfee, 2013.

274 *Child Protection Act of 2012*, Congressional Budget Office Cost Estimate (30 de julio de 2012), http://www.cbo.gov/sites/default/files/cbofiles/attachments/hr6063.pdf

Las empresas y organizaciones no tienen capacidad de padecer los daños morales derivados de un ciberataque. No obstante, los sufren de manera indirecta cuando los padecen las personas que las forman (ya sean empleados, socios o clientes).

Los esfuerzos para estimar el coste de los daños intangibles (en comparación con la facilidad de valorar los daños puramente materiales) ponen de manifiesto la dificultad de determinar el verdadero coste del cibercrimen. En este sentido, es importante advertir que el daño moral producido por un delito es muy amplio, ya que puede variar desde el producido por los asesinatos hasta los pequeños hurtos. Así, el coste de los cibercrímenes habituales como el fraude, la falsificación o la malversación de fondos son bajos o difíciles de estimar[275].

En todo caso, la existencia del coste social de los ciberataques se puede advertir al comparar el cibercrimen con cualquier otra actividad criminal. De tal manera, uno de los principales efectos será la pérdida de reputación, que afecta tanto a los sujetos que lo padecen directamente, como a la reputación implícita de un sector o industria, y el aumento del coste en desarrollo de sistemas de seguridad. Además, el cibercrimen produce un alto coste de oportunidad que está formado por la pérdida de clientes y oportunidades de desarrollo de nuevos negocios. El rápido desarrollo de las IT ha venido motivado por la confianza de los usuarios de internet, pero, como consecuencia de los cibercrímenes, han aumentado las exigencias de seguridad de los usuarios, lo que ha incrementado el coste de la seguridad.

En este sentido, se debe advertir que el coste económico más importante del cibercrimen es el deterioro del desarrollo de las IT y la pérdida de competitividad e innovación en el mercado. Especialmente, el ciberespionaje es la forma de ciberataque con mayor relevancia entre estos daños, ya que puede producir un coste intangible muy alto. El estudio *The Economic Impact of Cyber Crime and Cyber Spionage* mantiene que los daños ocasionados por la pérdida de propiedad intelectual producen un incremento del coste de producción. Y es que en el supuesto concreto puede suponer tener que reescribir el software de un avión militar después de haber sufrido este tipo de ataques[276].

El departamento de ciberseguridad y seguridad de la información del Cabinet Office de Reino Unido afirma que, en el mejor escenario, el coste anual del cibercrimen para la economía de Reino Unido representa 21 billones de libras (este daño se produce principalmente por el robo de propiedad intelectual,

275 William Alan Bartley, «Valuation of Specific Crime Rates: Final Report», http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2835847/#R12 y https://www.ncjrs.gov/pdffiles1/pr/188070.pdf

276 *The Economic Impact of Cyber Crime and Cyber Spionage*, McAfee, 2014, p. 6.

cuyo daño se valora en 9,2 billones)[277]. Por otra parte, el US Department of Commerce estima que el coste del robo de propiedad intelectual para las compañías estadounidenses es de 200 a 250 billones de USD anuales[278]. Y aunque no se traten de datos con carácter general, los estudios a los que estamos haciendo referencia[279] muestran que el escaso riesgo que ofrecen las IT facilita la comisión de estos crímenes por medio del ciberespionaje.

El análisis publicado por la World Intellectual Property Organization (WIPO)[280] en 2011 consideraba que el mercado de la propiedad intelectual producía 180 billones de USD anuales en comisiones y licencias. Por ello, advertía McAfee en 2014[281] sobre la relevancia que tienen las pérdidas por robo de propiedad intelectual en el coste total del cibercrimen.

Aunque los daños se concentran en ciertos sectores, como los mercados financieros, la industria química, aeroespacial, energética y los productores de IT, el robo de propiedad intelectual por medio del ciberespionaje es una amenaza para el sistema económico. Ya que se estima que produce la pérdida de 200.000 puestos de trabajo al año en Estados Unidos (en relación con el coste de oportunidad de las exportaciones pérdidas)[282], y en Europa (donde se crean 16,7 puestos de trabajo por cada millón de euros en exportaciones[283]), tales pérdidas alcanzarían los 150.000 puestos de trabajo al año[284].

Uno de los sectores más afectados por el cibercrimen ha sido la banca y los mercados financieros, que sufren las técnicas más avanzadas de robo de

277 *The Cost of Cyber Crime*, DETICA y The Office of Cybersecurity and Information Assurance in the Cabinet Office, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

278 «Stolen Intellectual Property Harms American Businesses Says Acting Deputy Secretary Blank», The Commerce Blog, U.S. Department of Commerce (29 de noviembre de 2011), http://www.commerce.gov/blog/2011/11/29/stolen-intellectual-property-harms-american-businessessays-acting-deputy-secretary-

279 *The Cost of Cyber Crime*, *op. cit.*, p. 20.

280 *World Intellectual Property Report 2011*, WIPO Economics & Statistics Series (2011), http://www.wipo.int/edocs/pubdocs/en/intproperty/944/wipo_pub_944_2011.pdf

281 *The Economic Impact of Cyber Crime and Cyber Spionage*, McAfee, 2014, p. 13.

282 International Trade Administration, «Jobs Supported by Exports: An Update», 12 de marzo de 2012, http://www.trade.gov/mas/ian/build/groups/public/@tg_ian/documents/webcontent/tg_ian_003639.pdf

283 N. Sousa, J. M. Rueda-Cantuche, I. Arto y V. Andreoni, «Extra: EU Exports and Employment», Chief Economists Note, European Commission, Trade, Issue 2 (2012), http://trade.ec.europa.eu/doclib/docs/2012/may/tradoc_149511.%202_24.05.2012.pdf. Ver también: «Unemployment Statistics», European Commission: Euro Stat, http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Unemployment_statistics; epp.eurostat.ec.europa.eu/cache/.../3-31012014-AP-EN.PDF

284 *The Economic Impact of Cyber Crime and Cyber Spionage*, McAfee, 2014, p. 3.

información. Al mismo tiempo, es el sector que aporta mayor rentabilidad para las organizaciones criminales por tratarse de datos de gran valor. De tal forma, el informe *The Economic Impact of Cyber Crime and Cyber Spionage* mantiene que estos crímenes son generalmente perpetrados por bandas organizadas que tienen la capacidad de vulnerar cualquier sistema de ciberseguridad a nivel institucional[285].

Sin lugar a dudas, los ataques contra el sector bancario generan una gran alarma social, por lo que el coste de oportunidad que causa para el desarrollo de las IT y del sistema económico es muy elevado. Además, ya existen ejemplos de ataques con efectos globales causados por la manipulación de los mercados, mediante el uso de sistemas como el denominado «pump and dump», que requieren de la previa obtención de información privilegiada de instituciones financieras por medio de ciberataques[286].

El cibercrimen es el nuevo medio por el que las organizaciones criminales obtienen sus beneficios, por lo que podemos esperar un aumento constante de las amenazas. Y en consecuencia, se hará necesaria la mejora de las técnicas y sistemas de seguridad informática, lo que supone un aumento del coste de las IT. Tal circunstancia constituye una nueva barrera para las economías en desarrollo y un obstáculo para la estabilidad de las principales economías mundiales.

4.2.2. El coste social del cibercrimen

El coste indirecto de los ciberriesgos se materializa en la necesidad de elevar la inversión en sistemas, políticas e infraestructuras para evitar o minimizar los daños. Y especialmente en el desarrollo de sistemas de prevención, la gestión del siniestro y la detección de los daños. Todo esto se debe sumar a los costes directos reflejados en el propio daño y en la necesidad de repararlo.

El desarrollo de una gestión completa y general de los ciberriesgos —a la que nos hemos referido en los apartados anteriores— suele escontrarse por encima de las posibilidades de los usuarios individuales, por lo que son el sector más desprotegido ante los ciberataques. No obstante, los usuarios pueden reducir el impacto de la ciberdelincuencia tomando una serie de precauciones básicas para la seguridad de sus operaciones y sistemas, tales como instalar un firewall, actualizar con regularidad las aplicaciones de software y el uso de antivirus. Además, pueden contratar pólizas de seguro de ciberriesgo

285 *Op. cit.*, McAfee, 2014, p. 15.

286 «Net Losses: Estimating the Global Cost of Cybercrim», McAfee (junio de 2014), p. 16, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

(como los que cubren el impacto del robo de identidad)[287], que ofrecen coberturas económicas y asistenciales que facilitan la protección y recuperación de los sistemas.

Las mencionadas medidas de seguridad son necesarias, pero en muchos casos no son suficientes para evitar que los ciberataques se produzcan. Y en especial si nos referimos a los que están relacionados con el cibercrimen, por cuya consecuencia se pueden derivar los siguientes daños:

- el robo de identidad, aprovechado para la suscripción de créditos o contratos en nombre de la víctima;
- el robo de datos de las tarjetas de crédito, que permite la utilización de las mismas para comprar o hacer pagos;
- por medio del *phishing*, los delincuentes engañan a las víctimas para obtener contraseñas, números PIN y otra información financiera sensible que pueda venderse posteriormente o ser explotada, o ser compelidos a descargar software defectuoso tras recibir y descargar un *scareware*.

La amplitud y la escala de estos cibercrímenes individuales hacen que puedan llegar a producir un efecto agregado perjudicial para la economía, además del coste indirecto provocado por la desconfianza de los consumidores y usuarios en las IT, que se materializa con la pérdida de oportunidades de desarrollo y negocio. Por ello, mantiene el estudio *The Cost of Cyber Crimen* que el crimen cibernético no es únicamente una cuestión de interés nacional, ni se limita a las infraestructuras críticas, sino que tiene unos efectos mucho más extensos[288] que implican a los negocios y usuarios individuales.

El principal impacto en los usuarios individuales procede del robo de identidad, las estafas *online* y el *scareware*. A su vez, y según la información publicada por CIFAS, el impacto de los robos de identidad se puede estimar de dos formas[289]: en función del coste medio de cada incidente o por la probabilidad de incidentes, con las que se llega a resultados similares (según

287 *Op. cit.*, DETICA y the Office of Cybersecurity and Information Assurance in the Cabinet Office (enero de 2011), p. 11

288 *Op. cit.*, DETICA y the Office of Cybersecurity and Information Assurance in the Cabinet Office (enero de 2011), p. 18.

289 *Research Findings, Identity Fraud – What About The Victim?*, CIFAS (marzo de 2006), https://www.cifas.org.uk/secure/contentPORT/uploads/documents/External-Identity%20Fraud%20-%20What%20About%20the%20Victim%20Research%20Findings.pdf

el estudio de CIFAS, las pérdidas estimadas podrían alcanzar 1,7 billones de libras al año, y conforme al estudio del IFSC[290], alcanzarían 1,2 billones de libras al año).

Conforme la información publicada por Symantec, entre los tipos de cibercrimen, el que mayor coste origina son las estafas *online*, que podrían alcanzar 1,4 billones de libras; mientras que el coste de los *scareware* y de la descarga de antivirus falsos es el menor de los causados por este tipo de crímenes[291], que se limitaría a 30 millones de libras al año, aunque ha sido considerado como un tipo de incidente en aumento. Y en términos generales, según el informe *The Cost of Cyber Crime*, el impacto del cibercrimen para los ciudadanos es de 3,1 billones de libras al año.

Además, algunos de los ataques sufridos por las empresas afectan indirectamente a los usuarios, como el robo de la información sensible de los clientes, según deduce el estudio de referencia de la información aportada por el Department for Business, Innovation and Skills[292] y por el Ponemon Institute[293]. Para este tipo de daños la característica principal es el tamaño de la empresa y el volumen de datos que maneja[294], de manera que el impacto total de la pérdida de datos se estima entre 0,96 billones de libras y 1,44 billones de libras al año (la diferencia entre estas cuantías se debe a la dificultad para estimar el coste asociado al daño reputacional)[295].

En efecto, los usuarios de internet son el eslabón más débil, pero al mismo tiempo el más atractivo para los cibercriminales. Por ello, se produce una acumulación de riesgo cuyos límites son inestimables que afecta a todo el sistema socioeconómico. Y pone de manifiesto que el coste social puede ser mayor que el coste para las empresas individuales, como advierte Lewis («The cost to society may be greater than the cost to an individual company»)[296].

---

290 *New Estimate of Cost of Identity Fraud to the UK Economy*, Identity Fraud Steering Group (IFSC), 2008.

291 *Report on Rogue Security Software*, Symantec, 2009.

292 *Information Security Breaches Survey 2004 Technical Report*, Department of Trade and Industry, 2004.

293 *Cost of UK data breaches 2010*, Ponemon Institute (julio de 2010).

294 The definitions of company sizes are consistent with those used in the BERR 2008 Information Breach Survey.

295 *Op. cit.*, DETICA y the Office of Cybersecurity and Information Assurance in the Cabinet Office (enero de 2011), p. 20.

296 «Annual U.S. Cybercrime Costs Estimated at $100 Billion», *The Wall Street Journal* (22 de julio de 2013), http://online.wsj.com/articles/SB10001424127887324328904578621880966242990

4.3. Ciberterrorismo

4.3.1. Concepto

El ciberterrorismo se puede considerar como el uso de sistemas informáticos para atacar infraestructuras críticas o sistemas pertenecientes a la Administración pública o el Gobierno. Además, puede llevarse a cabo mediante una coacción o intimidación que afecte a los organismos públicos y población civil[297]. Ya en la Convención de 1937 para la prevención y represión del terrorismo, se estableció que formaban parte del concepto de terrorismo los «actos criminales contra un Estado o cuya finalidad sea infundir terror a personas individuales, grupos de personas o al público en general»[298].

Por tanto, el principal elemento que permite calificar como ciberterrorismo un ciberataque es que este debe dar lugar a la violencia contra personas o bienes, o que tenga tal entidad que la propia amenaza del daño sea suficiente para causar temor sobre quien lo padece. Como ejemplos de este concepto podemos mencionar aquellos ataques que producen la muerte o lesiones corporales, explosiones o graves pérdidas económicas. Además, los ataques contra estructuras críticas pueden ser considerados como actos de ciberterrorismo en función de su impacto y de los efectos que este produzca[299].

A pesar de la copiosa utilización de este término, no existe una metodología de consenso que permita calificar a unos actos como «ciberterrorismo». El término fue acuñado por primera vez en la década de 1980 por Barry Collin (COLLIN, 1997)[300] y su utilización fue común en diversos estudios durante la década de 1990, entre los que destacan: «Protect yourself from the cyberterrorist»; «Insure yourself against cyberterrorism»; «Funding forthcoming to fight cyberterrorism» (HAMBLEN, 1999[301]; LUENING, 2000[302]).

---

297 James Lewis, *United States. Center for Strategic and International Studies. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Washington, D.C., 2002.

298 Convention pour la prévention et de la répression du terrorisme/Convention for the Prevention and Punishment of Terrorism (16 de noviembre de 1937), https://www.wdl.org/es/item/11579/view/1/1/

299 D. Denning, «Cyberterrorism», Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives (23 de mayo de 2000), http://www.cs.georgetown.edu/~denning/infosec/cyberter ror.html

300 B. Collin, «The Future of Cyberterrorism, Crime and Justice International» (marzo de 1997), pp. 15-18.

301 M. Hamblen, «Clinton commits $1.46B to fight cyberterrorism», http://www.cnn.com/TECH/computing/9901/26/clinton.idg, (26 de enero de 1999).

302 E. Luening, «Clinton launches plan to protect IT infrastructure», *CNET* (7 de enero de 2000).

En todo caso, para calificar los elementos que pueden definir un concepto práctico de ciberterrorismo que se ajuste a los preceptos del ordenamiento jurídico español será conveniente atender, en primer lugar, a la definición tradicional de terrorismo. Tal concepto se estudiará conforme a la amplísima recopilación de jurisprudencia del artículo «Evolución jurisprudencial en la interpretación de los diversos elementos integrantes de los principales tipos delictivos aplicados respecto del terrorismo de ETA», publicado por Gema Varona Martínez[303], y se aplicará con independencia del efecto que un ciberataque tenga en los sistemas informáticos y la relación de este con el ciberespacio.

Esta cuestión tiene una gran importancia para las conclusiones de nuestro estudio ya que, como apuntaremos, los daños producidos como consecuencia de los actos terroristas quedan excluidos en las pólizas de responsabilidad civil.

En la STS 2/1997, de 29 de noviembre, se indica que «la búsqueda de una definición con relevancia jurídico-penal ha de ser ajena a descripciones teóricas de signo fenomenológico, a categorías analógicas simples, a puras connotaciones políticas o a reduccionismos conceptuales tan abundantes en el campo especulativo»[304]. No obstante, ante la ausencia de una definición legal expresa de terrorismo debe acudirse a la descripción que el CP efectúa sobre los distintos tipos de los delitos de terrorismo, ubicados dentro de los delitos contra el orden público.

De la legislación actualmente en vigor pueden distinguirse tres elementos definidores del terrorismo según la reiterada jurisprudencia de los tribunales: su finalidad, sus medios violentos y/o su carácter organizado[305].

En cuanto a la finalidad y medios, las SSTC 199/1987, de 16 de diciembre, y 89/1993, de 12 de marzo, consideran que el terrorismo pretende instaurar el terror en la sociedad y alterar violentamente el orden constitucional democrático. En el mismo sentido, las SSTS, de 24 de octubre de 1987, de 12 de junio de 1989, de 8 de mayo de 1993 y de 14 de diciembre de 1993, se refieren a la «tendencia interna intensificada» en este tipo de delitos, que permite atender

303 Gema Varona Martínez, «Evolución jurisprudencial en la interpretación de los diversos elementos integrantes de los principales tipos delictivos aplicados respecto del terrorismo de ETA», http://www.ehu.eus/documents/1736829/2067438/05+-+Evolucion+jurisprudencial+I.pdf

304 J. L. González Cussac y A. Fernández Hernández, «Sobre el concepto jurídico penal», *Teoría y Derecho: Revista de Pensamiento Jurídico*, nº 3 (2008), p. 35; y Asúa Batarrita, «Concepto jurídico del terrorismo y elementos subjetivos», en Echano Basaldua, J. (coord.), *Estudios jurídicos en memoria de José María Lidón*, Universidad de Deusto, Bilbao, 2002, pp. 41-85.

305 M. Capita Remezal, *Análisis de la legislación*, pp. 27-28 y 37-44.

a la «actitud anímica inmediata de los sujetos», independientemente de que operen también otro tipo de motivaciones.

Además, se requiere una alteración grave de la paz pública como determinante de la finalidad terrorista (STC 59/1990, de 29 de marzo; SSTS de 25 de febrero de 1987, de 16 de octubre de 1991 y de 29 de noviembre de 1994).

Por su parte, la STS 2838/1993, de 14 de diciembre, se refiere tanto al elemento estructural como finalístico, así como a los medios violentos. Y la STS 2/1997, de 29 de noviembre, hace alusión a los mismos aspectos al definir el terrorismo como: «actividad planificada que individualmente o con la cobertura de una organización, con reiteración o aisladamente, y a través de la utilización de medios o la realización de actos destinados a crear una situación de grave inseguridad, temor social o alteración de la paz pública, tiene por finalidad subvertir total o parcialmente el orden político constituido», ya que «ninguna actividad que incluya la violencia como método de lucha política (puede resultar)… homologada para participar en la vida pública. Se garantiza así el pluralismo político y la libertad ideológica».

La STS 633/2002, de 21 de mayo, se refiere también al elemento subjetivo o finalidad perseguida con los actos cometidos violentamente, lo que en definitiva se considera incompatible con los principios constitucionales (STC 48/2003, de 12 de marzo). Tales criterios fueron recogidos por la STS 2/1998, de 29 de julio, que aumentó los elementos de juicio por los que se puede atribuir a un grupo el carácter de «banda armada»[306]. Y posteriormente fueron completados por la STS de 19 de enero de 2007, que reconoce el carácter de «organización terrorista» al advertir que cierta actividad haya sido «diseñada, coordinada, graduada y controlada por» otra organización del mismo carácter[307].

Estos planteamientos jurisprudenciales han sentado las bases fundamentales del término «organización terrorista», lo que en un futuro podrá constituir una herramienta útil para calificar los actos llevados a cabo en el ciberespacio en los que se cumplan las mencionadas características. Y en particular, la STC 199/1987, de 16 de diciembre, insistió en el elemento estructural u organizativo de la definición de terrorismo, que con matices se pueden asimilar los conceptos de banda armada, organización y grupo terrorista.

306 J. L. González Cussac y A. Fernández Hernández, «Sobre el concepto jurídico penal», *Teoría y Derecho: Revista de Pensamiento Jurídico*, nº 3 (2008), pp. 46-48.

307 Eduardo de Urbano Castrillo, «El terrorismo como forma de organización delictiva», *La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario*, nº 49 (2008), p. 14.

En todo caso, solo tiene la característica de «terrorista» la banda, organización o grupo que desarrolle una finalidad determinada:

- Provocar el terror en la sociedad;
- o alterar gravemente el orden democrático.

La STC de 12 de marzo de 1993 ya se refiere a la posibilidad del terrorismo individual, ya que lo verdaderamente distintivo del terrorismo es el propósito o el efecto de «difundir una situación de alarma o de inseguridad social, como consecuencia del carácter sistemático, reiterado, y muy frecuentemente indiscriminado, de esa actividad delictiva». En este sentido, y frente al reconocimiento del terrorismo individual, debemos destacar que fuera del artículo 577 CP solo pueden cometer los tipos delictivos recogidos de los arts. 571 a 574 CP quienes pertenezcan, actúen en servicio o colaboren con bandas armadas, organizaciones o grupos terroristas.

La STS 2/1997, de 29 de noviembre, contempló la posibilidad del terrorismo individual como actividad planificada individualmente. No obstante, el Auto del TS de 23 de septiembre de 2003 ha requerido para aplicar el art. 577 CP no solo el elemento finalístico, sino también cierta estructura y capacidad operativa de los sujetos, de manera que supongan una verdadera amenaza que ponga en peligro los bienes jurídicos protegidos.

En la STS de 7 de noviembre de 2008, por la que se juzgó a un grupo de terroristas islamistas por el intento de atentar contra la Audiencia Nacional, el Tribunal Supremo reconoció que no puede incluirse dentro de las células terroristas a los «círculos concéntricos del núcleo central». De esta forma, ha considerado que no se puede atribuir el carácter de terrorista si no se prueba la decisión o aceptación de participar en la imposición violenta de las ideas. Y en este sentido ha mantenido la sentencia que deben existir pruebas más allá de la ideología radical, sin perjuicio de que ciertos sujetos hayan llegado a «proclamar sus convicciones sin ocultar sus deseos de acabar con los infieles» o «anhelar la eliminación de líderes políticos».

Así, Reinares, en su artículo «¿Coinciden el Gobierno y los ciudadanos en qué medidas adoptar contra el terrorismo internacional?» (2006), considera que, de hecho, en la STS de 7 de noviembre de 2008 se indica que la legislación penal puede tener lagunas respecto a la complejidad del yihadismo. Ante la legislación actual, la sentencia citada no sanciona aquellas conductas exaltadas o potencialmente peligrosas que solo permiten la adopción de medidas de prevención frente a unos sujetos proclives a llevar a cabo acciones que evidencien que la idea no se ha quedado en la mente del autor, sino que ha pasado a la acción. En todo caso, la referenciada sentencia de 7 de

noviembre de 2008 sigue la anterior STS de 17 de julio de 2008 —sobre el 11M—, que confirmó la mayoría de las condenas de la Audiencia Nacional[308].

Y, finalmente, la distinción entre estas conductas y las de colaboración terrorista se funda en que las primeras tienen valor en sí mismas (STS de 25 de abril de 1997). La Audiencia Nacional ha considerado bajo el art. 574 CP diferentes modalidades de robo (SSAN 24/2003, de 13 de junio; y 54/2005, de 26 de diciembre), aunque en alguna sentencia anterior configuró las conductas bajo el art. 575 CP, al haber sido calificado de este modo por el Ministerio Fiscal (SAN 28/2000, de 20 de octubre). En el ámbito de este estudio, la colaboración terrorista guarda una especial relevancia, ya que para la utilización de ciertos ciberataques como los DDoS, y en especial para mantener el anonimato de los atacantes, estos pueden tratar de implicar de forma voluntaria o involuntaria a un gran grupo de sistemas informáticos (*bots net*).

El art. 576 CP se refiere a actos de colaboración genérica. El propósito del legislador consiste en reducir al máximo «toda forma de apoyo posible a una banda armada o terrorista» (STS de 2 de febrero de 1993). La STS de 8 de marzo de 1995 indica que el delito de colaboración recoge cualquier acto de participación que favorezca a la banda armada, a sus miembros o a sus finalidades, fuera de los supuestos recogidos por el Código Penal. De esta forma, considera que se trata de actos de complicidad, necesaria o simple, en el marco de la actividad de las bandas terroristas, y que no están sometidos «a las exigencias del principio de accesoriedad» (SSTS de 22 de abril de 2005 y de 22 de febrero de 2006), ni requieren que se pruebe «su efectivo aprovechamiento» por la actividad terrorista.

De esta forma, para reconocer que concurre el referenciado ilícito será suficiente con «poner a disposición de la banda armada determinadas aportaciones, conociendo que los medios y métodos empleados por la organización consisten en hacer uso de la violencia, […] del terror y de la muerte» (STS de 16 de febrero de 1999). Y que, en tal caso, el acusado conozca la condición terrorista de las actividades o finalidades de la banda (STS de 15 de junio de 2007), por lo que no se podrá oponer en su contra una ignorancia «deliberada» (SSTS de 5 de noviembre de 2003 y de 29 de noviembre de 1997).

En definitiva, «el delito de colaboración con banda armada incluye aquellas acciones que, realizadas voluntariamente con este fin, facilitan cualquiera de las actividades de la organización, infraestructura, comunicaciones, organización, financiación, reclutamiento, entrenamiento, transporte, propaganda, etc., y no solamente las acciones armadas» (Auto del TS 2004/5209, de 8 de

308 F. Reinares, «¿Coinciden el Gobierno y los ciudadanos en qué medidas adoptar contra el terrorismo internacional?», *Análisis del Real Instituto El Cano, ARI*, nº 34 (2006).

septiembre). Por ello, aunque los ciberataques no puedan definirse como acciones armadas, podrían llevar aparejados los elementos propios de la definición de acto terrorista a los que nos estamos refiriendo.

En este sentido, parece evidente que el ciberterrorismo (entendido conforme a las pautas y elementos a los que se ha hecho referencia) forma parte de los ilícitos penales reconocidos por los artículos 571 y siguientes del Código Penal. Y en su caso, se podrá reconocer el carácter de grupo terrorista o colaborador a aquellos ciberdelincuentes que cumplan las características mencionadas. Todo ello tiene efectos especialmente relevantes en el ámbito de la responsabilidad y la aplicación de las pólizas de seguros a los que nos referiremos.

Por otra parte, es importante distinguir entre el concepto de ciberterrorismo y el «hacktivismo», que es un término utilizado para describir el activismo político que se ejerce mediante ataques informáticos. El hacktivismo generalmente tiene como objetivo dificultar el funcionamiento habitual de los sistemas sin causar graves daños o pérdidas económicas significativas[309].

El hacktivismo se puede definir conforme a los términos que hasta aquí hemos desarrollado como un acto de vandalismo electrónico claramente diferenciado de los actos de ciberterrorismo. Así, M. G. Devost, en «Information Terrorism: Political Violence in the Information Age», ha realizado una importante contribución al discurso sobre la importancia de la diferencia terminológica en relación con el ciberterrorismo y el hacktivismo. El autor ha examinado en esta obra el potencial de ciberterrorismo intentando proporcionar un modelo para prepararse para «la guerra de información». Además, ha realizado una completa aclaración sobre las ambigüedades terminológicas de terrorismo y delincuencia en el ámbito del ciberespacio, y señalado las diferentes respuestas legislativas, policiales y de seguridad nacional que deben adoptarse. En este sentido, afirmó que etiquetar como acto de ciberterrorismo a cualquier utilización maliciosa de los sistemas informáticos solo sirve para agravar la confusión y el pánico entre los usuarios y el público en general[310].

La tecnología ofrece una serie de herramientas de gran utilidad para los movimientos sociales y ciudadanos, lo que ha incrementado el número de estas acciones y grupos de ciudadanos durante la última década (el grupo de ciberactivistas Avaaz.org ha logrado 40 millones de miembros en ocho años,

309 «What is hacktivism?», *Stanford*, https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/Hacktivism/what.html

310 M. G. Devost, B. K. Houghton y N. A. Pollard, «Information Terrorism: Political Violence in the Information Age» (1998), http://www.terrorism.com/Denning.html.

y la web Change.org tiene 80 millones de usuarios), ya que el ciberespacio parece lograr amplificar el impacto de este tipo de grupos y acciones[311].

En este sentido, se entiende el *hacking* como las actividades llevadas a cabo en línea y de forma encubierta que buscan revelar, manipular o explotar vulnerabilidades en sistemas informáticos con fines políticos o ideológicos. Los ataques más utilizados por los hacktivistas son *virtual blockades*, *e-mail attacks*, *hacking and computer break-ins*, *computer viruses y worms*[312]. Por ello, es evidente la diferencia entre los conceptos de *hacktivism* y *cyberterrorism*, ya que este último se refiere a aquellas actividades llevadas a cabo mediante el ciberespacio cuyo objetivo es causar daños graves tanto físicos como económicos[313]. En algunos casos se ha considerado que el ciberterrorismo es la forma más grave de hacktivismo, ya que para alcanzar unos objetivos similares (ideológicos y políticos) busca ocasionar el mayor daño posible[314].

4.3.2. Características del ciberterrorismo

En los escenarios tradicionales, las situaciones de terrorismo son típicamente violentas o constituyen amenazas de violencia física o psicológica de tal índole, que hacen creer a quien las padece que va a sufrir algún daño. No obstante, la violencia como un fenómeno virtual es un campo relativamente nuevo que aún no se ha estudiado en profundidad[315]. Así, los efectos de la violencia en el mundo virtual se pueden definir conforme a la implicación física de los mismos, y entre otros se considera: la aplicación de los efectos psicológicos de la tradicional violencia en el mundo real a los entornos virtuales; la modificación del comportamiento como resultado de la violencia en entornos virtuales; los traumas físicos de la violencia virtual; y el uso de la violencia virtual en los entrenamientos militares (STONE, 1993[316]; WHITEBACK, 1993[317]).

311 *Op. cit.*, World Economic Forum (2016), p. 41.

312 Gabriel Weimann, «Cyber Terrorism: How real is the threat» (13 de mayo de 2004), p. 4, https://www.usip.org/sites/default/files/sr119.pdf

313 Dorothy E. Denning, «Activism, Hacktivism, and Cyberterrorism (2000)», p. 241, https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf

314 «What is hacktivism?», *Stanford*, https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/Hacktivism/what.html

315 Sarah Gordon y Richard Ford, «Cyberterrorism?», *Symantec Security Response*, 2003, pp. 6-7, https://www.symantec.com/avcenter/reference/cyberterrorism.pdf

316 V. Stone, «Social interaction and social development in virtual environments», *Teleoperators and Virtual Environments*, vol. 2 (1993), pp. 153-161.

317 C. Whiteback, *op. cit.*, *Teleoperators and Virtual Environments*, vol. 2 (1993), pp. 147-152.

En particular, el denominado *pure cyberterrorism* implica que una acción terrorista se lleva a cabo en su totalidad dentro del ámbito cibernético. Este ámbito proporciona diversas características que permiten el desarrollo de actividades terroristas con facilidad, entre las que podemos destacar: la posibilidad de reunirse de forma completamente anónima, y la facilidad y rapidez con la que se puede organizar un grupo[318]. En estos casos, los sistemas informáticos ayudan al desempeño de acciones terroristas o complementan a las mismas, pero no implican por sí mismas un ciberataque[319] o *pure cyberterrorism*.

En agosto de 1999, el Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School in Monterrey, California, publicó un informe titulado «Cyberterror: Prospects and Implications», cuyo objetivo era articular la situación y el interés de las organizaciones terroristas frente al ciberterrorismo. Con tal propósito se evaluó la perspectiva de las organizaciones terroristas en relación con estos ataques, concluyendo que la barrera de entrada para cualquier acción que fuera más allá de la interrupción de los sistemas era bastante alta, y que las organizaciones terroristas, en general, carecían de los medios y el capital humano necesario para montar una operación significativa. En definitiva, determinaron que el ciberterrorismo era un ámbito poco explotado, aunque podía llevarse a cabo como un ataque auxiliar, y en tal caso el grupo de Monterrey define tres niveles de capacidad de ciberterror[320]:

- **Simple o no estructurada:** con capacidad para llevar a cabo los cortes básicos contra los sistemas individuales utilizando herramientas creadas por otra persona. En estos casos, la organización posee poco análisis objetivo, capacidad de mando y control.

- **Avanzado o estructuradas:** con capacidad para llevar a cabo ataques más sofisticados contra múltiples sistemas o redes, y para modificar o crear herramientas básicas de piratería. En tales supuestos, la organización posee una estructura primaria del análisis, mando y control, y capacidad de aprendizaje.

- **Complejo o coordinado:** con capacidad para unos ataques coordinados capaces de causar la interrupción en masa de sistemas informáticos, además de tener capacidad para crear herramientas de *hacking* sofisticadas con un grado avanzado de análisis, mando y control, y la capacidad de aprendizaje.

318 Sarah Gordon y Richard Ford, «Cyberterrorism?», *Symantec Security Response*, 2003, p. 8, https://www.symantec.com/avcenter/reference/cyberterrorism.pdf

319 *Op. cit.*, World Economic Forum (2011).

320 Dorothy E. Denning, «Cyberterrorism», Georgetown University (23 de mayo de 2000), p. 4, http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf

El *pure cyber terrorism* es una realidad en continuo desarrollo debido a las ventajas que presenta el ciberespacio para los grupos terroristas, ya que su implementación requiere un menor número de personas y fondos más limitados. Además, el ciberespacio permite mantener el anonimato de los atacantes con gran facilidad, y cometer los ataques desde cualquier lugar del mundo[321]. No obstante, actualmente parece que el mayor daño lo ocasionan los ciberataques cuando se utilizan de forma combinada con ataques físicos.

4.3.3. Desarrollo del ciberterrorismo

En diversas ocasiones los ciberataques han impedido el funcionamiento de los sitios web de instituciones públicas y gobiernos, medios de comunicación e instituciones financieras hasta llegar a producir conflictos diplomáticos. Tales circunstancias han dado lugar al estudio de la posibilidad de crear un centro de investigación, apoyado por la OTAN, capaz de identificar la fuente de ataques cibernéticos.

Desde el ciberconflicto mantenido entre Israel y Palestina en el año 2000 se sucedieron diversos ataques DDoS contra el ISP de Israel (Internet Service Provider) Netvision. Aunque inicialmente el ataque tuvo éxito y consiguió bloquear los sistemas de Netvision, esta institución ha conseguido resistir a los ciberataques posteriores mediante el aumento de la inversión en sistemas de seguridad.

En abril de 2007, numerosas organizaciones periodísticas asociadas con «Associated Press» informaron que los ataques cibernéticos que afectaron a la infraestructura de información crítica de Estonia fueron llevados a cabo desde servidores ubicados en Rusia, aunque posteriormente se ha demostrado que fue un ataque DDoS ejecutado desde numerosas partes del mundo. En agosto de 2008, un ataque similar se llevó a cabo contra Georgia y en octubre de 2007 un grupo radical nacionalista ruso de hackers atacó el sitio web del presidente de Ucrania, Viktor Jushenko.

Un analista de la Agencia Central de Inteligencia de EE. UU. (CIA) reveló públicamente que en enero de 2008 un grupo de hackers cerró con éxito las redes de suministro de energía en varias ciudades de Estados Unidos. En noviembre de 2008, el Departamento de Defensa de Estados Unidos (DoD), después de los numerosos ataques cibernéticos sufridos por el Pentágono, decidió prohibir el uso de dispositivos de hardware externos, como la memoria flash y los DVD en sus instalaciones. En 2008 un grupo de hackers llamado «Greek Security Team» logró vulnerar la seguridad del CERN (Centro

321 M. Cereijo, «Cuba the threat II: Cyberterrorism and Cyberwar» (16 de mayo de 2006), http://www.lanuevacuba.com/archivo/manuel-cereijo-110.htm

Europeo de Investigación Nuclear) hasta tal punto, que estuvieron cerca de tomar el control de uno de los detectores de LHC (Large Hadron Collider) del acelerador de partículas[322].

El desarrollo del ciberterrorismo parece constante como mantienen los sucesivos informes del Global Risks Report (2006[323], 2010[324] y 2011[325]), y entre los que la OTAN destaca[326]:

- El ataque a los sistemas IT del Gobierno de Israel en junio de 2009.
- El ataque al motor de búsqueda chino Baidu en junio de 2010.
- El ataque sufrido por diversos órganos del Gobierno canadiense en junio de 2011.
- En agosto del 2012 sufrieron diversos ataques las compañías energéticas Aramco y RasGas.

El 15 de julio de 2016 la US Federal Court condenó a un hacker de Kosovo por cometer un delito de terrorismo por acceder y publicar los datos personales de 1.000 empleados del Gobierno federal de EE. UU. Tal reconocimiento tiene un efecto sin precedentes en el ámbito asegurador, ya que la exclusión de acto terrorista que contienen la mayoría de las pólizas exige el reconocimiento judicial del mismo. Por ello, el precedente que sienta esta condena al atribuir a un ciberataque el carácter de acto terrorista puede permitir que este criterio se siga en casos futuros[327]. Y así se podrá llegar a activar la cobertura de los *pools* que cubren los daños derivados del terrorismo[328] (TRIA en Estados Unidos y el Consorcio de Compensación de Seguros en España).

---

322 Mitko Bogdanoski, Drage Petreski, «Cyber Terrorism-Global Security Theart», International *Scientific Defence, Security and Peace Journal*, http://eprints.ugd.edu.mk/6849/1/CYBER%20TERRORISM%E2%80%93%20GLOBAL%20SECURITY%20THREAT%20-%20Mitko%20Bogdanoski.pdf

323 *Op. cit.*, World Economic Forum (2006), p. 2.

324 *Op. cit.*, Global Risks Report (2010), p. 32.

325 *Op. cit.*, World Economic Forum (2011), p. 5.

326 «The history of cyber attacks», *NATO Review magazine*, http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm

327 «2016 Terrorism Risk Insurance Report», Marsh (julio de 2016), p. 7, https://www.marsh.com/content/dam/marsh/Documents/PDF/USen/2016%20Terrorism%20Risk%20Insurance%20Report.pdf

328 Jason Krauss, «Carefull How you Code…», Willis Towers Watson, https://www.willistowerswatson.com/api/sitecore/Article/Download?itemId=07ca0cd8-23b3-479d-96e1-3f17c23da863&lang=en-GB

4.3.4. Principales políticas internacionales contra el ciberterrorismo[329]

Durante los últimos años, y especialmente tras la Conferencia de Praga de 2002[330], la OTAN ha desarrollado de forma amplia su capacidad y sistemas orientados a la defensa en el ámbito de la *cyber warfare*. El programa de *cyber terrorism* de la OTAN comprende la creación de diversas organizaciones como: Communication and Information Systems Services Agency (NCSA), INFOSEC Techinical Center (NITC), Information Assurance Operations Centre (NIAOC), Computer Incident Response Capability (NCIRC)[331] y la Cyber Defence Management Authority (CDMA), que permite gestionar de forma conjunta los ciberataques[332].

En 2004 fue creado el Cooperative Cyber Defence Center of Excellence (CCD-CoE)[333], que se trata del órgano que promueve la cooperación, la transmisión de información, el aprendizaje y desarrollo en el ámbito de la ciberdefensa, mediante la acumulación y creación de conocimiento entre los miembros y socios de la OTAN[334].

En Estados Unidos las políticas relacionadas con el ciberterrorismo se atienden desde el Counter Terrorism Committee[335] establecido por el Security Council[336] y la International Telecommunication Union (ITU)[337], y tales políticas forman parte de la UN Global Counter-Terrorism Strategy.

329 Mitko Bogdanoski, Drage Petreski, «Cyber Terrorism-Global Security Theart», International Scientific Defence, Security and Peace Journal, http://eprints.ugd.edu.mk/6849/1/CYBER%20TERRORISM%E2%80%93%20GLOBAL%20SECURITY%20THREAT%20-%20Mitko%20Bogdanoski.pdf

330 Prague Summit Declaration Article 4(f), NATO (21 de noviembre de 2002), http://www.nato.int/docu/pr/2002/p02-127e.htm.

331 Communication and Information Systems Services Agency, NATO, http://www.ncsa.nato.int/topics/combating_cyber_terrorism.htm

332 «Defending against cyber attacks: what does this mean in practice?», NATO (31 de marzo de 2008), http:// www.nato.int/issues/cyber_defence/practice.html

333 History and way ahead, CCD-CoE, http://www.ccdcoe.org/12.html

334 Mission and Vision, CCD-CoE, http://www.ccdcoe.org/11.html

335 Counter-Terrorism Committee, UN Security Council, http://www.un.org/sc/ctc/index.html

336 «Report of the Counter-Terrorism Committee to the Security Council on the implementation of resolution 1624», UN Security Council (15 de septiembre de 2006), pp. 6, 16 y 43, http://daccess-dds.un.org/doc/UNDOC/GEN/N06/520/37/PDF/N0652037.pdf?OpenElement

337 ITU Global Cybersecurity Agenda, GCA, Framework for International Cooperation in Cybersecurity (2007), http://www.ifap.ru/library/book169.pdf

5. LA RESPONSABILIDAD CIVIL EN EL ÁMBITO DE LOS CIBERRIESGOS

Los ciberriesgos son aquellas amenazas que se desarrollan en el ámbito del ciberespacio y que pueden llegar a afectar a cualquier bien o derecho que forme parte del mismo, con independencia de que se encuentre conectado a este, o que dependa directa o indirectamente de él.

El desarrollo de las IT ha generado el aumento de las interconexiones entre sistemas hasta llegar a la hiperconectividad, lo que conlleva una fuerte dependencia de los sistemas y estructuras con el ciberespacio. Actualmente, son innumerables las situaciones en las que las circunstancias acaecidas en el ciberespacio pueden desplegar sus efectos en plano físico. Así, el IoT y las IC ponen de manifiesto la influencia que los ciberriesgos pueden llegar a tener en cualquier ámbito, desde las acciones en las que se utilizan los elementos más cotidianos, o procesos industriales (conectados por medio del IoT), hasta el mantenimiento de las estructuras más relevantes para el ámbito socioeconómico (como las estructuras energéticas o los sistemas de transporte).

Por todo ello, el elemento principal de los ciberriesgos proviene de los posibles daños por hechos indirectos conforme a los que un ciberevento ocasiona la alteración, destrucción o paralización de algún sistema conectado, que, a su vez, produce un daño a terceros cuyos bienes o derechos dependan de estos sistemas, o a los que ostenten algún derecho frente a los titulares del sistema afectado. Y, además, también podrán producirse daños directos contra las infraestructuras, los sistemas y los datos que se encuentren almacenados o formen parte de estos.

En este sentido, la posible responsabilidad derivada del desarrollo de una actividad o actuación concreta en el ciberespacio[338] es muy amplia y despliega sus efectos en diversos ámbitos del ordenamiento jurídico. Y de esta situación pueden derivarse distintos tipos de responsabilidad, entre los que destacan:

- **Responsabilidad civil,** de la que a su vez se puede distinguir la responsabilidad contractual (como en los casos en los que una paralización de

338 «La transferencia del ciberriesgo en España», *THIBER* (abril de 2016), p. 34, http://www.thiber.org/ciberseguros.pdf

la actividad impide prestar el servicio debido) y extracontractual (cuando los afectados por el ciberincidente sean terceros con los que no existe una relación obligacional previa).

- **Responsabilidad penal** de particulares y empresas, así como de los integrantes de estas, como consecuencia de su propia actuación, o la de un tercero del que sean responsables por la comisión de delitos y faltas dentro del ámbito del ciberespacio, o valiéndose de este.

- **Responsabilidad laboral** frente a los propios trabajadores de la compañía que se hayan visto afectados por el ciberincidente[339].

- **Responsabilidad administrativa** que pudiera derivarse frente a organismos regulatorios por el incumplimiento de determinadas obligaciones administrativas establecidas conforme a las normas de toda índole.

Antes de abordar el análisis de cada uno de los elementos de la responsabilidad civil que se manifiestan en el terreno de los cibereventos, debemos advertir que el ámbito cibernético puede poner de manifiesto ciertas dudas sobre la imposibilidad de aplicar alguno de los criterios de la imputación de la responsabilidad. De esta forma, las particularidades de los cibereventos hacen que se refuerce la idea del elemento culpabilístico, y de la aplicación de los elementos tradicionales de la responsabilidad civil en el ciberespacio. Y esto se estudiará conforme al análisis pormenorizado de las particularidades y circunstancias propias de las IT, que aún no han sido resueltas por la doctrina académica. No obstante, nuestro propósito es postular ciertas bases para abordar esta materia, definir conceptos esenciales y plantear circunstancias generales que podrán requerir la realización de estudios concretos en un futuro.

Además, la dependencia del ciberespacio y la extensión de sus efectos a todas y cada una de las realidades físicas hace que, en un futuro próximo, la mayoría de eventos de los que se derive un daño a un tercero tengan algún componente cibernético. Por ello, es esencial para la evolución de la doctrina académica en materia de Responsabilidad Civil que abordemos con profusión el objeto del presente estudio. Y es que hasta este momento los estudios sobre la materia que estamos desarrollando se han limitado a un ámbito de carácter divulgativo, sin el rigor académico que permitirá delimitar cada aspecto de forma inequívoca.

339 *Op. cit.*, *THIBER* (abril de 2016), p. 34, http://www.thiber.org/ciberseguros.pdf

5.1. Concepto y límites

La responsabilidad civil ha sido definida por Díez-Picazo como «la sujeción de una persona que vulnera un deber de conducta impuesto en interés de otro sujeto a la obligación de reparar el daño producido»[340]. Así, el origen de este concepto proviene del principio romano *alterum non ladere* —reconocido por Ulpiano en el *Digesto* 1.2.10.1 como uno de los tres principios del Derecho— a través del cual se establecía como una norma propia de la vida en sociedad la prohibición de no causar daño a otro.

El tratado sobre responsabilidad civil escrito por Ricardo de Ángel Yágüez comienza con la acertada consideración de que «el no causar daño a los demás es quizá la más importante regla de las que gobiernan la convivencia humana»[341]. Lo que indica, como consideraba el Derecho Romano, que la obligación del resarcimiento del daño constituía una máxima necesaria para el desarrollo de la vida en sociedad.

La obligación de reparar el daño causado fue reconocida por el artículo 1902 del Código Civil desde su redacción inicial al que se refiere Reglero Campos, que mantiene que «con carácter general puede afirmarse que un sujeto es responsable cuando incumple un deber o una obligación o cuando causa un daño»[342]. Y en este sentido, la sentencia del Tribunal Constitucional 181/2000, de 29 de junio, reconoció por primera vez la relevancia constitucional del referenciado derecho de reparación del daño, en cuanto el artículo 15 de la Constitución desarrolla la tutela civil del derecho a la vida y la integridad física y moral por medio de «un sistema adecuado y suficiente de reparación de los daños causados a los mismos».

En la actualidad, el concepto romano de desarrollo de la vida social parece extenderse al ámbito del ciberespacio al que se considera como un ecosistema separado e independiente en el que diversos sujetos interactúan y desarrollan sus derechos y libertades en un plano esencialmente social. Y, además, es importante destacar que un gran número de los hechos y acciones que allí se producen afectan a la realidad social del mundo físico. De todo ello resulta que la importancia que aquí atribuimos al estudio de la responsabilidad civil se fundamenta en la entidad y en el valor de los bienes

340 Luis Díez-Picazo y Antonio Gullón, *Sistema de derecho civil*, vol. II, Tecnos, 1989, p. 591.

341 Ricardo de Ángel Yágüez, *La responsabilidad civil*, Universidad de Deusto, Bilbao, 2.º ed. (1989), p. 21.

342 José Manuel Busto Lago y L. Fernando Reglero Campos (coord.), «Lección 2ª. Los sistemas de responsabilidad», en *Lecciones de Responsabilidad Civil*, Aranzadi, Navarra, 2013, p. 42.

jurídicos que pueden resultar afectados por los ciberriesgos, y no solo a un reduccionista análisis económico de la cuestión jurídica[343].

En este sentido, procede considerar que el principio *alterum non ladere* es un fundamento esencial para el desarrollo del ciberespacio por medio del cual se podrá evitar que la excesiva actividad regulatoria del Estado limite artificialmente las libertades de este nuevo entorno. Así, se hace necesario para garantizar la conservación de tales libertades realizar una apropiada adecuación de tal principio que pueda ser útil para el desarrollo del ordenamiento jurídico, y permita la adecuación de la doctrina a las nuevas realidades de la vida jurídica y social.

La doctrina jurídica que ha tratado el concepto del resarcimiento del daño desde el punto de vista filosófico se ha dividido en dos corrientes básicas formadas por los partidarios de la aplicación del principio de justicia distributivo y los que mantienen un principio de justicia conmutativo[344].

De esta forma, la doctrina de la justicia conmutativa ha sido reconocida por la gran mayoría de ordenamientos jurídicos, y fue mantenida por santo Tomás de Aquino al entender que la ley atiende solo a la diferencia del daño, de manera que el juez intentará dar solución a aquello que es injusto, que ha sido consecuencia del daño que uno propinó a otro, y que por tanto ha producido una situación de desigualdad, devolviendo tal situación de igualdad en la misma cantidad de cosas[345].

La justicia conmutativa se establece entre dos sujetos que compran y venden[346], y determina las mutuas cantidades debidas entre dos sujetos, de tal manera que obliga a «corresponder» en la misma medida de lo que se «recibe»[347]; o en el caso de la responsabilidad, en la medida en la que se «daña». En este sentido, la doctrina española ha supuesto una de las principales influencias para el desarrollo de este principio jurídico, y actualmente es el fundamento de la responsabilidad civil. Así, uno de los mejores ejemplos del arraigo con el que nuestra doctrina ha tratado estos principios se encuentra en la obra de Domingo de Soto, *De Iustitia et Iure* (libro V sobre las injusticias

343 José Manuel Busto Lago y L. Fernando Reglero Campos (coord.), *op. cit.*, p. 44.

344 Richard W. Wright, «Right, Justice and Tort Law», publicado en *Moral Foundations of the law of Torts*, Oxford University Press, 1995.

345 Santo Tomás de Aquino. *Comentario a la ética a Nicómaco de Aristóteles* (trad. Ana Mallea), Eunsa, Pamplona, 2012, p. 304.

346 Francisco de Vitoria, *Comentarios a la Secunda Secundae de Santo Tomás*, Salamanca, 1932, vol. 2, p. 55.

347 Millán-Puelles. *III. Obras completas: La función social de los saberes liberales* (1961), *Persona humana y justicia social* (1962), *La formación de la persona humana* (1963), Asociación de Filosofía y Ciencia Contemporánea, Rialp, Madrid, 2013, p. 145.

que se cometen contra la voluntad de los hombres, y el libro VI sobre las injusticias que afectan a los contratos[348]).

Y finalmente esta doctrina académica fue recogida en la Constitución Española por medio de la cual se puede afirmar, con carácter general, que «toda persona tiene un derecho constitucional a no sufrir un daño injusto contra un bien o derecho objeto de tutela jurídica», lo que se manifiesta tanto en la protección de los derechos fundamentales —artículo 15—, como en el respeto a la propiedad privada —artículo 33.1—. Tales derechos hoy adoptan las formas propias del ciberespacio a las que en adelante nos referiremos. Pues estos nuevos riesgos se plantean como un reto importante para tratar de mantener y adaptar los elementos clásicos de la responsabilidad civil.

5.1.1. Responsabilidad contractual y extracontractual

La obligación de reparar un daño puede provenir de actos muy diversos, pero todos ellos pueden agruparse en dos categorías que constituyen la responsabilidad civil contractual o extracontractual[349], cuyas particularidades presentan los siguientes elementos:

- La responsabilidad civil contractual surge del incumplimiento de una obligación previa en la que el hecho dañoso viene producido como resultado de tal incumplimiento. Su origen lo podemos situar en el principio romano *naeminem laedere*, que se consagró en el artículo 1101 del Código Civil en el que se establece que «quedan sujetos a la indemnización de los daños y perjuicios causados los que en el cumplimiento de sus obligaciones incurrieren en dolo, negligencia o morosidad, y los que de cualquier modo contravinieren al tenor de aquellas». Conforme a este precepto, nos referiremos a la responsabilidad contractual en sentido estricto, que se puede poner de manifiesto bajo muy diversas circunstancias como consecuencia de los ciberriesgos. Así, es importante advertir que cualquier empresa prestadora de productos y servicios, principalmente aquellas que ofrecen servicios relacionados con las IT, pueden incurrir en un incumplimiento contractual como consecuencia de un evento cibernético (por ejemplo, cuando una empresa de *hosting*, como consecuencia de un ciberevento, interrumpe sus servicios; o cuando una compañía pierde información confidencial perteneciente a otra, cuya integridad y confidencialidad se había obligado a salvaguardar).

348 Ángel Poncela González, *La Escuela de Salamanca*, Verbum, Madrid, 2015, p. 199.

349 Mariano Yzquierdo Tolsada, *Responsabilidad civil extracontractual, Parte general Delimitación y especies. Elementos. Efectos o consecuencias*, Dykinson, 2015, p. 91.

- La responsabilidad extracontractual o responsabilidad aquiliana ya fue reconocida por la *Lex aquilia de damno* y procede del genérico deber de conducta de no dañar a nadie. Este régimen de responsabilidad se manifiesta cuando por razones ajenas a una obligación o contrato uno daña a otro y ha sido consagrado en el artículo 1902 del Código Civil antes citado.

  En el ámbito de los ciberriesgos puede surgir como consecuencia de una innumerable tipología de situaciones, y entre ellas podemos poner como ejemplo: la responsabilidad que surge de la transmisión de un malware o por la creación de una vulnerabilidad en un sistema ajeno, y la responsabilidad que surge de cualquier daño que sea consecuencia de haber sufrido un ciberevento en los sistemas propios (entre otros, el accidente de un medio de transporte como consecuencia de un ciberevento en los sistemas de la compañía que lo gestiona y opera, o los daños ocasionados por un producto defectuoso cuando el defecto proceda de un ciberevento).

Es importante la determinación de la naturaleza de la responsabilidad civil procedente de los cibereventos ya que permite la aplicación del régimen jurídico concreto. No obstante, la diversidad de situaciones en las que se pueden manifestar los ciberriesgos hace que no resulte posible acoger una definición general de la naturaleza de la responsabilidad que procede de los mismos, sino que debemos definir cada caso en concreto.

En todo caso, sostiene Mariano Yzquierdo que los principios de la responsabilidad aquiliana constituyen el derecho común de la teoría de la reparación de los daños civiles[350], por lo que serán aplicables en todo caso y siempre que no lo sean las que componen el régimen especial de la responsabilidad civil extracontractual. Tal régimen especial exige «que exista un contrato válido entre el responsable y la víctima, y que el daño resulte de su incumplimiento»[351]. Así, debemos hacer una especial reflexión sobre los dos elementos que componen esta afirmación:

La existencia de un contrato previo

Sobre este aspecto la doctrina que ha estudiado la naturaleza de la responsabilidad de los datos personales del artículo 19.1 de la LOPDCP no es pacífica a la hora de considerar la naturaleza de este régimen de responsabilidad. No obstante, esta discusión nos sirve para explicar el carácter de la responsabilidad civil generada por los cibereventos de toda índole, que

350 Mariano Yzquierdo Tolsada, *op. cit.*, Dykinson, 2015, p. 99.

351 Mariano Yzquierdo Tolsada, *op. cit.*, Dykinson, 2015, p. 100.

como venimos advirtiendo no solo se reducen al ámbito de la pérdida y robo de datos personales.

La doctrina mayoritaria considera que se trata de un supuesto de responsabilidad civil extracontractual[352]. Y, frente a esta opinión, algunos autores han mantenido que se puede calificar como contractual, ya que surge del incumplimiento de las obligaciones legales de los responsables del tratamiento de datos personales (quienes resultan obligados de forma previa a garantizar la integridad de los datos)[353].

En conclusión, no parece que pueda darse una respuesta universalmente válida para todos los supuestos, ya que la naturaleza contractual, o no, de la acción ejercitada dependerá de la existencia, o no, de una relación contractual previa conforme a la cual se hayan cedido los datos personales al responsable del fichero[354], quien se obliga a garantizar la integridad de los mismos.

Por todo ello, como considera José Manuel Busto Lago, la responsabilidad civil contemplada en el artículo 19.1 de la LOPDCP tiene una naturaleza extracontractual sin perjuicio de la posible atribución del carácter «contractual» a algunos supuestos en los que existe un vínculo obligacional previo[355].

Por ello, con independencia de las obligaciones legales y presunciones que puedan establecerse para la salvaguarda de la seguridad en el ciberespacio, la responsabilidad solo adquiere la naturaleza contractual cuando se cumpla la regla general de que exista un vínculo previo entre el perjudicado y el causante del daño.

No obstante, la existencia de este vínculo en el ámbito del ciberespacio puede resultar bastante compleja, y ejemplos de ello son la recopilación de datos de usuarios de una determinada web o la instalación de *cookies* en sus sistemas para lo que no siempre ni en todos los ordenamientos jurídicos se exige el acuerdo expreso del usuario.

---

352 M. Heredero Higueras, *La Ley Orgánica 5/1992, de regulación de tratamiento automatizado de datos personales*, Ed. Tecnos, Madrid, 1996, p. 140; A. Ortí Vallejo, *Derecho a la intimidad e informática (Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada)*, Ed. Comares, Granada, 1994, p. 170; J. Aparicio Salom, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Ed. Aranzadi, Cizur Menor, 2.ª ed., 2002, p. 167.

353 M.ª P. García Rubio, *Bases de datos y confidencialidad en Internet*, *op. cit.*, p. 487.

354 G. Buttarelli, *Banche dati e tutela della riservatezza (La privacy nella Società dell'Informazione)*, Giuffrè Editore, Milán, 1997, pp. 351 y 352.

355 José Manuel Busto Lago, «La responsabilidad civil de los servidores y operadores de datos», Seminario sobre Protección de Datos, Ciudad Real (9 y 10 de noviembre de 2005), http://www.uclm.net/actividades0506/seminarios/proteccion_datos/pdf/busto.pdf

Que el daño resulte del incumplimiento del contrato

No solo es necesario que exista un vínculo previo, sino que el daño provenga del incumplimiento de aquello que forma parte del contrato. Aunque en ciertos casos es difícil delimitar si esta condición procede o no, por lo que Mariano Yzquierdo distingue tres casos con los que se puede observar esta zona trasfronteriza entre ambas naturalezas de la responsabilidad civil[356]:

1. El contrato y su ejecución constituyen solo una ocasión accidental para la producción del daño. Este es el caso en el que la relación operativa de los sistemas de un cliente y su proveedor ocasiona una vulnerabilidad en la seguridad de aquel, como consecuencia de la falta de seguridad de este, siempre que en el contrato no se hubiera garantizado tal idoneidad.

2. Cuando se incumple una obligación, pero el daño se produce sobre bienes de la personalidad, por lo que concluye que con independencia del bien que soporta el daño, la naturaleza de la responsabilidad se somete a la existencia de un contrato «en cuyo círculo de previsiones, expresas o no, figura» el bien que ha resultado dañado. Así, parece que la afirmación «expresas o no» introduce una amplia relación de posibles circunstancias en las que pueda existir responsabilidad contractual como consecuencia de un ciberevento. En este sentido, podemos poner como ejemplo el hecho, cierto, de que aunque nada se estipule en el contrato, parece que se tratará de responsabilidad civil contractual la que se genere como consecuencia de la brecha de seguridad causada por el informático que no puso todos los medios para evitar un ciberevento, o que permitió voluntariamente que se generasen ciertas vulnerabilidades.

3. Incumplimiento de una prestación accesoria que se encuentre íntimamente ligada a la naturaleza del contrato. Entre ellas, destaca la obligación de la sujeción a la buena fe que en el plano de la responsabilidad civil profesional extiende las obligaciones propias del contrato a deberes que no son los puramente técnicos (como el secreto profesional y cualquier otra obligación de carácter deontológico). De ello, podemos concluir que el profesional también responderá en el plano contractual del incumplimiento de aquellas obligaciones accesorias, cuando tal incumplimiento sea consecuencia de no haber aplicado las medidas de ciberseguridad adecuadas.

Así, parece que en ciertos casos, como el artículo 19.1 de la LOPDCP, existe una obligación previa ya que surge *ope legis*, pero esto no es suficiente para concluir que entre el perjudicando y el causante del daño existía un vínculo obligacional previo. Por ello, el artículo 19 y cualquier otra obligación legal de

356 Mariano Yzquierdo Tolsada, *op. cit.*, Dykinson, 2015, pp. 112-118.

velar por la integridad de un sujeto u objeto en el marco del ciberespacio requerirá que el daño se haya causado como consecuencia del incumplimiento de las obligaciones expresamente establecidas en el contrato, o de aquellas que sean causa necesaria de las mismas, ya sea porque lo determina la ley o por tratarse de un elemento íntimamente ligado o implícito a la obligación de que se trate.

En este sentido, la doctrina del Tribunal Supremo ha sido muy restrictiva en cuanto a la aplicación del régimen especial de la responsabilidad contractual y, en particular, desde la STS de 9 de marzo de 1983 se empezó a utilizar la doctrina de «la rigurosa órbita de lo pactado» por medio de la que se exige que «no es bastante que haya un contrato entre las partes para que la responsabilidad contractual opere necesariamente con exclusión de la aquiliana, sino que se requiere para que ello suceda la realización de un hecho dentro de la rigurosa órbita de lo pactado y como desarrollo del contenido negocial» (SSTS, 6 de mayo de 1985 y 10 de mayo de 1984).

Estas conclusiones tienen una especial relevancia en ciertos sectores del ámbito de las IT, entre las que podemos adelantar ciertas circunstancias que pueden llegar a resultar controvertidas.

La responsabilidad en el ámbito del Internet of Things (IoT)

El internet de las cosas (IoT) es una red global emergente[357] por medio de la que se interconectan diferentes sistemas para facilitar el funcionamiento de diversos instrumentos y objetos. Así, una de las principales características que de forma general suelen proporcionar estos sistemas es el funcionamiento autónomo de aquellos objetos[358], lo que podría llegar a alterar los límites de la responsabilidad de los fabricantes y proveedores de estos productos.

De tal forma, parece que se extiende el régimen de responsabilidad de los fabricantes y proveedores de los productos que forman parte del IoT a la mayor parte de los efectos del funcionamiento del producto, ya que el IoT sustituye la actuación del usuario por la interacción automática y programada. Así, la máxima de que el producto es defectuoso si no ofrece la seguridad que

357 Rolf H. Weber, «Internet of Things – New security and privacy challenges», *Computer Law & Security Review*, 26 (2010), p. 25, https://www.researchgate.net/profile/Rolf_Weber3/publication/222708179_Internet_of_Things_-_New_security_and_privacy_challenges/links/0c96053cab03fee371000000.pdf

358 Gerd Kortuem, Fahim Kawsar, Daniel Fitton, Vasughi Sundramoorthy, «Smart Objects as Building Blocks for the Internet of Things», the IEEE Computer Society (febrero de 2010), pp. 46-49, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5342399

legítimamente cabría esperar[359] se extiende al funcionamiento autónomo del mismo. Y de esta forma, la responsabilidad por los accidentes o fallos de los vehículos autónomos podría circunscribirse al ámbito de la responsabilidad del fabricante o provedor si se considera que la venta de estos vehículos lleva implícita la garantía del preciso y seguro funcionamiento de los mismos.

En este sentido, resulta adecuado hacer referencia al primer accidente mortal en un vehículo autónomo Tesla, por el que se criticó a la compañía por haber generado una expectativa de seguridad que se puso en evidencia. No obstante, la referenciada compañía ha mantenido que su sistema *autopilot* requiere que sea activado por el conductor, que deberá continuar en todo momento controlando el vehículo y con las manos sobre el volante, por lo que consideran que sigue siendo responsable del vehículo[360]. Y en contra de esto, Volvo admite la existencia de sistemas de conducción completamente autónoma que no requieren de la intervención de un conductor[361], y sobre los que como fabricante declara hacerse responsable de los riesgos que puedan surgir como consecuencia de la circulación del vehículo[362].

En definitiva, el límite de la responsabilidad del fabricante dependerá de la autonomía del objeto que forma parte del IoT y, como hemos dicho, de la seguridad que legítimamente cabría esperar[363] respecto al funcionamiento del mismo. Y, en este sentido, serán determinantes las advertencias de los riesgos y las precauciones de uso que el fabricante ofrezca [STS, 1.ª, 21.11.2008 (nº sentencia 1087/2008)].

La responsabilidad de los proveedores de servicios de software

En este sentido, podría llegar a reconocerse la responsabilidad de los proveedores de servicios de software cuando una determinada vulnerabilidad haya sido producida por un error en su software. Por ello, parece esencial de-

359 «Responsabilidad civil del fabricante por daños causados por productos defectuosos», Universidad Pompeu Fabra, p. 6, https://www.upf.edu/dretcivil/_pdf/mat_fernando/T82008.pdf

360 J. Raúl Fernández, «La responsabilidad en vehículos autónomos», Derecho y Nuevas Tecnologías (5 de julio de 2016), http://www.jraulfernandez.es/la-responsabilidad-vehiculos-autonomos/

361 Estas son las razones por las que el coche autónomo «siempre» va a tener la culpa en caso de accidente, *El blog de Mapfre* (14 de diciembre de 2016), http://blogmapfre.com/motor/estas-son-las-razones-por-las-que-el-coche-autonomo-siempre-va-tener-la-culpa-en-caso-de-accidente/#sthash.ISWBLwSz.dpuf

362 «¿De quién es la culpa del accidente cuando hay un coche autónomo de por medio?» *Tecvolución volvo* (3 de diciembre de 2016), http://tecvolucion.com/quien-es-responsabilidad-legal-accidente-cuando-hay-coche-autonomo-de-por-medio/

363 «Responsabilidad civil del fabricante por daños causados por productos defectuosos», Universidad Pompeu Fabra, p. 6, https://www.upf.edu/dretcivil/_pdf/mat_fernando/T82008.pdf

terminar los límites de la obligación de estos agentes, y en concreto aquellos que afectan al deber de mantener y actualizar sus programas para prevenir vulnerabilidades.

Tal y como se consideraba en el artículo «¿Quién es responsable de WannaCrypt?»[364], se puede definir una vulnerabilidad como aquellos puntos débiles del software que permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad del mismo. Y pueden clasificarse según su impacto potencial, su complejidad[365], o según el conocimiento que se tiene de su existencia. En el caso de la vulnerabilidad explotada por WannaCrypt («EternalBlue»), formaba parte de las calificadas como 0-day[366] por proceder de circunstancias desconocidas[367] para quien se encarga de mantener el sistema o software afectado[368].

Por ello, no concurren los requisitos de responsabilidad admitidos por la sentencia de la Audiencia Provincial de Pontevedra de 2 de octubre de 2014, ya que no se trata de una vulnerabilidad o brecha de seguridad evidente y que debía ser conocida por quien desarrollo el software. De tal forma, y sin perjuicio de una valoración más extensa, no puede afirmarse que concurran los requisitos que ha señalado la jurisprudencia para aplicar el régimen de responsabilidad civil, pues una vez se descubrió y publicó la existencia de tal vulnerabilidad, Microsoft desarrolló un parche para solventarla. Así, parece que debe entenderse cumplida la diligencia exigible al proveedor de software en tanto se reconoce generalmente que las vulnerabilidades 0-day recaen sobre aspectos muy concretos del software afectado, y que resultaban completamente desconocidas para aquellos[369].

Así, la existencia de una vulnerabilidad no permite presumir «que hay una discrepancia entre la situación del producto y lo que, según su diseño, tendría que resultar, a consecuencia de una anomalía en el proceso de producción del bien»

364 Jesús Jimeno, «¿Quién es responsable de WannaCrypt?, *Boletín Rc y Seguros*, INESE (1 de junio de 2017), http://boletinrc.inese.es/apendice-n36.html

365 Microsoft Security Intelligence Report, Microsoft, 2016, http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft_Security_Intelligence_Report_Volume_21_English.pdf

366 Dan Goodin, «NSA-leaking Shadow Brokers just dumped IT most damaging release yet», *arstechnica* (14 de abril de 2017), https://arstechnica.com/security/2017/04/nsa-leaking-shadow-brokers-just-dumped-IT-most-damaging-release-yet/

367 «What is a Zero-Day Vulnerability?», *Pctools*, http://www.pctools.com/security-news/zero-day-vulnerability/

368 Tony Bradley, *lifewire* (14 de octubre de 2016), https://www.lifewire.com/zero-day-exploIT-2487435

369 «What is Zero Day Exploit?», *kaspersky*, https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

[STS, 1.ª, 23.06.1993 (RJ 1993\5380), 8.2.1995 (RJ 1995\1630), 4.10.1996 (RJ 1996\7034)] por la que deba concurrir la «responsabilidad solidaria del fabricante» [STS, 1.ª, 14.7.2003 (RJ 2003\5837)]. Y, en definitiva, cualquier malware requiere de la concurrencia de un acto doloso de un tercero que aprovecha la vulnerabilidad para causar un daño o producir un efecto concreto, por lo que tampoco podría apreciarse la existencia del nexo causal entre el posible error de software y el daño.

Además, el pasado 14 de marzo de 2017 Microsoft publicó los parches de seguridad que permiten subsanar la referenciada vulnerabilidad que ya entonces calificó como crítica, por lo que puso en manos de todos los usuarios la información y herramientas adecuadas para la prevención de este malware. De tal forma, parece que la responsabilidad del proveedor recae no solo sobre la adecuada producción del software, sino que se extiende al posterior funcionamiento y mantenimiento del mismo. Y en este sentido, debemos hacer hincapié una vez más en los elementos de la imputabilidad de la responsabilidad que con relación a los productores de software plantean dudas sobre los límites de su obligación (como por ejemplo la obligación de continuar manteniendo las versiones obsoletas de software[370]).

Así, en el ejemplo de referencia, uno de los sistemas operativos afectados por tal vulnerabilidad fue Windows XP que Microsoft dejó de mantener y actualizar en abril de 2014, pero sigue siendo utilizado por millones de usuarios en todo el mundo[371].

Por ello, actualmente se ha abierto un debate sobre las posibles obligaciones de los fabricantes de software en relación con los sistemas antiguos y obsoletos de cuyos fallos y vulnerabilidades podrían llegar a responder[372]. Tal cuestión no sería aplicable al resto de versiones que resultaron afectadas, pero pone de manifiesto un aspecto que puede llegar a ser muy relevante en el ámbito de la responsabilidad civil de los proveedores de productos tecnológicos, y especialmente de aquellos que producen sistemas de IoT.

No obstante, la obligación de los proveedores de software e instrumentos que forman parte del IoT no puede resultar ilimitada como se ha mantenido en algunos casos, sino que como cualquier producto también está sometido a unos

370 Russell Brandom, «Is Microsoft to blame for the largest ransomware attacks in internet history?» *The verge* (15 de mayo de 2017), https://www.theverge.com/2017/5/15/15641198/microsoft-ransomware-wannacry-security-patch-upgrade-wannacrypt

371 Zeynep Tufekci, «The World Is Getting Hacked. Why Don't We Do More to Stop It?», *The New York Times* (13 de mayo de 2017), https://www.nytimes.com/2017/05/13/opinion/the-world-is-getting-hacked-why-dont-we-do-more-to-stop-it.html?_r=1

372 Russell Brandom, «Is Microsoft to blame for the largest ransomware attacks in internet history?» *The verge* (15 de mayo de 2017), https://www.theverge.com/2017/5/15/15641198/microsoft-ransomware-wannacry-security-patch-upgrade-wannacrypt

periodos de caducidad u obsolescencia (lo que es inevitable ya que depende del estado de la ciencia en cada momento concreto). Así, como veremos en relación con los elementos de la atribución de la responsabilidad, la cuestión principal parece que residirá en si tal riesgo —que en este caso desempeña el propio hecho de dejar de mantener un determinado software— ha sido adecuadamente notificado a los usuarios. En concreto, parece que debe plantearse la cuestión sobre si existe una verdadera relación de causalidad entre la falta de información de las limitaciones del software y los daños [SSTS, 1.ª, 28.5.2012 (RJ 2012\6545), 6.6.2012 (RJ 2012\6702), 25.3.2013 (JUR 2013\205719), 18.6.2013 (JUR 2013\216269)].

5.1.2. Responsabilidad civil ex delicto

Como ya hemos visto, la responsabilidad civil procede de un daño ocasionado por la acción u omisión de un sujeto sobre otro. Y esto, además de darse en el ámbito de las relaciones contractuales y extracontractuales, puede originarse o proceder de la comisión de un ilícito penal del que resulte un derecho de resarcimiento, o de una infracción en el ámbito laboral por la que se deba satisfacer una indemnización determinada que permita compensar el daño causado.

La responsabilidad civil ex delicto tiene por objeto la obligación de reparar el daño que se ocasiona por medio de la comisión de un ilícito penal, y se ha consagrado como una de las fuentes de las obligaciones reconocidas por el artículo 1089 del Código Civil en el que se establece que «las obligaciones nacen de la ley, de los contratos y cuasi contratos, y de los actos y omisiones ilícitos o en que intervenga cualquier género de culpa o negligencia». De tal manera, se diferencia a su vez entre dos fuentes de obligaciones que son: «las obligaciones civiles que nazcan de los delitos o faltas» (artículo 1092 del Código Civil) y «las que se deriven de actos u omisiones en que intervenga culpa o negligencia no penadas por la ley» (artículo 1093 del Código Civil). Así, las primeras recogen la responsabilidad civil derivada del ilícito penal, mientras que las segundas hacen referencia a la responsabilidad puramente civil.

Según ordena el artículo 1092 del Código Civil, la responsabilidad civil ex delicto ha quedado recogida por el artículo 109 del Código Penal que dispone que «1. La ejecución de un hecho descrito por la ley como delito obliga a reparar, en los términos previstos en las leyes, los daños y perjuicios por él causados. 2. El perjudicado podrá optar, en todo caso, por exigir la responsabilidad civil ante la Jurisdicción Civil». Y su ejercicio ha quedado sometido al procedimiento establecido en el artículo 112 de la Ley de Enjuiciamiento Criminal.

No obstante, como mantiene Mariano Yzquierdo, «la responsabilidad civil deriva solo del daño, y el hecho de que la acción que generó sea, además, constitutiva de una infracción penal, en nada modifica la naturaleza de la

obligación[373]. Y con independencia de la discusión sobre la utilidad de este régimen dual —que no atañe al presente estudio—, la referenciada afirmación nos facilitará considerar de forma general la responsabilidad civil procedente de los ciberriesgos.

Así, el desarrollo de este tipo de daños hace que los tipos delictivos que giran en torno a ellos se encuentren en un proceso de cambio y desarrollo. Por ello, referirnos a la responsabilidad civil en función del daño y no de la existencia del ilícito penal evitará que este estudio quede obsoleto en la medida en la que puedan surgir nuevos tipos penales o se modifiquen los existentes.

Por todo lo hasta aquí dicho, este apartado deberá completarse con cualquier otra obligación de reparar el daño causado según se tipifiquen unas u otras conductas, entre las que ya se puede hacer referencia a dos realidades que están formadas:

- por una parte, por los delitos recogidos por el artículo 264 del Código Penal, cuyo interés jurídico es la protección frente a los daños a sistemas informáticos y las IT;

- y, por otra parte, por cualquier otra actuación criminal que se sirva de las IT y el ciberespacio para cometer una acción penada por la ley.

La redacción del inicial artículo 264 del Código Penal fue modificada por medio de LO 5/2010, de 22 de junio, por la que se configuran como un tipo específico y claramente diferenciado de los daños del artículo 263. Esta redacción fue consecuencia directa del Convenio sobre la Ciberdelincuencia celebrado en Budapest en 2001 y la Decisión Marco 2005/222/JAI del Consejo. Y actualmente el contenido del artículo 264 resulta del texto introducido por la Ley Orgánica 1/2015, de 30 de marzo.

El artículo 264 del Código Penal establece que la conducta externa que puede dar lugar a la aparición del tipo penal es la de borrar, deteriorar, alterar, suprimir o hacer inaccesibles «datos, programas informáticos o documentos electrónicos ajenos». Y junto con tales elementos externos deben concurrir otras circunstancias a las que hace referencia en el mismo artículo, que son: que se produzcan «por cualquier medio», «sin autorización» y «de manera grave».

Para entender de manera adecuada el contenido de aquellas acciones que constituyen los elementos externos, consideramos procedente seguir la explicación que elabora Jorge A. González en su tesis sobre los daños informáticos

373 Mariano Yzquierdo Tolsada, *op. cit.*, Dykinson, 2015, p. 64.

del artículo 264 del Código Penal[374], ya que se trata del estudio más completo sobre el mismo que se ha realizado hasta la fecha. Y en él se analiza cada uno de los elementos externos desde la siguiente perspectiva:

- Las acciones de borrar y suprimir datos, programas informáticos o documentos electrónicos, así: la primera, se refieren a eliminar texto, datos o documentos, sin suprimir los archivos del soporte, de manera que se habilita el espacio que están ocupando, pero se podrán recuperar con facilidad; y la segunda, supone la desaparición total del objeto.

- La acción de hacer inaccesibles datos, programas informáticos o documentos electrónicos, lo que incluye cualquier actuación que impida el acceso a los mismos, aunque sea de manera temporal, sin que ello conlleve un verdadero daño o menoscabo de su contenido.

- La acción de alterar datos, programas informáticos o documentos electrónicos, que puede conllevar: la inaccesibilidad de los mismos a través de la alteración de su propia sustancia, la eliminación de parte de su contenido o cualquier modificación que afecte al mismo.

- La acción de deteriorar datos, programas informáticos o documentos electrónicos es una modificación destructiva en la que además de perder valor económico se pierde sustancia de la cosa.

- La acción de dañar datos, programas informáticos o documentos electrónicos, de la que forman parte las acciones de destruir, deteriorar o inutilizar los mismos.

Y en cuanto a las demás circunstancias recogidas en el artículo 264 del Código Penal:

- La expresión «por cualquier medio» puede suscitar una discusión sobre si el tipo penal engloba los daños físicos que pueda sufrir el hardware, y a su vez afectar a datos, programas informáticos o documentos electrónicos. En concreto, parece haberse admitido que los daños físicos que cumplan con el resto de requisitos también pueden constituir la acción que aquí se persigue, por lo que resulta apropiado atender a una interpretación extensiva[375]. No obstante, en el plano estrictamente civil, estos daños físicos difícilmente

374 González Hurtado, Jorge Alexandre, *Daños informáticos del artículo 264 del Código Penal y propuesta de reforma*, Universidad Complutense de Madrid, Madrid, 2013.

375 F. Miró Llinares, «Delitos informáticos: Hacking. Daños», p. 161, y en el mismo sentido, N. J. De La Mata Barranco, *Derecho Penal Informático*, Ed. Thomson Reuters, Navarra, 1.ª edición, 2010, p. 161.

pueden ser considerados como un ciberataque, ya que las circunstancias en torno a las que se producen los mismos no guardan ninguna relación con los elementos de las IT, salvo en lo relativo a la cuantificación del daño.

- El referenciado artículo exige que los hechos acaezcan «de manera grave», y sobre tal expresión ha discutido la doctrina al entender que la gravedad se puede poner de manifiesto en la acción o en el resultado de manera indistinta, aunque parece que la mayoría de autores[376] admiten que esta exigencia cualificada de gravedad se refiere al resultado. En términos de Derecho Civil es desde luego más útil determinar con precisión el resultado, aunque la gravedad de la acción y cualquier elemento que gire en torno a la misma podrá ser determinante a efectos de la atribución de la culpa (con las circunstancias propias del dolo si lo hubiere) y la existencia de nexo causal.

- Sobre la ajenidad y la falta de consentimiento, ambos son conceptos con una evidente relevancia civil que en este caso, además, constituyen elementos del tipo cuya apreciación debe ser necesaria [Audiencia Provincial de Málaga (Sección 1ª), Sentencia nº 60/2005, de 28 de enero). Así, de la destrucción de datos propios no puede deducirse la comisión de este tipo de delitos como mantiene el auto de 30 de octubre de 2013 del Juzgado de Instrucción nº 32 de Madrid[377]. La importancia de estos dos elementos a efectos de la responsabilidad civil ex delicto es determinante, ya que, según veremos, el consentimiento o participación del perjudicado en el daño impedirá la atribución del nexo causal. En el ámbito de los daños informáticos y las ciberamenazas, este elemento plantea una gran cantidad de situaciones de difícil resolución jurídica, ya que, según hemos visto en el primer capítulo de nuestro estudio, un número elevado de cibereventos se debe a la actuación directa o indirecta de *insiders* (empleados, o personas que forman parte o están vinculadas con la entidad afectada).

- Además, se establece un tipo *agravado* «cuando el resultado producido fuera grave», lo que además pone de manifiesto que se trata de un delito de resultado[378], que en la mayoría de los casos dará lugar a un perjuicio

376 Fernando Miró Llinares, «Delitos contra bienes inmateriales, corrupción y receptación: análisis y consideraciones críticas ante la nueva reforma penal», 2015, p. 161, y en el mismo sentido, N. J. De La Mata Barranco, *Derecho Penal Informático*, Ed. Thomson Reuters, Navarra, 1.ª edición, 2010, p. 164.

377 Andreu Van den Eynde Adroer, Análisis jurídico del sabotaje informático, ENATIC, Consejo General de la Abogacía Española, http://www.abogacia.es/2015/03/09/analisis-juridico-del-sabotaje-informatico/

378 J. J. González Rus, «El cracking y otros supuestos de sabotaje informático», en *Estudios Jurídicos*. Ministerio Fiscal, nº 2 (2003). El mismo autor en Juan José González Rus, «Daños a través de internet y denegación de servicios», en A. Jorge Barreiro (coord.), *Homenaje al profesor Dr.*

económicamente resarcible. Así, el requisito de la gravedad en el resultado tiene un especial efecto en cuanto a la responsabilidad civil ex delicto, y en torno a él ha discutido la doctrina sobre los evidentes efectos materiales y económicos de los delitos informáticos. En este sentido, llegan a reconocer Miró Llinares[379] y De La Mata Barranco [380]que uno de los elementos del tipo es que se produzca un daño económicamente valorable [Audiencia Provincial de Madrid (Sección 4.ª), Auto n° 16/2007, de 15 de enero]; y añade A. C. Andrés Domínguez[381] que el valor económico constituye un elemento típico del delito de daños, por lo que la cosa corporal y ajena ha de ser económicamente valorable, y tal valor debe ser intrínseco a la misma [Audiencia Provincial de Valencia (Sección 4.ª), Sentencia n° 447/2011, de 10 de junio].

En este sentido, mantiene Jorge A. González en su tesis que desde la obra *Delincuencia informática*[382] de Mir Puig se ha puesto de manifiesto que aunque el objeto dañado no sea económicamente valorable, los daños informáticos pueden producir una serie de daños generales. Y para el referenciado autor, estos efectos se limitarían exclusivamente a la esfera del Derecho Civil, ya que el ataque informático no produce un daño económicamente valorable sobre el bien en el que incide de manera directa. Esta tesis es además la que mantiene el Auto de la AP Barcelona de 30 de octubre de 2000, que establece:

«Ni siquiera mediante el recurso a la interpretación extensiva es posible incardinar el traspaso de una reserva de viaje hecha por un cliente y anotada en un programa informático a otra empresa, aun cuando se traduzca en eliminar materialmente dicha anotación, en el apartado 2.° del artículo 264 del Código Penal en el que se recoge, al igual que en su apartado 1.°, un tipo agravado del delito de daños regulado en

---

Gonzalo Rodríguez Mourullo, Ed. Thomson Civitas, Navarra, 1.ª edición, 2005, pp. 1.472 y ss.; J. J. González Rus, «Los ilícitos en la red (I): *hackers, crackers, cyberpunks, sniffers*, denegación de servicio y otros comportamientos semejantes», en C. M. Romeo Casabona (dir.), *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Ed. Comares, Granada, 2006, pp. 248 y ss. y J. J. González Rus, «Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos», en J. L. Díez Ripollés, C. M. Romeo Casabona, L. Gracia Martín y J. F. Higuera Guimerá (coords.), *La ciencia del Derecho Penal ante el nuevo siglo. Libro homenaje al profesor doctor don José Cerezo Mir*, Ed. Tecnos, Madrid, 1.ª edición, 2002, p. 248.

379 Fernando Miró Llinares, «Delitos informáticos: *Hacking*. Daños», en Íñigo Ortiz de Urbina Gimeno (coord.): *Memento Experto. Reforma Penal*, Ed. Ediciones Francis Lefebvre, Madrid, 1.ª edición, 2010, op. cit., p. 162.

380 Norberto Javier De La Mata Barranco y Leyre Hernández Díaz, «El delito de daños informáticos. Una tipificación defectuosa», *En Estudios Penales y Criminológicos*, n° 29 (2009), p. 165.

381 A. C. Andrés Domínguez, *El delito de daños: consideraciones jurídico-políticas y dogmáticas*, Ed. Universidad de Burgos, Burgos, 1.ª edición, 1999, p. 122.

382 S. Mir Puig, *Delincuencia informática*, Ed. PPU, Barcelona, 1.ª edición, 1992, pp. 172 y ss.; en Jorge Alexandre González Hurtado, *op. cit.*, Universidad Complutense de Madrid, Madrid, 2013.

el artículo 263 del mismo texto legal. En efecto, el delito de daños constituye una figura concretada en la destrucción o menoscabo material o funcional de la propiedad ajena, de manera que el objeto de ajeno dominio sobre el cual se lleve a cabo la acción resulte destruido o menoscabada, sea en su entidad física sea en la funcionalidad que le es propia lo que, desde luego, no sucede con la conducta llevada a cabo por la imputada que se limitó a hacer desaparecer o a no darle el destino al que estaba laboralmente obligada unas reservas de viajes efectuadas por clientes, sin 'destruir, alterar, inutilizar o dañar de cualquier otro modo' datos, programas o documentos electrónicos contenidos en soporte informático, destrucción, inutilización, alteración que debe comportar un daño patrimonial (por reparación o sustitución del objeto material sobre el que ha operado la acción delictiva) superior a 50.000 ptas, extremo del que ni siquiera se habla en la denuncia o en el recurso sino, en su caso, de perjuicios posibles derivados de la pérdida de las comisiones que habrían devengado la efectividad de las reservas llevadas a cabo y luego traspasadas (reservas por las que ni siquiera se pagó) en caso de haberse confirmado, lo que en todo caso sería susceptible de calificarse como de lucro cesante civilmente resarcible, pero no del daño típico de las figuras penales de daños».

El artículo único de la Ley Orgánica 1/2015, de 30 de marzo, introdujo diversas modificaciones en el Código Penal entre las que tenemos que destacar la reforma del referenciado artículo 264, cuyo desarrollo es consecuencia de la transposición de los preceptos de la Directiva 2013/40/UE, de 12 de agosto.

Así, el apartado XIII de la Exposición de Motivos establece que «las modificaciones propuestas pretenden superar las limitaciones de la regulación vigente para ofrecer respuesta a la delincuencia informática en el sentido de la normativa europea». Por ello, se introduce en el Código Penal tres nuevos preceptos (264 bis, 264 ter y 264 quarter) de cuyo contenido podemos destacar:

- Por medio del artículo 264 ter, se tipifica la facilitación o la producción de programas informáticos o equipos que tengan por objeto facilitar la comisión de delitos de esta índole. Y dentro del mismo precepto, también se tipifica la acción de proporcionar el acceso de un sistema a quien no esté autorizado, cuya comisión es muy común, según los datos que hemos estudiado en los primeros capítulos al hacer referencia a los ciberevents provocados por *insiders*.

- Se regulan de forma separada los supuestos de daños informáticos y las interferencias en los sistemas de información. El artículo 264 bis recoge de forma exclusiva la interrupción u obstaculización de los sistemas informáticos, cuya práctica se ha extendido por medio de los ataques DDoS. Además, introduce un tipo agravado para el caso en el que esta paralización

«perjudique de forma relevante la actividad normal de una empresa, negocio o de una Administración pública». Y se establece un tipo agravado para aquellos casos en los que se haya obtenido acceso al sistema por medio de la utilización ilícita de datos personales.

- El artículo 264 quarter establece el régimen de responsabilidad de las personas jurídicas a las que conforme al artículo 31 bis se las pueda atribuir la responsabilidad de este tipo de acciones delictivas.

En relación con la propiedad intelectual, el artículo único de la Ley Orgánica 1/2015, de 30 de marzo, ha introducido diversas novedades relevantes al efecto de la responsabilidad civil.

Así, se modificó el tipo objetivo del tradicional artículo 270 para extenderlo a cualquier tipo de acción (al incorporar la posibilidad de «explotar económicamente de cualquier otro modo»). Tal novedad responde a la necesidad de establecer normas dinámicas que sean capaces de adaptarse al desarrollo del ciberespacio y los ciberataques. Y también se modifica el tipo subjetivo al introducir la expresión «dolo y ánimo de lucro directo o indirecto»[383], de tal modo que puedan comprenderse conductas en las que el beneficio es indirecto, lo que en términos de la responsabilidad civil ex delicto permite exigir el resarcimiento íntegro al causante del daño aunque este no se haya beneficiado de forma directa.

La nueva redacción del artículo 270.2 tipifica de forma específica la actividad desarrollada por los sitios web que proporcionan enlaces a contenido objeto de propiedad intelectual publicado sin autorización. Y esto, conforme al siguiente tenor literal: «los que facilitan el acceso o localización en internet de obras o prestaciones objeto de propiedad intelectual sin autorización de los titulares».

Otra de las novedades que introdujo la Ley Orgánica 1/2015, de 30 de marzo, con especiales efectos a la hora de determinar la responsabilidad civil, es la reforma del artículo 197 con la introducción de las disposiciones 197 bis, 197 ter, 197 quarter, 197 quinquies[384]. Así, el legislador ha incluido dentro del tipo objetivo del artículo 197.7 el requisito de la difusión sin consentimiento, y tal circunstancia es además importante a efectos civiles porque será determinante en cuanto al daño moral que pueda padecer la víctima.

---

383 Júlia Bacaria Gea, «Aspectos TIC en la reforma del Código Penal», *gld* (3 de junio de 2015), http://legal-data.net/aspectos-tic-en-la-reforma-del-codigo-penal/

384 Cuadro Comparativo, Ley Orgánica 1/2015, de 30 marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, ICAM, p. 195, http://web.icam.es/bucket/CUADRO%20COMPARATIVO%20DEL%20C%C3%93DIGO%20PENAL_%20LO%201-2015_%20CP.pdf

Por su parte, la introducción de los artículos 197 bis al 197 quinquies responde a la aplicación de la Directiva 2013/40/UE, de 12 de agosto, y en ellos se desarrolla una completa tipificación del acceso no autorizado a las IT, el ciberespionaje, la creación de herramientas y programas que permitan el acceso no autorizado a sistemas, y la interceptaciones entre sistemas o equipos[385]. No obstante, resulta difícil comprender en qué casos podrá surgir un daño resarcible conforme a las normas del Derecho Civil. Y ello, porque del simple acceso no autorizado no tiene por qué surgir un daño determinado, cierto y económicamente valorable. Salvo en los casos en los que se publique la información obtenida o pueda extenderse la responsabilidad a aquel que ha facilitado el acceso a los sistemas, y en definitiva en cualquier caso que pueda valorarse el daño causado (Juzgado de lo Penal de Valencia, Sentencia nº 321/2004, de 15 de junio).

5.1.3. La responsabilidad civil en el ámbito de la jurisdicción social

En el ámbito de las relaciones laborales también puede producirse un daño como consecuencia directa o indirecta de la acción u omisión de un trabajador o empresario, de la que consecuentemente surja la obligación de resarcir tal daño.

En concreto, nuestro ordenamiento jurídico y la jurisprudencia se han preocupado de los daños que pueden sufrir los trabajadores y la responsabilidad de los empresarios como consecuencia de los mismos. Y en este sentido, la sentencia del Tribunal Supremo de 24 de mayo de 1994 y 30 de septiembre de 1997, entre otras, ha declarado que «es competente el orden social para conocer los daños causados al trabajador por todas las conductas del empresario en que este actúe como tal empresario con imputación de culpa bien se plantee esta como contractual, bien se plantee como extracontractual, que sea causa del daño producido»[386].

El artículo 1 de la Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social atribuye la competencia para conocer las cuestiones que se susciten dentro de la rama laboral de Derecho a la jurisdicción social. El artículo 2 delimita el ámbito de tal competencia al recoger una serie de supuestos o ejemplos[387] por los que se atribuye la misma a los órganos de la jurisdicción social.

---

385 Júlia Bacaria Gea, *op. cit.* (3 de junio de 2015), http://legal-data.net/aspectos-tic-en-la-reforma-del-codigo-penal/

386 I. Albiol Montesinos, C. L. Alfonso Mellado, A. Blasco Pellicer, J. M. Goerlich Peset, *Derecho Procesal Laboral*, Tirant lo Blanch, Valencia, 1996, p. 38.

387 J. Motero Aaroca, M. Iglesias Cabero, J. M. Martín Correa, M. Sampedro Corral, *Comentarios a la Ley de Procedimiento Laboral*, t. I, Civitas, Madrid, 1993, p. 38; *cfr.* también A. Montoya

En este sentido, el artículo 2.b establece que los órganos de la jurisdicción social conocerán las cuestiones que se promuevan en materia de responsabilidad contractual y extracontractual al establecer que «en relación con las acciones que puedan ejercitar los trabajadores o sus causahabientes contra el empresario o contra aquellos a quienes se les atribuya legal, convencional o contractualmente responsabilidad por los daños originados en el ámbito de la prestación de servicios o que tengan su causa en accidentes de trabajo o enfermedades profesionales, incluida la acción directa contra la aseguradora y sin perjuicio de la acción de repetición que pudiera corresponder ante el orden competente».

En este ámbito, atenderemos a dos supuestos de los que principalmente podrá derivar la responsabilidad civil del empresario frente a los trabajadores que son: la responsabilidad civil en materia de seguridad y salud en el trabajo, y el resarcimiento por la vulneración de derechos fundamentales.

a. La responsabilidad civil en materia de seguridad y salud en el trabajo

El artículo 42.1 de la Ley 31/1995 de Prevención de Riesgos Laborales establece que «en el cumplimiento por los empresarios de sus obligaciones en materia de prevención de riesgos laborales dará lugar a responsabilidades administrativas, así como, en su caso, a responsabilidades penales y a las civiles por los daños y perjuicios que pueden derivarse de dicho incumplimiento». En todo caso, esta responsabilidad tiene como objeto resarcir el daño que un trabajador haya padecido como consecuencia de un accidente de trabajo, por lo que nos deberemos centrar en aquellos casos en los que nuestro ordenamiento jurídico permita atribuir tal responsabilidad al empresario. **Y en el ámbito de los ciberriesgos es importante que atendamos a esta materia en la medida en que un ciberevento podría llegar a provocar un fallo en los sistemas de seguridad de los trabajadores y ocasionar un accidente, cuya responsabilidad pueda derivarse al empresario en el plano de la responsabilidad extracontractual.**

Los daños ocasionados como consecuencia del incumplimiento por parte del empresario de las normas de seguridad se atribuyen al ámbito de la responsabilidad contractual. Y la responsabilidad extracontractual es exigible al empresario con carácter subsidiario para aquellos supuestos en los que el trabajador a su servicio fuera elemento causante de daños a otras personas, trabajador o terceros[388].

Melgar, J. M. Galiana Moreno, A. V. Sempere Navarro, B. Ríos Salmerón, *Curso de Procedimiento Laboral*, 5.ª ed., Tecnos, Madrid, 1998, pp. 36-37.

388 José Antonio Fernández Avilés, «La responsabilidad civil en el ámbito de la jurisdicción social: puntos críticos», pp. 27 y 28, http://www.asociacionabogadosrcs.org/ponencias/pon2-4.pdf

En todo caso, es importante advertir que la obligación del empresario es *de medios* y tiene un carácter especialmente amplio y extenso. Por ello, se ha llegado a considerar que se trata de una responsabilidad objetiva[389], cuya apreciación se deriva únicamente de la constatación de la producción del daño.

La atribución de este régimen de responsabilidad exige la existencia de culpa por parte del empresario, lo que hace necesario la prueba de la existencia del daño y del incumplimiento de una norma en materia de riesgos laborales. Y por parte, del empresario se exige que cumpla sus obligaciones con la diligencia del buen empresario de la que participan: el deber de previsión, el deber de evitación o prevención —sentencia del Tribunal Supremo de 1 de octubre de 1998— y el deber de vigilancia efectiva —sentencia del Tribunal Supremo de 31 de diciembre de 1998—. En ciertos casos, el empresario es además responsable del incumplimiento de sus trabajadores o de otras empresas sobre las que ostenta el deber de vigilancia —24.3 LPRL—.

La determinación del grado de cumplimiento de las obligaciones en materia de prevención deberá adecuarse a las circunstancias de cada caso y al estado de la ciencia del momento, ya que se trata de una obligación dinámica que se encuentra condicionada a evolución tecnológica y a la necesidad de revisión periódica[390]. Y, además, comprende todos aquellos medios exigidos por alguna norma y aquellos cuya utilización sea eficiente para evitar el accidente.

El artículo 14.2 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales establece una obligación de carácter general al referirse a las obligaciones del empresario, ya que exige que garantice «la seguridad y la salud de los trabajadores a su servicio en todos los aspectos relacionados con el trabajo», para lo que deberá adoptar «cuantas medidas sean necesarias para la protección de la seguridad y la salud de los trabajadores».

Actualmente, el desarrollo de las IT y en especial de las IoT pueden facilitar que todos los sistemas de seguridad y prevención de una empresa estén conectados al ciberespacio, por lo que una parte esencial de los mismos es la integridad de esta conexión y su funcionamiento como sistema que opera por medio de las IT. Y en tales casos, la seguridad del propio sistema puede llegar

389 C. L. Alfonso Mellado, *Responsabilidad empresarial en materia de seguridad y salud laboral*, Tirant lo Blanch, Valencia, 1998, p. 127.

390 José Antonio Fernández Avilés, *op. cit.*, p. 32, http://www.asociacionabogadosrcs.org/ponencias/pon2-4.pdf

a formar parte de la genérica obligación de garantizar la seguridad y salud de los trabajadores.

El referenciado artículo 14.2 establece que «el empresario desarrollará una acción permanente de seguimiento de la actividad preventiva con el fin de perfeccionar de manera continua las actividades de identificación, evaluación y control de los riesgos que no se hayan podido evitar y los niveles de protección existentes, y dispondrá lo necesario para la adaptación de las medidas de prevención señaladas en el párrafo anterior a las modificaciones que puedan experimentar las circunstancias que incidan en la realización del trabajo». De esta forma, parece que el desarrollo de la ciencia en el ámbito de la seguridad cibernética y la prevención de aquellos ciberriesgos que puedan afectar a la integridad de los trabajadores también estará comprendida dentro de la obligación genérica de seguridad a la que está sometido el empresario.

b. Responsabilidad civil por vulneración de derechos fundamentales

La acción de tutela de los derechos fundamentales tiene un carácter complejo (sentencias del Tribunal Supremo de 9 de junio de 1993, 14 de julio de 1993 y 8 de mayo de 1995) y normalmente se compone por cuatro pretensiones cuyo objeto —conforme al artículo 182 de la Ley 36/2011, de 10 de octubre— es:

- Obtener una sentencia declarativa que reconozca que se ha vulnerado un determinado derecho.
- Declarar la nulidad radical de la actuación.
- Ordenar el cese inmediato de la actuación contraria a derechos fundamentales o a libertades públicas.
- Y disponer el restablecimiento del demandante en la integridad de su derecho y la reposición de la situación al momento anterior a producirse la lesión del derecho fundamental, así como la reparación de las consecuencias.

El artículo 177 de la Ley 36/2011, de 10 de octubre, Reguladora de la Jurisdicción Social establece que «cualquier trabajador o sindicato que, invocando un derecho o interés legítimo, considere lesionados los derechos de libertad sindical, huelga u otros derechos fundamentales y libertades públicas, incluida la prohibición de tratamiento discriminatorio y del acoso, podrá recabar su tutela a través de este procedimiento cuando la pretensión se suscite en el ámbito de las relaciones jurídicas atribuidas al conocimiento del orden jurisdiccional social o en conexión directa con las mismas, incluidas las que

se formulen contra terceros vinculados al empresario por cualquier título, cuando la vulneración alegada tenga conexión directa con la prestación de servicios».

Y, además, el artículo 177.4 añade, haciendo expresa referencia al acoso laboral, que «la víctima del acoso o de la lesión de derechos fundamentales y libertades públicas, con motivo u ocasión de las relaciones jurídicas atribuidas al conocimiento del orden jurisdiccional social o en conexión directa con las mismas, podrá dirigir pretensiones tanto contra el empresario como contra cualquier otro sujeto que resulte responsable, con independencia del tipo de vínculo que le una al empresario».

Como hemos tratado en los primeros capítulos, el ciberespacio es un medio en el que las personas se relacionan y desarrollan sus actividades profesionales y laborales, y en él despliegan sus derechos y libertades. Por ello, son susceptibles de padecer cualquier género de vulneración que provenga de un ciberevento o de otra agresión. Y en la medida en que las distintas operaciones y actividades que se desarrollan en una empresa se hagan por medio del ciberespacio, sus trabajadores quedarán expuestos a estos riesgos.

De esta manera, la acción que recoge el artículo 177 podrá ejercitarse contra el empresario por el trabajador que haya padecido un robo de su información personal, ciberacoso, o cualquier otro ataque contra sus libertades y derechos fundamentales, y se podrá llegar a responsabilizarse a aquel si se prueba que no ha aplicado las medidas de prevención suficientes para evitar el daño.

El ciberacoso no forma parte de la definición de evento cibernético a la que nos estamos refiriendo, ya que no requiere del quebrantamiento de las medidas de seguridad de las IT, ni produce un daño a estas y los sistemas que de ellas depende. De tal forma, no constituye en sí el objeto de un ciberriesgo ni cualquier género de amenaza cibernética, sin perjuicio de que lo sea alguna acción que se relacione con este. No obstante, no se puede olvidar que del ciberacoso producido en el ámbito laboral podrá ejercitarse una acción de responsabilidad civil contra el sujeto causante del daño y contra el empresario por un hecho propio o ajeno.

En conclusión, parece perfectamente lógico afirmar que por vía de los procedimientos ante la jurisdicción laboral a los que nos hemos referido podrá exigirse la responsabilidad de aquellos empresarios que no hayan dispuesto de las medidas de protección y seguridad adecuadas para evitar que, como consecuencia de un ciberevento, resulte dañada la integridad de los trabajadores, o que por medio de este se vulneren sus derechos y libertades fundamentales.

Por ello, estas medidas de seguridad tendrán por objeto principal intentar garantizar conforme al estado de la ciencia la seguridad de las IT y de los sistemas de los que depende la seguridad de los trabajadores, y la integridad

de cualquier otro sistema o maquinaria que como consecuencia de un ciberevento pueda ocasionar un daño a los trabajadores.

5.2. Elementos de la responsabilidad civil y ciberriesgos

El desarrollo del ciberespacio ha creado una gran cantidad de situaciones de las que puede surgir una relación de responsabilidad contractual o extracontractual. El informe publicado por la OCDE en 2002 por el que se recopilan las directrices que este organismo ha ido manteniendo en materia de ciberseguridad considera que todos los participantes en el ciberespacio dependen de los sistemas y redes de información locales y globales. Por ello, mantiene que deben comprender su responsabilidad en la salvaguarda de la seguridad de los sistemas y redes de información, y responder ante esta responsabilidad de una manera apropiada a su papel individual. Asimismo, estos participantes deberán revisar sus propias políticas, prácticas, medidas y procedimientos de manera regular, y evaluar si son apropiadas conforme a su ámbito.

En este sentido, exige el informe que aquellos que desarrollan, diseñan o suministran productos o servicios deberán elevar la seguridad de los sistemas y redes, y distribuir a los usuarios de manera apropiada información adecuada en materia de seguridad. Y entre ellas, deberán incluir actualizaciones para que estos entiendan mejor la funcionalidad de la seguridad de sus productos y servicios, y atender debidamente a la responsabilidad que les corresponde en materia de seguridad[391].

No obstante, para que pueda atribuirse responsabilidad civil a alguno de los sujetos participantes en el ciberespacio es necesario que concurran los requisitos fundamentales de la misma:

- que concurra una acción u omisión de un determinado sujeto;
- que produzca un daño a un tercero;
- y que entre aquella acción u omisión y el daño exista una relación de causalidad.

Así, para estudiar los supuestos en los que una ciberamenaza puede llegar a causar esta responsabilidad será necesario atender a los requisitos y particularidades de cada uno de los referenciados elementos.

391 «Directrices de la OCDE para la seguridad de sistemas y redes de información: Hacia una cultura de seguridad», OCDE (2004), p. 7, http://www.oecd.org/internet/ieconomy/34912912.pdf

5.2.1. Las acciones y omisiones en los ciberriesgos

El primer elemento de la responsabilidad civil es la acción y omisión, cuya relevancia ha sido destacada por Rogel Vide[392], que considera que este se debería estudiar prescindiendo de los restantes elementos de la responsabilidad civil. En la responsabilidad civil contractual se trata de cualquier incumplimiento o cumplimiento defectuoso de la obligación previamente pactada. Y en el caso de la responsabilidad aquiliana, las acciones consisten en una agresión injustificada de un bien, derecho o interés de otro. Las omisiones procederán de la falta de ejecución de aquello que se debía hacer o del ejercicio de lo que, como reconoce Lawson[393], se debía omitir, por lo que requiere que exista un previo deber de actuar[394].

La antijuridicidad es uno de los elementos que tradicionalmente se han ligado a la acción y omisión, aunque como advierte Pena López actualmente este concepto parece carecer de relevancia práctica. Por ello, no nos detendremos en la discusión sobre el carácter de la antijuridicidad, máxime cuando el Tribunal Supremo tiene reconocido que «es requisito bastante para declarar la responsabilidad extracontractual, el de la ilicitud ampliamente entendida por haber transgredido el agente las reglas de conducta, faltando al cuidado y diligencia exigibles y dañado bienes jurídicamente protegidos».

Así, en el ámbito de los ciberriesgos, la realidad material que se encuentra en continuo proceso evolutivo excede de los límites de la regulación que es escasa, y está sometida a la situación del momento en el que se dictó. Por ello, no será útil limitar el ámbito de la responsabilidad civil a aquellos supuestos en los que se produzca el incumplimiento de un precepto legalmente establecido, ya que exigiría un aumento desproporcionado de la regulación con el que quedarían desatendidas todas aquellas situaciones que no estén expresamente amparadas por la ley. Y en todo caso, será conveniente que sigamos la doctrina del Tribunal Supremo entendiendo la ilicitud desde un punto de vista amplio. De esta forma, los intereses jurídicamente protegidos se deberán considerar conforme a los bienes y derechos que subyacen en los mismos cuando aún no hayan sido objeto de una regulación específica.

A su vez, Mariano Yzquierdo se decanta por la distinción entre daños justificados —que no dan lugar al surgimiento del derecho de resarcimiento— y no justificados —de los que aparece la obligación de resarcir—, debiendo atenderse a aquellos casos en los que la acción u omisión deba entenderse justificada. Y esto, con independencia de que consideremos (como hace la

392 Rogel Vide, *La responsabilidad civil extracontractual*, ed. Civitas, Madrid, 1976, p. 76.

393 F. H. Lawson, *Negligence in the civil law*, Oxford, 1950, p. 29.

394 Mariano Yzquierdo Tolsada, *op. cit.*, Dykinson, 2015, pp. 137-138.

doctrina administrativista) que lo verdaderamente resarcible son los daños que la víctima no tenga el deber jurídico de soportar (sentencia del Tribunal Supremo de 11 de febrero de 1999), o simplemente aquellos daños con el carácter ilícito amplio al que nos hemos referido.

a) Los daños consentidos

El consentimiento del daño es la exposición voluntaria de la víctima por medio de una actividad a la que el riesgo es inherente, y tal voluntad debe ponerse de manifiesto de forma previa a que ocurra el daño. Esta situación tradicionalmente ha impedido la posibilidad de declarar la existencia de un daño según el tradicional aforismo *volenti non fit inuiria*.

En el caso de los ciberdaños, existen diversas situaciones que pueden llegar a poner en peligro de forma consciente algún bien o derecho. Y entre ellas podemos destacar las relativas a aquellas acciones en las que la víctima conoce que está asumiendo un riesgo (como puede ser el caso de la navegación en sitios web cuya seguridad se advierte que no está garantizada), o cuando la víctima consiente el daño (al facilitar de forma voluntaria sus claves de acceso).

No obstante, este consentimiento solo se puede prestar sobre aquellos bienes y derechos de carácter disponible, y en ningún caso podrá reconocerse que la víctima ha consentido un daño sobre bienes y derechos cuya naturaleza es indisponible, como el derecho al honor y a la dignidad personal.

Así, es oportuno aplicar a los ciberdaños la doctrina que sobre esta materia ha sentado el Tribunal Supremo, que considera en su sentencia de 20 de diciembre de 2007 que «si el empleado del circo quiere dar de beber a los tigres de bengala abriendo el pestillo de seguridad y metiendo su brazo en la jaula, lo que no puede hacer es reclamar daños y perjuicios porque uno de los animales le arranque el brazo, pues su acción se revela carente de toda prudencia». En este mismo sentido, la jurisprudencia ha distinguido entre la asunción del daño que todo deportista hace cuando practica un deporte de riesgo (STS, 22 de octubre de 1992), de aquellos que son ajenos al riesgo, por lo que no podrá evidenciarse tal asunción (STS, 9 de marzo de 2006).

Actualmente, podemos considerar a los ciberriesgos como un asunto cuyo conocimiento se ha generalizado. Así, es importante destacar que la utilización de cualquier sistema conectado conlleva la asunción de un cierto riesgo inherente por parte de cualquier usuario, cuya delimitación deberá hacerse conforme al principio de la equidad. Y esto es aún más evidente cuando se trata de ciertos ciberdaños en los que es la víctima la que desarrolla una actividad de reconocido peligro como: acceder a contenido ilegal, descargar contenido

de servidores o usuarios desconocidos, conectarse a redes públicas que no garanticen la seguridad, facilitar sus datos de acceso de forma voluntaria en webs cuya seguridad no está garantizada o publicar datos personales.

El criterio de la sentencia de 20 de diciembre de 2007 se puede aplicar a una gran cantidad de situaciones en las que los usuarios conectan sus dispositivos al ciberespacio sin ninguna seguridad, por lo que asumen parte de los daños que puedan llegar a padecer. No obstante, parece lógico que se deberá atender a la entidad del daño y los conocimientos técnicos del usuario para determinar el grado de asunción de dicho riesgo.

En conclusión, aunque es muy extenso el número de ejemplos a los que podríamos hacer referencia sobre la asunción del daño en el ámbito de los ciberriesgos, debe llamarse la atención sobre el siguiente supuesto. Así, aunque sea generalmente conocido que el acceso a una red wifi pública conlleva una serie de riesgos (de tal manera que podríamos afirmar que quien se conecta a ellas asume los riesgos inherentes a una navegación no segura), en ciertos casos como en hoteles, restaurantes o cafeterías el acceso se encuentra restringido a los clientes, quienes tienen que solicitar una contraseña e incluso abonar una cantidad por la utilización de este servicio. Por ello, parece que en estos casos se genera una confianza ficticia en usuario —que además es cliente de este servicio—, quien puede llegar a pensar que de la misma manera que el hotel tiene medidas de seguridad físicas (un guardia de seguridad en la puerta, cámaras…), tendrá medidas de ciberseguridad eficientes en su red wifi, y demás sistemas y elementos que formen parte de las IT.

b) Legítima defensa y estado de necesidad

El actual estado de la ciencia en el ámbito del ciberespacio no nos permite considerar ningún caso en el que se desenvuelvan y produzcan sus efectos las clásicas figuras de la legítima defensa (no se produce la responsabilidad civil porque prima el interés de quien pretende evitar la agresión frente al agresor[395]), y el estado de necesidad (el agente obra para evitar un mal y lesiona con ello un bien jurídico de otra persona[396]). No obstante, ambas situaciones parecen posibles y su desarrollo se puede apreciar en ámbitos muy diferentes.

Así, es posible que, como consecuencia de algún medio de ciberdefensa, pueda resultar dañado algún derecho del atacante (aunque con las técnicas actuales no parece que estas situaciones se lleven a cabo). Y en cuanto al

395 Rogel Vide, *op. cit.*, Civitas, Madrid, 1976, p. 290.

396 Mariano Yzquierdo Tolsada, *op. cit.*, Dykinson, 2015, p. 151.

estado de necesidad, como venimos advirtiendo, el desarrollo del ciberespacio produce que una gran cantidad de elementos del mundo físico dependan de este, por ello cualquier situación de necesidad podría llegar a tener una solución que implique la generación de un ciberevento. En este último caso debemos advertir que uno de los principales elementos del ciberespacio es su carácter global, por lo que las desigualdades socioeconómicas y las incompatibilidades entre la normativa de diversos países podrían plantear conflictos jurídicos a la hora de aplicar el principio del estado de necesidad.

c) El abuso del derecho

La doctrina del abuso del derecho fue admitida por la jurisprudencia española desde la sentencia del Tribunal Supremo de 14 de febrero de 1944 en la que se reconoce que se trata de[397]:

1. El uso de un derecho que externamente puede ser considerado como legal;

2. por medio del que se causa cualquier daño a un interés, no protegido por una específica prerrogativa jurídica;

3. y que manifestada en forma subjetiva u objetiva la inmoralidad o antisocialidad del mismo.

Este principio fue introducido en el párrafo segundo del artículo 7 del Código Civil por medio de la reforma de 1974, que establece:

> «*La ley no ampara el abuso del derecho o el ejercicio antisocial del mismo. Todo acto u omisión que por la intención de su autor, por su objeto o por las circunstancias en que se realice sobrepase manifiestamente los límites normales del ejercicio de un derecho, con daño para tercero, dará lugar a la correspondiente indemnización y a la adopción de las medidas judiciales o administrativas que impidan la persistencia en el abuso*».

El desconocimiento del sentido que tomara la evolución de las IT y el ciberespacio hace, según hemos advertido de forma reiterada, que sea muy difícil legislar sobre cada aspecto o circunstancia que va surgiendo en torno a este ámbito. Por ello, la doctrina del abuso del derecho permitirá exigir la responsabilidad

397 Abuso del derecho, Guías jurídicas, wolterskluwer, http://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAEAMtMSbF1jTAAAUNDYwsLtbLUouLM_DxbIwMDCwNzA7BAZlqlS35ySGVBqm1aYk5xKgB-Pb9sNQAAAA==WKE

correspondiente a aquellos actos que la ley permitía con arreglo a la realidad física, pero que implican un daño si son llevados a cabo en el ciberespacio. Y en este sentido concluye José León Barandiarán que «el derecho no es absoluto, no puede ejercitarse de una manera que lastime los imperativos humanos de solidaridad social y de consideración intersubjetiva»[398].

5.2.2. El daño

El diccionario de la RAE define *dañar*[399] como «causar detrimento, perjuicio, menoscabo, dolor o molestia» que, según Díez-Picazo, se asienta en que el objeto que lo padece se encuentre protegido por el ordenamiento jurídico, cuya calificación no puede dejarse en manos del criterio subjetivo del juzgador[400]. Por ello, advierte el referenciado autor que hay que atender a un concepto del daño que englobe e incorpore los factores que permitan evaluarlo y repararlo[401].

En este sentido, la doctrina del Tribunal Supremo mantiene que el daño debe ser cierto, actual y determinado o determinable, para lo que exige que se cumplan una serie de elementos que se pueden resumir conforme a los siguientes pronunciamientos:

- «Los perjuicios han de tener existencia real al tiempo que se ejercita la acción. Por tanto, la simple eventualidad del daño no basta para exigir una responsabilidad» (sentencia del Tribunal Supremo de 9 de abril de 1996).

- «La determinación del importe cierto del perjuicio sufrido requiere que se acredite debidamente la existencia del mismo y su valor, y que se hubiere ocasionado realmente, porque no cabe en modo alguno suponerlo habido o derivado de meras posibilidades de inseguros resultados y desprovistas de certidumbre» (S. de la Audiencia Territorial de Albacete de 4 de julio de 1980).

- «El daño indemnizable, cuando de acción de responsabilidad civil se trata, ha de ser cierto y la prueba de su realidad corresponde a quien reclama su indemnización, sin que pueda admitirse la existencia de perjuicios

398 José León Barandiarán, «Comentarios al Código Civil peruano», *Rev. Derecho y Ciencias Políticas*, Año XII, n° 2, en Enrique Cuentas Ormachea, «El abuso del derecho», p. 469, https://dialnet.unirioja.es/ descarga/articulo/5085322.pdf

399 Dañar, *Diccionario de la Lengua Española*, RAE, http://dle.rae.es/?id=BrdY6Ro

400 L. Díez-Picazo y A. Guillón Ballesteros, *Sistema de Derecho Civil*, editorial Tecnos, Madrid, 9.ª edición, 2005, vol. II, p. 545.

401 L. Díez-Picazo, *op. cit.*, 2011, p. 329 y ss.

puramente hipotéticos o eventuales» (sentencia del Tribunal Supremo de 11 de febrero de 1993).

- «La Jurisprudencia tiene declarado que para condenar por daños y perjuicios hay que probar su existencia» (sentencia del Tribunal Supremo de 1 de abril de 1996).

- «La carga de la prueba corresponde al reclamante del daño cuando le resulta disponible la misma. (...) Al faltar tal presupuesto necesario, no puede prosperar la acción por culpa extracontractual» (sentencia del Tribunal Supremo de 21 de febrero de 2003).

- «La obligación de indemnizar daños y perjuicios no es una consecuencia necesaria del incumplimiento atribuido a uno de los contratantes, sino que para que nazca y sea exigible, ha de demostrarse la realidad de producción de aquellos, sin que la obligación indemnizatoria pueda derivarse de perjuicios solo posibles» (sentencia del Tribunal Supremo de 28 de diciembre de 1995).

- «No puede basarse la apreciación de la producción de los perjuicios en supuestos meramente posibles pero de resultados inseguros, ni hasta que se demuestre la realidad de los perjuicios causados para que pueda hacerse efectiva la indemnización de los mismos, sino que es preciso, además, que su cuantía quede determinada» (sentencia del Tribunal Supremo de 22 de junio de 1982).

Una de las principales particularidades del ciberespacio es la existencia de múltiples bienes y derechos que pueden resultar afectados por un ciberevento. Y entre ellos podemos encontrar elementos dependientes de la realidad física o exclusivamente cibernéticos. De tal forma, los bienes y derechos que en este ámbito son susceptibles de padecer algún género de daño constituyen una realidad cambiante que depende del estado y desarrollo de las IT. Y en este sentido entiende el informe de The Institute of Risk Management por «cyber risk» cualquier riesgo o pérdida financiera, amenaza o daño para la reputación que resulte de un fallo de seguridad en las IT[402].

No obstante, parece esencial establecer una serie de pautas conforme a las que se puedan clasificar los bienes y derechos que resultan amenazados por los ciberriesgos, por lo que podemos dividirlos conforme a cuatro grupos:

402 *Cyber Risk*, The Institute of Risk Management, CGI, IRM (2014), p. 8, https://www.theirm.org/media/883443/Final_IRM_Cyber-Risk_Exec-Summ_A5_low-res.pdf

- **Cuestiones de interés general y seguridad nacional**, que se relacionan principalmente con el ciberterrorismo, la *cyberwarfare* y el *cyberhacktivism*. Y plantean diversas dudas en torno a la forma con la que deben de colaborar la industria aseguradora y el Estado en lo relativo a las estructuras críticas, la acumulación del riesgo y la posible suscripción obligatoria de ciberseguros.

- **La protección de los datos,** que es un pilar fundamental para el desarrollo de la ciberseguridad y la responsabilidad sobrevenida de la misma. Además, dentro de estos se pueden distinguir entre datos en sentido general («toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información, incluidos los programas que sirven para hacer que dicho sistema de información realice una función» —Decisión Marco 2005/222/JAI de 24 de febrero—) y datos personales.

- Las estructuras y sistemas que configuran y participan del ciberespacio forman el ámbito físico del mismo, por lo que se encuentran expuestos a sufrir un daño o menoscabo material cuya protección ha sido regulada por diversas normas entre las que destaca la Directiva 2013/40/UE de 12 de agosto de 2013, la Directiva 2016/1148 de 6 de julio de 2016 y la regulación relativa a las infraestructuras críticas.

  En particular, el desarrollo de las IT por medio de sistemas como el IoT pone de manifiesto la posibilidad cada día más evidente de que los ciberriesgos ocasionen cualquier tipo de daño físico o material sobre cualquier elemento conectado al ciberespacio. De tal forma, han supuesto la formación de importantes barreras en términos de ciberseguridad y la creación de nuevos riesgos y amenazas[403].

- **Los daños inmateriales,** entre los que destaca la paralización o el funcionamiento erróneo de determinadas infraestructuras y sistemas conectados, y los daños relativos a la pérdida de reputación y prestigio profesional.

La clasificación de los daños ha sido una materia especialmente controvertida para la doctrina, que ha llegado a reconocer un número muy extenso de situaciones. En este sentido, vamos a hacer referencia a los conceptos de mayor utilidad según la clasificación seguida por Mariano Yzquierdo, de los que nos valdremos para aportar ejemplos de daños que puedan ser ocasionados por un ciberevento:

403 Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination, Digital Agenda for Europe, European Commission DG Communications Networks, Content & Technology, p. 9, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9472

- En materia exclusivamente de responsabilidad civil contractual, podemos distinguir entre:

    a. Por un lado, los daños al interés contractual positivo (aquel que pretende que se le entregue la cosa objeto del contrato aunque sea tarde —como en el caso del retraso de un avión por un fallo en los sistemas—); y negativo (aquel que pretende la resolución e indemnización —como en el caso de la pérdida datos o información almacenados en los servidores de un proveedor—).

    b. Y por otro lado, los daños intrínsecos (el propio objeto del contrato resulta dañado como la pérdida de unas fotos por un ciberevento que afecta al ordenador del fotógrafo) o extrínsecos (el daño recae sobre aquello que no ha sido el objeto de contrato, como en el caso en el que los sistemas de una empresa sufren un ciberataque como consecuencia de haberse sincronizado a los de un proveedor —siempre que este no se encargue del mantenimiento o seguridad de dichos sistemas—).

- Daños presentes o futuros. Los daños presentes son aquellos cuya existencia necesariamente ha de resultar probada como la destrucción de un equipo informático como consecuencia de un ciberevento. Y los daños futuros son aquellos por los que se considera con seguridad que en el futuro se tendrá que incurrir en una serie de gastos como consecuencia de las secuelas permanentes que ya se conocen. Uno de los ejemplos más característicos son los gastos médicos para el tratamiento de secuelas físicas permanentes, que en el ámbito de los ciberriesgos pueden haber derivado de un accidente laboral por el fallo de las medidas de seguridad que dependían de las IT.

- Daño continuado, Roca Trías se refiere a aquellos «perjuicios causados por una conducta dañosa que persiste, de producción sucesiva o ininterrumpida»[404]. No obstante, parece más adecuada la explicación de Mariano Yzquierdo para quien lo que persiste es el daño y no la conducta que lo produce, como el caso de los gastos que durante un tiempo deberá realizar una empresa por la pérdida de reputación sobrevenida de un ciberataque. Esta deberá ser evaluada periódicamente tras el siniestro, y las labores para recuperar tal pérdida se extenderán hasta que se alcancen los niveles previos.

- Daños directos o indirectos. Los primeros se refieren a aquellos daños que se producen como consecuencia inmediata y directa del actuar de un

404 E. Roca Trías y M. Navarro Michel, *Derecho de Daños*, Tirant lo Blanch, Valencia, 6.ª ed., 2011, p. 199.

agente (los daños físicos que sufre aquel que es atropellado por un vehículo de conducción autónoma que ha sufrido un ciberevento); y los segundos ocasionan consecuencias indirectas o remotas a terceros (el daño sufrido por los hijos de aquel que fue atropellado por el vehículo autónomo y falleció).

- Daño emergente y lucro cesante, que conforme al artículo 1106 del CC se puede distinguir en aquella pérdida efectivamente sufrida («la disminución de los valores patrimoniales que el perjudicado tenía en su haber»[405]) y las ganancias dejadas de obtener[406]. Como ejemplo, supongamos que la negligencia de una empresa de mantenimiento informático causa un ciberevento a un cliente. En este caso, los gastos para la recuperación del sistema del cliente y su reputación serán el daño emergente, y las ventas que este pierda como consecuencia de aquella situación constituirán el lucro cesante.

- La pérdida de oportunidad consiste en la pérdida de la esperanza de una ganancia o situación futura de cuya existencia no podemos tener una certeza total. Este se produce en el caso de que un procurador no pueda presentar a tiempo un recurso por haber sufrido un ciberevento en sus sistemas que se lo impida.

- Daño patrimonial, daño corporal y daño moral. El primero representa a un perjuicio que afecta directamente a la propiedad o cualquier otro derecho de naturaleza patrimonial[407] como el robo mediante la obtención de los datos bancarios por medio de malware, ingeniería social… Y, por el contrario, los daños corporales y morales producen un menoscabo personal que afecta a la integridad física (el daño que sufre un paciente tras padecer un error en una operación como consecuencia de un ciberevento en los sistemas de control de la maquinaria médica utilizada) o al ámbito interno y psicológico, cuya desbocada extensión ha criticado Díez-Picazo[408] (el padecimiento psicológico que ocasionan a aquel paciente las secuelas del error).

Además de todos los daños hasta aquí vistos podemos hacer una especial referencia a aquellos que desenvuelven sus efectos con particular relevancia en el ciberespacio, entre los que destacan los relativos a la pérdida o robo de datos personales y los que afectan a bienes exclusivamente cibernéticos.

---

405 E. Roca Trías y M. Navarro Michel, *op. cit.*, p. 196.

406 E. Roca Trías y M. Navarro Michel, *op. cit.*, p. 197.

407 L. Díez-Picazo y A. Gullón Ballesteros, *Sistema de Derecho Civil*. Ed. Tecnos, Madrid, 9.ª ed., 2005, vol. II, p. 546.

408 L. Díez-Picazo y A. Gullón Ballesteros, *op. cit.*, p. 547.

a) La pérdida o robo de datos personales

El artículo 19 de la Ley Orgánica de Protección de Datos establece que «los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados». No obstante, la Ley Orgánica de Protección de Datos no establece criterios propios para la adecuada determinación del daño, por lo que se deberá atender a los principios generales de la responsabilidad civil[409].

En este sentido, el artículo 82 del Reglamento 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos determina que «toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos».

El artículo 19.1 de la LOPD condiciona el derecho de indemnización por daños a que este haya sido producido como consecuencia del incumplimiento de la regulación en materia de protección de datos. No obstante, el mencionado reglamento permite que el «responsable o encargado del tratamiento» se exonere de responsabilidad al introducir en el artículo 82.3 que «estará exento de responsabilidad en virtud del apartado 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios». Además, parece evidente que, a pesar de la contravención legal producida, puede no haberse producido un daño efectivo, lo que pone de manifiesto que el derecho al resarcimiento no surge de forma automática, necesaria y objetiva en el artículo 19. En todo caso, el daño cuyo resarcimiento se pretenda deberá acreditarse convenientemente, para lo que el artículo 19 establece una presunción *iuris tantum* por la que se entiende que se ha producido el daño siempre que haya una intromisión ilegítima de los derechos fundamentales que tutela la LOPD.

Por otra parte, dependiendo de la naturaleza jurídica subyacente, el vínculo que relaciona al perjudicado con el responsable tendrá carácter contractual o extracontractual. Y en cuanto a la posible consideración del daño como patrimonial o moral, Javier Puyol afirma que la doctrina no es pacífica en este punto, pero que parece considerarse de forma mayoritaria que se tratan de daños de naturaleza moral amparados por una presunción *iuris et de iure*.

409 Unai Aberasturi Gorriño, *Revista Aragonesa de Administración Pública*, nº 41-42 (2013), Zaragoza, pp. 179-180, http://w.aragon.es/estaticos/GobiernoAragon/Organismos/InstitutoAragonesAdministra cionPublica/Areas/03_Revista_Aragonesa_Formacion/04%20Unai%20Aberasturi.pdf

En este sentido, existe una corriente doctrinal que considera que se tratan de daños morales no por el carácter objetivo del bien, sino porque este no podrá ser restituido por medio de la entrega de una suma dineraria «por falta de una relación de equivalencia entre esta y aquel». Y los criterios para determinar la indemnización han sido establecidos por la doctrina del Tribunal Supremo por la sentencia de 19 de abril de 2002 —entre otras—, que hace referencia a diversos criterios tales como las circunstancias del daño, la gravedad del caso y la valoración del beneficio obtenido por el causante del daño.

Y en todo caso parece haber reconocido la doctrina (Atienza Navarro y Orti Vallejo, entre otros) que la dificultad de probar el daño moral no obsta para que el demandado tenga la posibilidad de probar que el incumplimiento no causó un daño, ya que existen casos en los que esta circunstancia puede ocurrir. Por ello, con independencia de que se traten de daños morales, la presunción que recoge el artículo 19 de la LOPD debe aceptar prueba en contrario[410], como sucede en caso de los daños contra el derecho al honor[411].

Finalmente, el Reglamento 2016/679, de 27 de abril de 2016, trata de garantizar el resarcimiento de los daños que se ocasionen como consecuencia de esta clase de incumplimientos mediante la introducción de un régimen de responsabilidad solidaria. De tal forma, el párrafo 5 de su artículo 82 dice que cada uno de los responsables o encargados del tratamiento de datos «será considerado responsable de todos los daños y perjuicios» con independencia de su grado de participación. Y ello, sin perjuicio de que pueda acreditar que «no es en modo alguno responsable del hecho» —artículo 82.3— y de su derecho de repetición contra el resto de responsables —artículo 82.5—.

b) El ciberdaño o perjuicio a bienes exclusivamente cibernéticos

El ciberespacio ha supuesto la creación de nuevas realidades, derechos y bienes que en muchos casos tienen un carácter intangible y dependen de la percepción subjetiva e interna de un grupo de sujetos. Por ello, resulta importante analizar qué tipo de daños se podrán poner de manifiesto en torno a estos bienes cibernéticos.

Un caso que refleja estas particularidades fue el acontecido en La Haya (Holanda) en 2007 cuando dos adolescentes utilizaron su avatar del juego de

410 Javier Puyol, «El ejercicio del derecho a la indemnización derivado del art. 19 de la LOPD», ECIXGROUP (3 de diciembre de 2014), http://ecixgroup.com/el-grupo/el-ejercicio-del-derecho-la-indemnizacion-derivado-del-art-19-de-la-lopd/

411 J. R. De Verda y Beamonte, *Veinticinco años de aplicación de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a La Intimidad Personal y Familiar y a la Propia Imagen*, ed. Thomson-Aranzadi, Cizur Menor (Navarra), 2007, p. 288.

multijugador MMORPG para amenazar a otro que, bajo tales amenazas, atendió a las peticiones de aquellos y dejó a la disposición de su avatar dos objetos del juego (una máscara y un amuleto). En este punto es importante destacar que el modelo comercial que plantea este tipo de videojuegos denominado *free-to-play* permite adquirir elementos del juego por medio de méritos o comprarlos. En torno a estos videojuegos *online* han surgido grupos de usuarios que intercambian avatares y elementos del juego, lo que en 2013 alcanzó en EE. UU. un volumen de transacciones de 2.900 millones de USD.

La defensa de los agresores alegó que la máscara y el amuleto no eran objetos tangibles o materiales, por lo que consideraba que carecían de valor económico. No obstante, el Tribunal Supremo de Holanda condenó a estos a resarcir el daño causado por considerar que «los bienes tienen un valor intrínseco para el demandante por el tiempo y energía que invirtió en su recolección dentro del juego»[412].

Una situación similar se produjo en 2003 en China cuando un joven denunció el robo de una serie de elementos del videojuego Redmoon, reclamando que se exigiera a la empresa gestora de este que revelara la identidad del culpable, le devolviera los elementos sustraídos[413], además del resarcimiento del daño moral que le había sido causado.

En este mismo sentido se plantea la reciente investigación del FBI por el acceso no autorizado a los sistemas de la compañía de videojuegos EA con el que un grupo de *hackers* conseguía obtener dinero virtual del videojuego FIFA, que posteriormente cambiaba a otros usuarios por monedas de curso legal[414].

Los ejemplos antes mencionados reflejan las características principales de los daños contra bienes y derechos cuyos efectos se limitan al ámbito del ciberespacio. Así, el desarrollo del ciberespacio y las relaciones entre los agentes que operan en él han llevado a la creación de diversos instrumentos que, aunque no gocen de realidad corpórea ni formen parte de los tradicionales derechos sobre bienes tangibles, producen unos efectos muy importantes en el ámbito socioeconómico mundial.

Así, la moneda del videojuego FIFA o un amuleto del MMORPG no son más que una combinación numérica generada por el software del videojuego, pero pueden alcanzar un valor de gran relevancia económica y personal.

---

412 Agustín Salaberry, «Robo de bienes virtuales genera condena en vida real», Hipertextual.com (31 de enero de 2012), https://hipertextual.com/2012/01/robo-de-bienes-virtuales-genera-condena-en-vida-real

413 «Denuncia a una empresa de juegos *online* por 'robarle sus armas biológicas' », EFE, Navegante.com, http://www.elmundo.es/navegante/2003/11/20/juegos/1069320761.html

414 «El FBI investiga una estafa millonaria a través de los videojuegos FIFA», *El Mundo* (16 de noviembre de 2016), http://www.elmundo.es/tecnologia/2016/11/16/582c289046163f820d8b460b.html

Por ello, es difícil afirmar con rotundidad que su pérdida no ocasiona un verdadero perjuicio económico, como mantenía la defensa de quien sustrajo el amuleto y la máscara, aunque sea sin perjuicio de su carácter intangible. La RAE define que un bien intangible es aquel que «no debe o no puede tocarse», pero ello no impide que sean económicamente valorables y que su pérdida produzca un verdadero daño patrimonial y moral.

En sentido propio, se puede considerar como intangible cualquier producto de la mente o de la conciencia que pueda ser manifestado de forma externa y que de alguna forma pueda ser monopolizado[415]. Además, los bienes intangibles pueden ser objeto de propiedad, siempre que estén dotados de alguna utilidad que permita satisfacer ciertas necesidades o interés, y que se encuentren dentro de los límites del tráfico jurídico —definido, entre otros, por los artículos 33.2, 35, 38 y 53,1 de la Constitución Española—[416].

Por otra parte, considera Nieto Sánchez que los bienes intangibles pueden ser considerados como patrimonio, y esto siempre que cumplan con las características que definen la naturaleza patrimonial del bien[417]. Así, deberemos excluir a los bienes y derechos que no tienen un contenido económico con la excepción de aquellos cuya lesión produce un derecho de resarcimiento —que forma parte del patrimonio de su titular—, y aquellos que no puedan ser identificados e individualizados, o sobre los que no se pueda ostentar ningún género de derecho.

No obstante, en contra del planteamiento seguido por Miró Echevarne[418], podrá reconocerse un régimen de protección concreta a los bienes inmateriales o intangibles aunque no hayan sido recogidos expresamente por la ley, ya que cualquier objeto lícito que surja de la autonomía de la voluntad se encuentra amparado por el ordenamiento jurídico español conforme a los límites y particularidades pactadas.

El daño patrimonial ha sido definido por Díez-Picazo como aquel que afecta directamente a la propiedad o a cualquier otro derecho de naturaleza patrimonial.

---

415 J. L. Lacruz Berdejo, «Elementos de Derecho Civil», tomo III. *Derechos Reales*. Librería Bosch, Barcelona, 1980, pp. 339-344, en Manuel Miró Echevarne, «Sessió 5: Els intangibles i la seva importancia jurídica, IAFI-IX Seminari», *Finances* (24 de febrero de 2006), p. 1, http://www.ub.edu/iafi/Recerca/Seminaris/miro.pdf

416 V. L. Montes, «Notas preliminares sobre la protección jurídica de los bienes inmateriales», *Revista General del Derecho*, nº 544-545, enero-febrero de 1990, pp. 442-446, en Manuel Miró Echevarne, *op. cit.*, p. 2, http://www.ub.edu/iafi/Recerca/Seminaris/miro.pdf

417 J. Nieto Sanchez, «El patrimonio profesional: su concepto, composición y transmisión», «El patrimonio familiar, profesional y empresarial», Bosch Casa Editorial S.A., Madrid, 2005, Capítulo 27, pp. 867-939, en Manuel Miró Echevarne, *op. cit.*, p. 4, http://www.ub.edu/iafi/Recerca/Seminaris/miro.pdf

418 Manuel Miró Echevarne, *op. cit.*, p. 5, http://www.ub.edu/iafi/Recerca/Seminaris/miro.pdf

En este sentido, el derecho que un usuario de un videojuego tiene sobre los elementos del juego (máscaras, amuletos o moneda ficticia…) queda sometido a las condiciones pactadas entre la empresa del videojuego y el usuario. Por ello, no puede afirmarse que en todos los casos el usuario tenga un verdadero derecho de propiedad sobre los objetos del juego. Y esto se puede extender a cualquier plataforma o aplicación conectada al ciberespacio en la que existan elementos intangibles que tengan alguna utilidad concreta. No obstante, la definición del referenciado autor permite considerar como patrimonial al daño que afecte a cualquier otro derecho de naturaleza patrimonial, de manera que el limitado derecho a la utilización de los elementos del juego podría alcanzar este carácter.

En todo caso, tendrá que existir una relación de naturaleza patrimonial entre el usuario y los elementos del juego frente a los que de forma más o menos limitada ostenta algún derecho. Y en concreto deberá poder considerarse que tales bienes forman parte del patrimonio del usuario, lo que no resulta difícil si entendemos, como hace la RAE, que el término «patrimonio» se refiere el conjunto de los bienes y derechos propios adquiridos por cualquier título, y el conjunto de bienes pertenecientes a una persona natural o jurídica, o afectos a un fin, susceptibles de estimación económica. Así, el usuario adquiere los elementos del juego, aunque lo haga para el uso acordado en las condiciones del mismo y con los límites materiales y físicos de este. Además, los elementos que forman parte de cualquier sistema o aplicación conectada con el ciberespacio siempre podrán definirse como conjunto de bienes —intangibles— afectos a un fin.

Y esto, con independencia de los acuerdos que puedan existir entre los usuarios y las empresas que producen y gestionan tales aplicaciones o programas.

Llegados a este punto, parece evidente que los aspectos más relevantes para el estudio de los ciberdaños giran en torno a la justificación de la relevancia económica y personal del bien cibernético, la determinación y existencia del daño, y la atribución del sujeto que sufre los perjuicios de su pérdida con independencia del título que ostente sobre el mismo.

Así, para valorar el daño deberemos atender a la utilidad económica del objeto, el interés personal y las particularidades del derecho que los usuarios ostentan sobre los elementos objeto del ciberdaño.

Y dentro de estas categorías podemos hacer referencia a las dos clases de daños que distingue la doctrina mayoritaria[419], y que también podrán producirse por la pérdida o deterioro de los bienes y derechos exclusivamente cibernéticos:

419 Ramón Maciá Gómez, «La dualidad del daño patrimonial y del daño moral», *Revista de Responsabilidad Civil y Seguro*, p. 22, http://asociacionabogadosrcs.org/doctrina/rc36doctrina2.pdf

1. **El daño patrimonial.** Se ha considerado desde un punto de vista extensivo que incluye el perjuicio patrimonial directo e indirecto. El primero se refiere a cualquier género de pérdida, deterioro o detrimento que sufra cualquier bien que pueda ser objeto de comercio[420]. Así, podemos mencionar el caso de los elementos que forman parte de un videojuego (como el referenciado amuleto), que puedan ser valorables económicamente (por ejemplo, por haber sido adquiridos a cambio de un precio en moneda de curso legal), y tal valor determinará la pérdida patrimonial sufrida si se pierde o deteriora como consecuencia de la acción de un tercero.

   Y el segundo comprende todos aquellos gastos en los que el perjudicado incurre para reparar o reponer los bienes o elementos que padecieron el daño (daño emergente), como por ejemplo la pérdida de archivos por cuya descarga tuvo que abonar una cantidad. Además de las ganancias frustradas (lucro cesante) como consecuencia de la pérdida y deterioro de un bien, como el valor por el que se pretendía vender una cuenta con una gran relevancia dentro de una determinada red social.

2. **Los daños morales** han sido reconocidos por la doctrina jurisprudencial del Tribunal Supremo desde la sentencia de 6 de diciembre de 1912, que se refería a ellos como un perjuicio contra la honra y el honor de quien lo padecía. Posteriormente, la sentencia del Tribunal Supremo de 28 de febrero de 1959 recogió una definición más actual al considerar que son aquellos que «se refieren al patrimonio espiritual, a los bienes inmateriales de la salud, el honor, la libertad y análogos, que son los más estimados y por ello más sensibles, más frágiles y más cuidadosamente guardados».

   En este mismo sentido, el artículo 11 de la resolución 75/7 del Comité de Ministros del Consejo de Europa considera que «la víctima debe ser indemnizada del perjuicio estético, de los dolores físicos y de los sufrimientos psíquicos. Esta última categoría comprende, en cuanto que concierne a la víctima, diversas perturbaciones y desagrados tales como malestares, insomnio, sentimiento de inferioridad, una disminución de los placeres de la vida causada especialmente por la imposibilidad de dedicarse a ciertas actividades de agrado». Mariano Yzquierdo distingue las modalidades de daño moral reconocidas por la doctrina francesa (que ha estudiado con dedicación este asunto), entre las que destaca: la pérdida del agrado o la dificultad para realizar los gestos de la vida cotidiana (ARCADIO, MOULAY y CHAUVINE, 1973), el perjuicio estético (VICENTE DOMINGO, 1994: 203), el perjuicio de afecto (DOMÍNGUEZ HIDALGO, 2000) y el *pretium doloris*[421].

---

420 Ramón Maciá Gómez, *op. cit.*, p. 22, http://asociacionabogadosrcs.org/doctrina/rc36doctrina2.pdf

421 Mariano Yzquierdo Tolsada, *op. cit.*, Dykinson, 2015, pp. 177-180.

Estos daños morales deben ser económicamente valorables, y para ello la sentencia del Tribunal Supremo de 21 de octubre de 1996 establecía que:

«Si bien es cierto que el precepto civil 1106 del Código Civil establece la forma normativa para regular los daños y perjuicios de condición exclusivamente material, no lo es menos ante la concurrencia de efectivos daños de no apreciación tangible —los llamados daños morales—, cuya valoración no puede obtenerse de una prueba objetiva, habiendo resuelto la jurisprudencia que su cuantificación puede ser establecida por los tribunales en los que cabe comprender los siguientes: toda la gama de sufrimientos y dolores físicos o 1.º) psíquicos que haya padecido la víctima a consecuencia del hecho ilícito... 2.º) moral, cualquier frustración, quebranto o ruptura en los sentimientos, lazos o afectos, por naturaleza o sangre que se dan entre personas allegadas fundamentalmente por vínculos parentales... Ahora bien, se puntualiza que en la integración de este daño moral, lo que se trata de incorporar a este concepto no son las privaciones materiales o alimenticias que, a consecuencia de dichas lesiones o muerte, pueden padecer las personas o supervivientes que estuviesen bajo la tutela, custodia o el estipendio económico del lesionado o fallecido, porque obvio es que tales contingencias se ubicarán dentro del campo de los daños corporales en general, o materiales en su modalidad de perjuicios; y es que lo que se pretende sustantivizar como daño moral es el dolor inferido o el sufrimiento, tristeza, angustia o soledad padecida por las personas ante ese hecho ilícito».

En la actualidad, dentro de las posibles circunstancias de las que puede sobrevenir un daño moral, pueden destacarse los daños al derecho al honor por su especial relevancia en las relaciones del ciberespacio. Así, Díez-Picazo considera que «el valor o bien jurídico protegido por el derecho al honor es el aprecio social, la buena fama, la reputación; en una palabra, el merecimiento a los ojos de los demás»[422], que en un ámbito plenamente libre y sin barreras como es el ciberespacio, en el que la información fluye con una enorme facilidad, puede resultar expuesto a un mayor número de riesgos.

Este planteamiento permitirá a las personas jurídicas obtener un derecho de resarcimiento por los daños y perjuicios que se les haya causado más allá de aquellos que sean puramente materiales o patrimoniales. Y ello, sin necesidad de contradecir la máxima comúnmente aceptada (SAP Madrid 423/2007, de 5 de julio de 2007) de que las personas jurídicas al no

422 L. M. Díez-Picazo Giménez, *Sistema de derechos fundamentales*, Thomson-Civitas, Cizur Menor (Navarra), 3.ª edición, 2008, p. 310.

tener sentimientos no pueden sufrir daño moral[423]. Así, no será necesario mantener un argumento artificial sobre los daños morales de las personas jurídicas —daños morales impropios—[424], ya que la presunción del artículo 9.3 de la Ley Orgánica 1/82 permite la tutela del derecho al honor sin daño moral.

Por ello, ya no habrá ningún obstáculo para la protección del derecho al honor de las personas jurídico-privadas[425] (como viene reconociendo la jurisprudencia desde la Sentencia del Tribunal Supremo 1119/2007, de 31 de octubre) que entre otras formas se manifiesta por medio del prestigio profesional (como se mantiene en las sentencias del Tribunal Supremo 63/2005, de 18 octubre de 2005, y de la Audiencia Provincial de Madrid 487/2006, de 26 de octubre de 2006)[426] o la imagen corporativa.

Así, asegura Ramón Maciá que el daño moral viene a ser subsidiario del daño material, ya que no existe ninguna configuración específica del concepto, y carece de toda consistencia si no es alegado y comprobado por la víctima. Pero, además, un mismo daño puede llegar a ser calificado de material o moral, ya que la línea fronteriza de ambas categorías es muy difusa[427].

En estos casos, la principal dificultad procede de la obligación de probar la existencia del daño (217.2 LEC) cuyos efectos materiales o patrimoniales en el ámbito de la realidad física pueden ser evidentes. Así, de un ciberevento podrán resultar daños materiales o morales, como puede ser el perjuicio por la amputación de un miembro tras haber sufrido un accidente en un coche autónomo que haya sido consecuencia de un fallo en el sistema de guía en la conducción.

No obstante, los perjuicios morales que se pongan de manifiesto como consecuencia exclusiva de un ciberdaño resultan mucho más difíciles de probar, ya que se tratan de daños intangibles, que a su vez son ocasionados por el deterioro de bienes cibernéticos que también son intangibles.

En el caso de la pérdida de datos personales, en EE. UU. ya son habituales las demandas colectivas por los daños y perjuicios. Así, uno de los supuestos más

423 A. M. Rodríguez Guitián, *El derecho al honor de las personas jurídicas*, Montecorvo, Madrid, 1996, pp. 103-104.

424 A. M. Rodríguez Guitián, *op. cit.*, 1996, p. 109 y ss.

425 Javier Gómez Garrido, «Derecho al honor y persona jurídico-privada», *REDUR 8* (diciembre de 2010), p. 218.

426 M. Rovira Suerio, *La responsabilidad civil derivada de los daños ocasionados al derecho al honor, a la intimidad personal y familiar y a la propia imagen*, Cedecs Editorial S.L., Barcelona, 1999, p. 112 y ss.

427 Ramón Maciá Gómez, «La dualidad del daño patrimonial y del daño moral», *Revista de Responsabilidad Civil y Seguro*, p. 31, http://asociacionabogadosrcs.org/doctrina/rc36doctrina2.pdf

relevantes ha sido el caso de la web de citas Ashley Madison (de la que fueron robados y desvelados los datos de 37 millones de usuarios[428]), propiedad de una compañía canadiense contra la que se han dirigido diversas demandas individuales y colectivas (entre ellas destaca una demanda colectiva en Canadá por la que se reclaman 578 millones de USD[429]).

El caso es particularmente interesante para nuestro estudio porque se tratan de reclamaciones por daños morales por responsabilidad contractual como consecuencia del incumplimiento de las condiciones pactadas (ya que en ciertos casos los usuarios pagaban una cuota para que se garantizase la seguridad y privacidad de sus datos), además de las reclamaciones en materia de incumplimiento de la legislación de protección de datos personales. No obstante, aún tendremos que esperar a que se publiquen las primeras resoluciones judiciales sobre el asunto.

Los supuestos de daños morales por la pérdida y el robo de datos personales no plantean la misma dificultad probatoria que los anteriormente estudiados daños a bienes cibernéticos, y sus circunstancias han sido ampliamente desarrolladas en el sentido al que ya nos hemos referido. Así, debemos advertir de la extrema dificultad que tiene la prueba de la existencia y la entidad de los ciberdaños morales, ya que en ciertos casos (con la excepción del daño patrimonial y material ya estudiados) se tratan de daños intangibles sobre bienes que también son intangibles. Y en este sentido podemos hacer referencia a diversos ejemplos:

a. El daño que puede sufrir el usuario de un videojuego al que le sustrajeron un elemento que utilizaba su avatar para cuya obtención había dedicado mucho tiempo y esfuerzo.

b. La pérdida del estatus, prestigio o la categoría en un videojuego, red social o cualquier otra plataforma del ciberespacio.

c. El padecimiento por la pérdida de las fotos cuya única copia dañó o borró un ciberevento.

La sentencia del Tribunal Supremo de 10 de febrero de 2006 considera que «en efecto, se viene manteniendo que la reparación del daño o sufrimiento moral, que no atiende a la reintegración de un patrimonio, va dirigida, principalmente,

428 «Ashley Madison hack reveals IT 37 million users deepest sexual fantasies», *Independent* (20 de agosto de 2015), http://www.independent.co.uk/life-style/love-sex/ashley-madison-hack-reveals-IT-37-million-users-deepest-sexual-fantasies-10463985.html

429 «Trial lawyers circle Ashley Madison», *The Hill* (29 de agosto de 2015), http://thehill.com/policy/cybersecurity/252203-trial-lawyers-circling-ashley-madison

a proporcionar en la medida de lo humanamente posible una satisfacción como compensación al sufrimiento que se ha causado, lo que conlleva la determinación de la cuantía de la indemnización apreciando las circunstancias concurrentes»[430]. Por ello, no podrá olvidarse que existe una gran cantidad de acciones que tienen lugar en el ciberespacio y que despliegan sus efectos en la realidad física, donde las circunstancias individuales de cada persona pueden poner de manifiesto cualquier tipo de padecimiento en el ámbito psicológico e interno.

El carácter intangible de los ciberdaños nos permite hacer referencia a una gran cantidad de ejemplos de potenciales daños entre los que se encuentran los señalados anteriormente. Así, como venimos advirtiendo reiteradamente, el ciberespacio ha creado un ámbito en el que diversos sujetos interactúan y desarrollan sus derechos y libertades generando relaciones y conflictos. Y todo ello tiene unos evidentes efectos jurídicos que se pueden poner de manifiesto tanto en el ciberespacio como en el ámbito de la realidad física, con independencia de la entidad que aparentemente tenga el hecho que los origine.

5.2.3. La causalidad

La causalidad es otro de los elementos fundamentales de la responsabilidad, por medio del cual se determina si entre el hecho del agente y el daño producido existe una relación de causa-efecto. En este sentido mantiene Mariano Yzquierdo que sin llegar a confundirse el juicio de causalidad con el de imputación —que analizaremos en el siguiente apartado— es conveniente que se realicen al mismo tiempo para poder atender a todos los matices y circunstancias subjetivas que intervinieron en la producción del daño.

De esta forma, parece esencial realizar un análisis pormenorizado de las acciones y omisiones que coadyuvan en el ciberespacio, ya que constituye una realidad múltiple que se desenvuelve en dos ámbitos completamente diferenciados: por un lado, está compuesto de una serie de sistemas físicos formados por las infraestructuras de telecomunicaciones, y todos los elementos y sistemas conectados a las mismas —como los que forman parte del IoT—; y por otro lado, 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.

Así, este ecosistema digital configura un nuevo medio en el que bienes y derechos de toda índole pueden llegar a resultar amenazados e incluso sufrir algún daño, menoscabo o deterioro. Por ello, resultará esencial la determinación del nivel de diligencia y seguridad al que los diferentes sujetos deben

430 Ramón Maciá Gómez, *op. cit.*, p. 28, http://asociacionabogadosr cs.org /doctrina/rc36doctrina 2.pdf

ajustar su comportamiento para impedir que de una u otra forma se ponga en riesgo la integridad de todo el ciberespacio[431].

La doctrina y la jurisprudencia han discutido sobre los requisitos que son necesarios para apreciar la causalidad al pasar de la amplísima causalidad próxima, a la doctrina de la causalidad adecuada, formulada en 1888 por el filósofo Von Kries (1889: 529 y ss.). Por medio de esta doctrina, se entiende que solo concurre una relación de causalidad cuando el daño puede asociarse a los antecedentes que según el curso normal de los acontecimientos han sido la causa directa e inmediata del mismo[432]. No obstante, la doctrina de la causalidad adecuada se ha ido oportunamente matizando desde la sentencia del Tribunal Supremo de 22 de octubre de 1948 («en la culpa extracontractual la determinación del nexo causal entre la conducta del agente y el daño producido ha de inspirarse en la valoración de las condiciones y circunstancias que el buen sentido señala en cada caso»), y desde aquel momento se ha ido configurando la denominada doctrina de la causalidad eficiente.

Y en este sentido, mantiene mi maestro Francisco de Santiago como argumento jurídico en sus escritos que la doctrina que el Tribunal Supremo tiene sentada acerca de la relación de causalidad exige que la atribución sea exclusiva, natural y eficiente, como se advierte en la sentencia de 2 de marzo de 2009, en la que se mantiene que «el nexo de causalidad no puede ser establecido únicamente en el plano fenomenológico, atendiendo exclusivamente a la sucesión de acontecimientos en el mundo externo, sino que la causalidad física debe ser acompañada de una valoración jurídica en virtud de la cual, con criterios tomados del ordenamiento, pueda llegarse a la conclusión de que el daño causado se encuentra dentro del alcance de la conducta del agente, en virtud de lo que en nuestro ámbito científico suele llamarse imputación objetiva».

Y continúa exponiendo que, conforme a la sentencia del Tribunal Supremo de 21 de abril de 2008, «la imputación objetiva consiste en que establecida una relación de causalidad física o fenomenológica entre el agente y el resultado dañoso, debe formularse un juicio mediante el cual se aprecia si las consecuencias dañosas de la actividad son susceptibles de ser atribuidas jurídicamente al agente, aplicando las pautas o criterios extraídos del ordenamiento jurídico que justifican o descartan dicha imputación cuando se ponen en relación con el alcance del acto dañoso particularmente considerado, con su proximidad al resultado producido, con su idoneidad para producir el daño y con los demás elementos y circunstancias concurrentes».

431 *Op. cit.*, World Economic Forum (2014), p. 39.

432 Mariano Yzquierdo Tolsada, *op. cit.*, Dykinson, 2015, p. 193.

Tal doctrina se resume en el mandato de que la apreciación del nexo causal como competencia del juez de instancia no puede quedarse en el plano único de la causalidad física, sino que debe llevarse a cabo «un proceso de valoración jurídica para determinar si, producida la omisión, puede atribuirse a esta el daño o perjuicio producido, con arreglo a criterios de imputabilidad derivados de las circunstancias que rodean el ejercicio de la profesión desde el punto de vista de su regulación jurídica y de la previsibilidad del daño, con sujeción a las reglas de experiencia atendida la naturaleza de dicha función».

En particular, el desarrollo de las IT por medio de sistemas como el IoT pone de manifiesto la posibilidad cada día más evidente de que los ciberriesgos ocasionen cualquier tipo de daño físico o material sobre cualquier elemento conectado al ciberespacio. De tal forma, han supuesto la creación de importantes vínculos entre cualquier ciberevento y los bienes y derechos que dependen del ciberespacio, lo que genera la creación de nuevos riesgos y amenazas[433].

El IoT puede considerarse como el comienzo de una nueva etapa en la que el ciberespacio y la realidad física han perdido la independencia de la que gozaban para pasar a ser realidades cada día más dependientes. Así, ciertas circunstancias como la conducción autónoma o asistida de vehículos reducen los riesgos humanos asociados a la conducción, pero introducen una nueva generación de riesgos[434], en los que parece resultar alterada la aplicación de los elementos de la responsabilidad civil conforme a los supuestos tradicionales. Así, las particularidades técnicas y circunstancias de las IoT, como la conducción de vehículos autónomos, podrían permitir extender el nexo causal al ámbito del propio fabricante del vehículo autónomo[435].

Además, la jurisprudencia mantiene que el nexo causal no se debe abordar desde un punto de vista exclusivamente jurídico, ya que su determinación se concreta con relación a los hechos y fundamentos fácticos que son de «exclusiva apreciación de la Sala sentenciadora» (Sentencia del Tribunal Supremo de 13 de junio de 1988). Para ello, Pantaleón[436] ha enunciado una serie de criterios de valoración objetiva que pueden resumirse en:

---

433 Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination, Digital Agenda for Europe, European Commission DG Communications Networks, Content & Technology, p. 9, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9472

434 «IoT: La revolución silenciosa» (11 de julio de 2016), https://www.t-systems.com/es/es/newsroom/perspectives/internet-of-things/iot/iot-the-quiet-revolution-344724

435 «¿De quién es la culpa del accidente cuando hay un coche autónomo de por medio?», *Tecvolución volvo* (3 de diciembre de 2016), http://tecvolucion.com/quien-es-responsabilidad-legal-accidente-cuando-hay-coche-autonomo-de-por-medio/

436 A. F. Pantaleón, «Causalidad e imputación objetiva: criterios de imputación», en Asociación de Profesores de Derecho Civil, *Centenario del Código Civil*, t. 2, Madrid, 1990, p. 1.561 y ss.

- **El riesgo general de la vida,** que impide la imputación de responsabilidad de aquel riesgo ligado a la propia existencia del hombre en sociedad. Tal planteamiento fue reconocido por la STS de 17 de julio de 2007, y es perfectamente aplicable en el ámbito del ciberespacio. En esta medida, se debe reconocer que podrá hablarse de riesgo normal de la vida en el ciberespacio cuando se trate de las acciones ordinarias y situaciones habituales. Así, y como venimos advirtiendo, el ciberespacio comporta en diversos ámbitos un riesgo común y general que es muy superior al que se puede plantear para el mismo bien jurídico protegido en la realidad física (como ocurre en el caso de la pérdida y el robo de datos). Además, existen una serie de riesgos generales de la vida que son propios y exclusivos del ciberespacio, como puede ocurrir con la denegación de los servicios de un servidor cuando sufre una saturación de tráfico, bien por causas normales, bien por haber sufrido un ataque DDoS que los titulares del aquel servicio en muchos casos no pueden ni prever, ni evitar.

- **Prohibición de regreso,** por la que se considera rota la cadena causal cuando interviene la acción dolosa de un tercero. De esta manera, no se podrá atribuir responsabilidad a aquel que inconscientemente nos envía un correo electrónico con un archivo infectado por un malware que permite a quien lo infectó acceder a nuestros datos.

- **Criterio de la provocación,** por medio del cual se podrá atribuir a quien causó un daño por medio de un ciberataque no solo las consecuencias directas del daño causado, sino también aquellos daños que infrinja la víctima al intentar solucionar o evitar aquel (por ejemplo, si para reparar y evitar que se extiendan los daños ocasionados por un malware, se tiene necesariamente que formatear un sistema, y con tal operación se pierden datos que no habían sido afectados inicialmente, también se podrá atribuir esta pérdida al malware).

- **El fin de protección de la norma,** que fundamenta la responsabilidad. Sobre tal concepto mantiene la sentencia del Tribunal Supremo de 10 de diciembre de 2008 que «no toda infracción antirreglamentaria es susceptible de ser calificada como acción u omisión negligente; y, además, no toda infracción antirreglamentaria puede ser calificada *per se* como una causa eficiente de un resultado lesivo». Por ello, es evidente que no todo incumplimiento en materia de ciberseguridad dará lugar a la atribución objetiva de responsabilidad, sino que se deberá estar a las circunstancias y elementos que resulten de cada caso.

- **El incremento del riesgo.** Se trata de aquellos casos en los que el daño se hubiera producido con independencia de la acción concreta. En estos casos, la acción u omisión no aumenta el riesgo de forma significativa. Así, el informático que olvidó actualizar el software no será responsable del daño

que produzca un malware que hubiera afectado al sistema, con independencia de que aquella actualización se hubiera ejecutado.

- **El criterio de la adecuación,** por el que se mantiene que el daño debe ser adecuado a la conducta que lo ocasione, de tal manera que:

    a. Si como consecuencia de la falta de medidas de seguridad en nuestro ordenador personal transmitimos involuntariamente un malware al ordenador del director de una central hidroeléctrica, cuyo contacto tenemos en nuestra agenda por ser un amigo de la infancia, no se nos podrá responsabilizar de la imprevisible paralización de los sistemas de aquella central;

    b. y, por el contrario, en caso de que seamos proveedores de algún servicio de mantenimiento de aquella central y nuestros sistemas se conecten de forma periódica por necesidades técnicas, el grado de previsión cambiará completamente, ya que en tal caso el daño sí que hubiera sido previsible y adecuado a nuestra actividad.

En todo caso, existen una serie de elementos que interfieren en la atribución del nexo causal denominados «circunstancias extrañas» por ser externas a la acción u omisión a la que se pretende atribuir la responsabilidad, entre las que Mariano Yzquierdo menciona que se encuentran:

- **El caso fortuito y la fuerza mayor,** que han sido reconocidos por el artículo 1105 del Código Civil, que impide la atribución de la responsabilidad siempre «que el suceso sea imprevisible o que, aun pudiendo preverse, sea inevitable». Y esto deberá relacionarse necesariamente con la regla de la diligencia prevista en el artículo 1104 del Código Civil, y es que en materia de ciberseguridad la rapidez con la que surgen nuevos riesgos dificulta el mantenimiento de un sistema efectivo de protección y prevención. En este sentido, ya hemos estudiado en los primeros apartados que el análisis de la diligencia con la que se ha actuado será un elemento determinante a la hora de atribuir la responsabilidad de los daños relacionados con los ciberriesgos.

  Así, Von Tuhr[437] mantiene que la fuerza mayor es un evento imprevisible que proviene del exterior de la actividad, lo que se pone de manifiesto en los casos reconocidos por el artículo 1575 del Código Civil (y por ejemplo, estos eventos impiden que se atribuya la responsabilidad del daño por la pérdida de datos cuando los servidores donde se encontraban resultaron dañados por un huracán). Y, en otro sentido, el referenciado autor considera

437 A. von Tuhr, *Tratado de las obligaciones*, t. II, Madrid, 1934.

que el caso fortuito son aquellos acontecimientos inevitables pero que se pueden tener en cuenta en el «curso normal de la vida» (en este caso se encuentran aquellos cibereventos cuyos efectos no puedan ser paliados según el estado de la técnica).

En el ámbito de los ciberriesgos existen una serie de circunstancias de las que con toda seguridad surgirán discusiones sobre la aplicación de estos criterios. Así, hemos estudiado en los primeros apartados el elevadísimo riesgo que las acciones terroristas y militares suponen para el ciberespacio y los sistemas conectados a él, cuyos efectos pueden ser considerados como caso fortuito o fuerza mayor. Y en este sentido, la hiperconectividad puede permitir que un malware procedente de una acción militar se expanda por la red causando daños en cascada de los que los agentes afectados se responsabilizan entre sí, pero su inicio pudo ser un acto de guerra, lo que forma parte de la definición de caso fortuito. Además, y como hemos visto, el continuo desarrollo de los ciberriesgos aumenta la dificultad para impedir el daño, por lo que será muy difícil delimitar conforme a criterios objetivos el concepto de caso fortuito que provenga exclusivamente de los cibereventos.

En esta cuestión, la imprevisibilidad supone un elemento esencial para la determinación de la culpa, pues una vez se toma consciencia de la existencia de un riesgo concreto y posible, la obligación de impedir sus consecuencias recae sobre los titulares de los sistemas, proveedores y demás sujetos a quienes corresponda su mantenimiento. De tal forma, parece que para calificar la actuación del proveedor de software como diligente, este tiene que haber procurado enmendar el error una vez fue adecuadamente conocido. En tal caso, únicamente podríamos dudar sobre si la notificación de la existencia de esta vulnerabilidad y la publicación de los parches fue adecuada para que los usuarios pudieran evitar el daño, y en concreto si existe una verdadera relación de causalidad entre la falta de información y los daños [SSTS, 1.ª, 28.5.2012 (RJ 2012\6545), 6.6.2012 (RJ 2012\6702), 25.3.2013 (JUR 2013\205719), 18.6.2013 (JUR 2013\216269)]. Así, la sentencia de la Audiencia Provincial de Pontevedra de 23 de julio de 2002 sostenía:

«Ocioso resulta recordar que uno de los presupuestos que exige el éxito de tal acción lo constituye la existencia de culpa o negligencia imputable al demandado. En la documentación aportada a la litis (informe y ratificación de la empresa 'NM Numa Data'), consta que el virus de que se trata (fichero Pretty Park EXE) se recibió en uno de los ordenadores de la entidad demandada, en un mensaje de correo electrónico de fecha 25 de octubre de 2000, procedente de un emisor con el que se mantenía normal y ordinaria comunicación electrónica, de modo que con absoluta confianza y normalidad se procedió a su apertura, infectándose automáticamente con ello el sistema y, habida cuenta de que dicho virus modifica el registro de Windows y se difunde de manera

automática enviando mensajes de correo a todas las direcciones que consten en la libreta de programa de correo electrónico Outlook, ***sin que el usuario tenga conocimiento de tal hecho, no fue posible impedir su propagación y consecuente causación de daños en el sistema informático de la actora. Con tales antecedentes resulta imposible hablar de un comportamiento culpable o negligente: los hechos absolutamente imprevisibles (caso fortuito del art. 1105 del Código Civil) constituyen el límite de la culpa y exoneran de responsabilidad el art. 1902 de dicho cuerpo legal»***.

- **La intervención de un tercero** impide la atribución del daño cuando su interferencia se puede considerar suficiente para romper con el nexo causal, por lo que se exonera al agente material del daño. Así, digamos que no se puede responsabilizar a un procurador de la falta de presentación de un escrito cuando esta no se pudo hacer efectiva por encontrarse sus sistemas fuera de servicio como consecuencia de un ciberataque perpetrado por un tercero (en este sentido se pronuncian las sentencias del Tribunal Supremo de 30 de marzo de 1971 y 16 de noviembre de 1983). Y ello, siempre que la conducta del tercero no haya sido agravada por la del agente, lo que constituye el elemento esencial para definir los límites de este criterio.

  Así, cualquier ciberataque requiere tal efectiva intervención de un tercero, por lo que el sujeto que haya permitido que de este se derive un daño a un tercero podrá oponer esta excepción siempre que se demuestre que su actuación no coadyuvó al resultado. De esta forma, la diligencia de cualquier sujeto se circunscribe a que una vez conocida la vulnerabilidad concreta tome medidas efectivas para evitar sus efectos. Así, la particularidad de algunas vulnerabilidades como las denominadas *0-day* es que resultaban completamente desconocidas hasta que se produce el ciberevento[438], por lo que será desde el momento en el que se descubren cuando el proveedor de software resulta obligado a ofrecer una solución. Y hasta entonces, la intervención del tercero que crea y distribuye el malware impide que se pueda apreciar la existencia del nexo causal entre el posible error de software y el daño.

- **Culpa de la víctima.** Tampoco se podrá atribuir o en todo caso se deberá mitigar la responsabilidad cuando el daño se deba a la actuación de la propia víctima. Un caso evidente será el atropello de un vehículo autónomo que no pudo esquivar a quien cruzó la calle por donde no debía. Y los casos más controvertidos pueden provenir de los supuestos en los que es la víctima quien al sufrir una acción de «ingeniería social» ofrece de manera

438 «What is Zero Day Exploit?», *Kaspersky,* https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

voluntaria sus datos o contraseñas a un tercero, por lo que en ningún caso se podrá responsabilizar a quien mantiene su seguridad de no haber actualizado los sistemas o contraseñas.

Además, resulta que para determinadas vulnerabilidades los usuarios tienen conocimiento de su existencia, y disponen de medios y herramientas adecuados para evitarlo. Máxime en aquellos supuestos en los que las compañías afectadas se tratan de multinacionales pertenecientes a sectores estratégicos cuyos medios son presumiblemente más amplios que los de un usuario particular. Por ello, podría llegar a entenderse que en estos casos los efectos de un ciberevento solo se deben a la omisión de los propios usuarios, ya que pudiendo haber descargado las actualizaciones y parches que los proveedores de software ponen a su disposición, deciden permanecer pasivos asumiendo el riesgo del que previamente se les ha advertido. De tal forma, en contra de lo establecido por la sentencia de 23 de julio de 2002, se podrá atribuir a la responsabilidad de estas compañías los efectos que haya ocasionado su omisión (sentencia de la Audiencia Provincial de Cantabria, 21 de octubre de 2008) o actuación «tardía» (sentencia de la Audiencia Provincial de Barcelona, 23 de septiembre de 2010).

En estos casos, ya manteníamos en el artículo «¿Quién es responsable de Wannacrypt?» que las compañías afectadas podrán probar que concurrió el caso fortuito al que se refiere la sentencia si consiguen acreditar que sus sistemas resultaron infectados a pesar de poner todos los medios posibles para evitar el malware. Así, las compañías que gestionan sistemas estratégicos e infraestructuras críticas no siguen una política de actualización automática de sistemas como se puede esperar de una organización que gestiona y mantiene sistemas de menor relevancia. Y es que la importancia de aquellos sistemas requiere que se realicen pruebas y analicen futuros escenarios antes de actualizar el software o de instalar nuevos parches. Por este motivo los malware *0-day* son tan peligrosos, ya que actúan antes de que el proveedor de software y sus clientes puedan reaccionar. No obstante, en este caso parece difícil mantener que sin lugar a dudas los afectados pusieron todos los medios para evitar la infección, pues la vulnerabilidad ya había sido reconocida, notificada y calificada como crítica dos meses antes.

Todo ello encuentra su aplicación en aquellos casos en los que el sistema de una compañía es infectado como consecuencia de haberse conectado a la red de otra que ya se encontraba afectada. No obstante, esta conclusión debe ser limitada y matizada a la luz de los requisitos básicos de la responsabilidad civil, y en concreto de la doctrina que nuestra jurisprudencia ha desarrollado sobre la concurrencia de culpas. Así, del propio funcionamiento de algunos malware resulta que, para que pueda transcender a un tercero, es necesario que este tampoco se haya descargado

la actualización del software, por lo que también habrá desatendido su obligación de mantener sus propios sistemas. Y en este sentido, tampoco podrá atribuirse aquella responsabilidad en los siguientes supuestos:

a. La pérdida de datos, ya que se hubiera evitado con el debido cumplimiento de la obligación de hacer copias de seguridad, cuya importancia resulta evidente y es conocida por todos los usuarios (sentencias de la Audiencia Provincial de Jaén de 4 de noviembre de 2009 y de la Audiencia Provincial de Madrid de 16 de noviembre de 2004).

b. Y «tampoco se podrá atribuir los daños derivados del incumplimiento de contratos, pues es obligación de los terceros tener copias de seguridad» (Audiencia Provincial de Madrid de 23 de marzo de 2007).

En conclusión, una vez se han analizado los elementos de la causalidad con relación al ámbito de los ciberriesgos, podemos advertir que, frente a la realidad cambiante y al continuo desarrollo que estos presentan, deberá hacerse un mayor esfuerzo para comprender cada una de las circunstancias fácticas que llevan al daño. Así, la dificultad técnica que plantean estos supuestos y la ausencia de antecedentes jurisprudenciales nos debe llevar a aplicar con cautela los principios jurídicos a los que hemos hecho referencia. Pues bien, como se ha advertido, una aplicación demasiado amplia de los elementos de exoneración (como el caso fortuito y la fuerza mayor) de la responsabilidad dejaría a la mayoría de los supuestos en los que se padezcan daños relacionados con los ciberriesgos huérfanos de toda responsabilidad.

5.3. Los factores de la atribución de la responsabilidad

Continuando con el esquema del estudio de la responsabilidad civil establecido por Mariano Yzquierdo, debemos considerar en palabras del autor que «aquí ya no hablamos de qué (consecuencias se responde), sino de por qué se responde». Por ello, en el presente apartado se analizará un escalón más del estudio de la responsabilidad civil al que se llega después de considerar que existe una relación causal entre la acción u omisión y el daño.

Así, mantiene Reglero Campos que se deberá decidir conforme a las normas sobre la responsabilidad si el perjudicado debe soportar el daño, «o si existe una razón suficiente para imputar el daño a otra persona»[439]. Y en este ámbito, estudia De Ángel Yágüez[440] que han existido tres hitos en la evolución de la atribución de la responsabilidad que define como: la inversión de la carga de

439 José Manuel Busto Lago y L. Fernando Reglero Campos (coord.), «Lección 2.ª. Los sistemas de responsabilidad», en *Lecciones de responsabilidad civil*, Aranzadi, Navarra, 2013, p. 65.

440 Ricardo De Ángel Yágüez, *Tratado de responsabilidad civil*, Madrid, 1993, p. 126.

la prueba, el progresivo aumento de la diligencia exigible y el reconocimiento de la responsabilidad objetiva.

En cuanto al segundo de estos elementos, la jurisprudencia parece haber aumentado de forma generalizada el grado de diligencia exigible para la atribución de la responsabilidad civil extracontractual. En este sentido, mantiene la sentencia del Tribunal Supremo de 20 de noviembre de 2008 (entre otras) que «cuando las garantías adoptadas, conforme a las disposiciones legales para prever y evitar los daños previsibles y evitables, no han ofrecido resultado positivo, revela ello la insuficiencia de las mismas y que faltaba algo por prevenir y que no se hallaba completa la diligencia». Así, el resultado de aplicar este criterio jurisprudencial a la atribución de la responsabilidad procedente de los ciberriesgos pone de manifiesto la certeza de la afirmación de Mariano Yzquierdo de que «a base de repetir las barbaridades no se consigue que dejen de serlo».

Pues bien, actualmente, el riesgo potencial y previsible que genera el ejercicio de cualquier acción en el ciberespacio es altísimo y, además, el rápido desarrollo de la técnica dificulta la posibilidad de afirmar con certeza si un daño podía evitarse o no. Por eso, una aplicación estricta de esta doctrina permite que se atribuya la responsabilidad de un daño sin necesidad de probar el grado de diligencia con el que se ha actuado, lo que en un ámbito tan técnico e inexplorado como la ciberseguridad parece imprescindible.

Y en relación con la responsabilidad objetiva —tercer elemento al que hace referencia De Ángel Yágüez—, podemos adelantar que se trata del régimen que permite la atribución de la responsabilidad sin determinar la culpa o negligencia del actor. Así, esta figura ha sido regulada por el legislador en relación con ciertas actividades (la caza, la conducción de vehículos a motor, la energía nuclear…) e introducida por la jurisprudencia en un gran número de casos.

5.3.1. Responsabilidad por actos propios

a. Factores subjetivos

Uno de los criterios clásicos de atribución de la responsabilidad es el de la culpa o negligencia que se define en el artículo 1104 del Código Civil como «la omisión de aquella diligencia que exija la naturaleza de la obligación y corresponda a las circunstancias de las personas, del tiempo y del lugar». Así, la culpa es un comportamiento que difiere de un comportamiento de conducta definida objetivamente por el Derecho como «diligencia debida». Por ello, afirma Reglero Campos[441] que es esencial la determinación de un deber

441 José Manuel Busto Lago y L. Fernando Reglero Campos (coord.), *op. cit*, Aranzadi, Navarra, 2013, p. 7.

de diligencia apropiado a cada sector de actividad, lo que tiene un especial efecto en el ámbito de la ciberseguridad por su carácter técnico.

En el caso de la responsabilidad extracontractual, Albadalejo[442] mantiene que deberá aplicarse el criterio de la culpa levísima consignado en el artículo 1089 del Código Civil, que establece que las obligaciones nacen «de cualquier género de culpa o negligencia», lo que ha asumido el Tribunal Supremo por medio de la doctrina del «agotamiento de la diligencia» (sentencias de 25 de marzo de 2011 y 30 de noviembre de 2011)[443]. Y esto obliga al agente a adecuar por todos los medios posibles su comportamiento al estándar objetivo de la actividad concreta.

Los ciberriesgos pueden afectar a cualquier sector, industria o aspecto de la vida que tenga relación con el ciberespacio, por lo que el estándar de diligencia debida dependerá de circunstancias muy diversas. No obstante, en los primeros apartados de nuestro estudio hemos intentando atender a las principales circunstancias que se deben tener en cuenta en el ámbito de la ciberseguridad.

En la práctica, para determinar si una actividad fue adecuada a la diligencia debida se estudiarán los dictámenes que algún experto independiente pueda elaborar sobre los hechos y circunstancias concretas, que se valoran conforme a la sana crítica del juzgador (artículo 348 LEC).

Así, el presente estudio ha analizado alguna de las circunstancias técnicas del ámbito de los ciberriesgos con el propósito de poder facilitar la comprensión de estos supuestos de responsabilidad. Por ello, se expone desde un punto de vista jurídico las complejas estructuras técnicas que giran en torno a los ciberriesgos sobre las que la doctrina deberá ir encajando los elementos básicos de la responsabilidad civil.

El segundo elemento por el que se puede atribuir la responsabilidad es el dolo que ha sido reconocido, entre otros, por los artículos 1101 y 1102 del Código Civil, por medio de los cuales se considera que «quedan sujetos a la indemnización de los daños y perjuicios causados los que en el cumplimiento de sus obligaciones incurrieren en dolo, negligencia o morosidad», y que «la responsabilidad procedente del dolo es exigible en todas las obligaciones». Así, en el caso de la responsabilidad contractual, «el dolo es la conciencia del deudor de hacerse voluntariamente incumplidor» con independencia de la

442 M. Albadalejo, *La responsabilidad por culpa extracontractual levísima*, Real academia de Jurisprudencia y Legislación, Madrid, 2000, p. 15 y ss.

443 Mariano Yzquierdo Tolsada, *op. cit.*, Dykinson, 2015, p. 243.

malicia o la voluntad en el dañar[444]. En este sentido, parece que si una empresa proveedora de hosting ofrece un ancho de banda menor al acordado y el servicio se sobrecarga, será responsable del daño que produzca su incumplimiento con independencia de que tuviera o no intención de que tal daño se produjera.

En cuanto a la responsabilidad extracontractual por dolo, en esta se da el caso de que el agente «quiere incumplir el deber general de no dañar, y además es consciente del resultado material que supondrá su conducta dañosa»[445]. Entre los múltiples ejemplos, podemos advertir que se deberá reconocer la responsabilidad por dolo del trabajador que de forma consciente y voluntaria descarga un malware en los sistemas de su empresa.

b. Factores objetivos

La doctrina clásica de la responsabilidad por culpa fue evolucionando durante el siglo XX hasta que la sentencia del Tribunal Supremo de 10 de julio de 1943 reconoció la doctrina de la inversión de la carga de la prueba en aquellos «supuestos en que resulte evidente un hecho que por sí solo determine probabilidad de culpa». A este criterio se le han ido añadiendo otros elementos tendentes a facilitar el acceso a la reparación del daño hasta llegar a la doctrina del riesgo.

Por medio de la mencionada doctrina se considera que quien se beneficie con la actividad empresarial que genera el riesgo debe asumir también la responsabilidad del mismo *ubi emolumentum, ibi onus*. No obstante, parece que la doctrina jurisprudencial se está postulando en contra de la objetivación de la responsabilidad, y como recoge la obra de Reglero Campos —actualizada por Peña López—, el propio ponente de la sala 1.ª del Tribunal Supremo, Juan Antonio Xiol, ha afirmado que «a partir del año 2005, advertimos un claro regreso a la teoría de la responsabilidad por culpa». En este sentido, ha precisado la jurisprudencia que la teoría del riesgo es aplicable únicamente a aquellas actividades que generan un riesgo superior a los estándares normales, como mantiene la sentencia del Tribunal Supremo de 18 de julio de 2002.

En concreto, la referenciada sentencia determina que «no se puede hablar de una responsabilidad por riesgo, la cual debe ser contemplada con un carácter restrictivo, ya que no se puede aplicar a todas las actividades de la vida, sino solamente a aquellas que impliquen o supongan un riesgo

444 Mariano Yzquierdo Tolsada, *op. cit.*, Dykinson, 2015, p. 255.

445 Mariano Yzquierdo Tolsada, *op. cit.*, Dykinson, 2015, p. 256.

considerablemente anormal en relación con los parámetros medios, o sea que dicha responsabilidad por riesgo debe excluirse como base indemnizatoria cuando se trata de riesgos o azares normales o actividades no preocupantes. Y en el presente caso, la realización de unas obras de excavación empleando la maquinaria lógica, que son necesarias para la edificación de un inmueble, enclavadas dentro de una actividad única y con carácter temporal muy concreto, no podrá nunca estimarse como una actividad de riesgo que permita una objetivación culposa».

Así, una vez más deberemos advertir que como consecuencia de la diversidad de situaciones que plantean los ciberriesgos, se tendrá que atender a las particularidades propias de cada caso para concluir si se trataba de una actividad de especial riesgo, o por el contrario este no excede del estándar general. Además, el desarrollo del estado de la ciencia en cada momento concreto es determinante para analizar los ciberriesgos a los que está sometida una actividad precisa en un momento determinado, ya que este puede contribuir a mitigar o agravar los mismos. Por ello, sería inútil y temerario adelantar una relación de las actividades que puedan llegar a considerarse de mayor riesgo.

No obstante, desde la perspectiva actual podemos considerar que existen dos circunstancias que determinan que una actividad sea generadora de un nivel especial de ciberriesgo, que son: la gravedad de la acción u omisión y el carácter del objeto sobre el que recae el riesgo. Ya mencionábamos que la gravedad en los ciberriesgos se puede poner de manifiesto por medio de las circunstancias propias del ciberevento, en el objeto sobre el que recae, o por ambos elementos.

Así, el criterio que sigue la referenciada sentencia del Tribunal Supremo considera que las circunstancias de la acción u omisión generadora del riesgo son el criterio determinante del carácter del mismo. Y esta conclusión, en el caso de los ciberriesgos, implicaría atribuir tal carácter a aquellas acciones especialmente invasivas o que desprotegen de forma singular los equipos, o a las diversas actuaciones que giran en torno a aquellos ciberataques, que requieren de una gran complejidad técnica. La generalización de este criterio objetivaría la responsabilidad en casos cuyos efectos son nimios, de tal manera que se podrá responsabilizar al proveedor de servicios de alquiler de servidores por la interrupción de la actividad de sus clientes como consecuencia de un ataque DDoS sin necesidad de elaborar un juicio sobre las acciones que coadyuvaron al resultado. Y esto, con independencia absoluta de la importancia o irrelevancia de la actividad que resultó perjudicada y los efectos que a la postre surgieron.

En otro sentido, el legislador parece más preocupado en los ciberriesgos que afectan a aquellos ámbitos que se consideran de mayor gravedad para la

estabilidad socioeconómica, como las infraestructuras críticas o la protección de datos personales. Y tal regulación se aborda atendiendo de forma exclusiva al objeto sobre el que recae el riesgo con independencia de la acción que produzca el daño —este criterio es el fundamento de la responsabilidad objetiva que introduce el artículo 4.1 de la Ley 12/2011, de 27 de mayo—. Por ello, no sería extraño que el criterio de objetivación se pueda llegar a aplicar en función del bien jurídico protegido que pueda verse afectado por el ciberriesgo, aunque tal aplicación permitiría imputar la responsabilidad sin necesidad de valorar la conducta del agente. Así, en estos casos podría atribuirse la responsabilidad de aquellos daños que hayan sido consecuencia de acciones de las que de ninguna forma lógica podrían haberse deducido tales consecuencias.

En conclusión, la dificultad técnica y las particularidades del ámbito de los ciberriesgos justifican la afirmación de Reglero Campos[446], quien considera que es esencial la determinación de un deber de diligencia apropiado a cada sector de actividad, además de estudiar de forma individual las circunstancias que coadyuvan en el resultado dañoso. Por ello, debemos mantener igual que el mencionado autor que la doctrina de la objetivación de la responsabilidad es una construcción que debe superarse en favor del necesario enjuiciamiento de la acción, que en el ámbito del ciberespacio tiene una especial importancia debido a la complejidad técnica que el sector lleva aparejada.

No obstante, si se decidiera aplicar el criterio de la imputación objetiva al ámbito de los ciberriesgos, será conveniente que para calificar una actividad como generadora de un especial riesgo se atienda tanto al objeto de la misma como a los medios, ya que solo de tal manera se podrá determinar la gravedad de la conducta de la forma más precisa posible y evitar los supuestos contradictorios a los que nos hemos referido.

5.3.2. Responsabilidad por actos ajenos

La responsabilidad por aquellos actos que ha generado un tercero se ha consagrado en el artículo 1903 del Código Civil por medio del cual la obligación general que impone el artículo 1902 «es exigible no solo por los actos u omisiones propios, sino por los de aquellas personas de quienes se debe responder». Así, responderán los padres —respecto de sus hijos—, los tutores —de los que estén bajo su guarda—, el titular o director de un establecimiento —de sus dependientes— y el titular de un centro de enseñanza no superior —de sus alumnos—, ya que estarán obligados a resarcir el daño causado por aquellos que se hallen bajo su responsabilidad. En este sentido, ya decía

446 José Manuel Busto Lago y L. Fernando Reglero Campos (coord.), «Lección 2.ª. Los sistemas de responsabilidad», en *Lecciones de responsabilidad civil*, Aranzadi, Navarra, 2013, p. 73.

Kenneth Cannar que se adopta el principio clásico de *qui facit per alium facit per se* para hacer responsable al empleador de los actos del empleado. Y de esta manera, se facilita a la víctima la posibilidad de ser resarcido al presumir que el empleador tendrá mayor capacidad para compensar el daño[447].

Actualmente, Reglero[448] hace referencia a que la jurisprudencia mayoritaria considera que la responsabilidad derivada del artículo 1903 del Código Civil se funda en la culpa al imponer que «cuando entre el autor material del hecho y el que queda responsable hay un vínculo tal que la ley puede presumir fundadamente que sí hubo daño, este debe atribuirse, más que al autor material, el descuido o defecto de la vigilancia de otra persona, por lo que el fundamento de esta responsabilidad es una presunción de culpa» (sentencias del Tribunal Supremo de 21 de junio de 2006 y 6 de marzo de 2007).

Una vez más, debemos advertir que nos encontramos ante un elemento cuya aplicación en el ámbito de los ciberriesgos podrá ser muy significativa, y en especial en lo relativo a la exoneración del artículo 1903 del Código Civil, que determina que cesará la responsabilidad cuando se pruebe que se empleó «toda la diligencia de un buen padre de familia para prevenir el daño». Y esto conlleva que los límites de la responsabilidad de aquellos que deban responder por otros se hayan extendido a un número muy amplio de relaciones como consecuencia de la hiperconectividad y de los efectos del ciberespacio. Así, podemos plantear una serie de situaciones en las que el control de los hijos, alumnos, empleados y demás personas de las que se responda no parece que se pueda llevar a cabo por medio de instrumentos materiales y jurídicos de los que en la actualidad disponemos.

En relación con la responsabilidad de los padres e instituciones educativas, ¿quién responderá por aquellos actos que realice un alumno desde su casa con la tableta del colegio?

Pues bien, la respuesta parece que será los dos, ya que, en este sentido, la doctrina mayoritaria (DÍAZ ALABART, 1987: 803; ABRIL CAMPOY, 2003: 28; MARTÍN CASALS, RIBOT y SOLÉ FELIÚ, 2006: 388) ha mantenido que la culpa de los padres se presume como hace el Tribunal Supremo en su sentencia de 13 de octubre de 1998, en la que responsabiliza a los padres de un menor que realizó fotos a otro en los vestuarios de un club deportivo. Así, este criterio «contempla una responsabilidad por riesgo o cuasiobjetiva» que se encuentra «justificada por la transgresión del deber de vigilancia que a los padres incumbe sobre los hijos sometidos a su potestad»[449].

447 Kenneth Cannar, *Liability Insurance Claims*, London Witherby & Co, 1978, p. 69.

448 Ídem, p. 152.

449 Mariano Yzquierdo Tolsada, *op. cit.*, Dykinson, 2015, pp. 277-279.

Pues bien, llegados a este punto nos deberemos cuestionar si los padres tienen verdaderos medios para evitar que sus hijos cometan daños por medio del ciberespacio, y si el nivel de diligencia se agota con la instalación de instrumentos como el software de protección infantil. Igualmente, el centro de enseñanza tendrá que acreditar que mantiene un control efectivo sobre las IT que proporciona a los alumnos para su actividad escolar. Así, parece que estos sistemas (entre los que destacan las plataformas que mantienen aulas virtuales) extienden la responsabilidad del colegio que tradicionalmente se limitaba al aula y al horario escolar al ilimitado ámbito del ciberespacio, con independencia del lugar o el tiempo en el que el alumno cause el daño.

Y en el caso de la responsabilidad derivada de los actos de empleados y dependientes, parece que se pueden atribuir conclusiones similares, así:

¿La empresa deberá responder de cualquier acción que realice un empleado en su puesto de trabajo aunque sea mediante un terminal móvil particular?, y ¿responderá de aquellas acciones que realice el empleado fuera de su puesto de trabajo pero por medio de los sistemas informáticos de la propia empresa?

La jurisprudencia mayoritaria (a la que se refiere BARCELÓ DOMENECH, 1995: 303 y 304 —desde STS de 28 de febrero de 1983 hasta la STS de 14 de mayo de 2010—) mantiene que el fundamento de la responsabilidad del empresario es la culpa *in vigilando* o *in diligendo*. Por lo que advierte Mariano Yzquierdo que «el empresario responde, en definitiva, porque es empresario, y eso es todo»… de tal forma que «allí donde esté el beneficio, ahí ha de estar también la carga»[450].

No obstante, para que concurra la responsabilidad del empresario se han de dar una serie de requisitos por medio de los que resolveremos las dudas planteadas, que son:

1. La culpa *in operando*.

2. La relación de dependencia, jerarquía o encargo.

3. La actuación del dependiente en el desempeño de sus obligaciones, por lo que «debe existir un nexo de ocasionalidad entre el hecho dañoso y las funciones asignadas, de manera que el desempeño de este viene a ser la ocasión necesaria de aquel»[451]. Por ello, parece que el empresario solo responderá de aquello que se limite al ámbito de las obligaciones del empleado.

450 Mariano Yzquierdo Tolsada, *op. cit.*, Dykinson, 2015, pp. 312 y 313.

451 Ídem, p. 319.

No obstante, mantiene la sentencia del Tribunal Supremo de 10 de febrero de 1972 que bastará con que el hecho tenga lugar «con ocasión próxima del mismo servicio, haciendo uso de medios o instrumentos puestos a su disposición». Así, debemos advertir que la utilización de los sistemas informáticos de la empresa podría llegar a atribuir a esta la responsabilidad de los actos del empleado (lo que pone de manifiesto la relevancia de la pregunta que nos hacíamos sobre la utilización de los sistemas informáticos de la empresa).

Y, sobre la atribución de la responsabilidad conforme al horario y al lugar de trabajo mantiene Mariano Yzquierdo[452] que no es determinante para la atribución de la responsabilidad, aunque el Tribunal Supremo reconoce en su sentencia de 23 de junio de 2005 que «es cierto que no se encontraba en el ejercicio de sus funciones en sentido estricto, pero su presencia en el lugar de los hechos y las facilidades para acceder a ese lugar se derivan de su relación de dependencia con la empresa» (por lo que se reconoce la responsabilidad de la empresa por el robo, violación y homicidio que cometió un trabajador que se ausentó de una fiesta organizada por su empresa). Y en la sentencia de 1 de julio de 2002 la empresa era responsable subsidiaria de la violación cometida por un guarda de seguridad porque los hechos habían tenido lugar «no solo en el contexto de la actividad desarrollada por el acusado, sino incluso en el lugar donde desempeñaba su función».

En conclusión, muy a nuestro pesar, los órganos jurisdiccionales podrán reconocer sobre la base de esta desacertada doctrina que la empresa es responsable de los actos que un trabajador cometa en el ciberespacio con tal de que se encuentre en el lugar de trabajo o utilice un sistema proporcionado por la empresa. Tal conclusión pone de manifiesto la necesidad de adaptar ciertos planteamientos a la realidad socioeconómica de cada momento y a las máximas de la razón y la lógica. De tal forma, los ciberriesgos hacen más evidente que nunca que la responsabilidad *in vigilando* e *in diligendo* debe restringirse de forma estricta al cumplimiento de las funciones del trabajador. Y es que la cantidad de acciones dañosas que un trabajador puede llevar a cabo por medio de un ordenador o un smartphone es inabarcable.

452 Ídem, p. 321.

6. LA ESPECIAL REFERENCIA A LA RESPONSABILIDAD DE ADMINISTRADORES Y DIRECTIVOS EN RELACIÓN CON LOS CIBERRIESGOS

6.1. Concepto y evolución de la responsabilidad de los administradores y directivos

Las negligencias profesionales se pueden definir como el incumplimiento del deber de cuidado cometido por un profesional, que por medio de un error u omisión en el ejercicio de su profesión causa un daño o pérdida a un cliente o a cualquier tercero[453]. No obstante, los profesionales trabajan en ámbitos en los que no siempre se puede asegurar que el resultado será el esperado por su cliente, por lo que tradicionalmente se ha requerido que el profesional cumpla con un grado de competencia adecuado para la función que desempeña. De manera que el grado de competencia se pondera con el contenido del acuerdo al que haya llegado el profesional con su cliente.

En este sentido, hasta los años ochenta —en el ordenamiento jurídico del Reino Unido— se reconocía que el profesional solo respondía de su actuación conforme a los límites pactados en el contrato. Tal doctrina fue modificada por The House of Lords al resolver el caso Tai Hing Cotton Mill Ltd. V. Lui Chong Hing Bank Ltd., a partir del cual se extiende la responsabilidad del profesional a las obligaciones que proceden de situaciones y elementos próximos a su relación con el cliente. Este cambio en la doctrina ha permitido que ciertos profesionales —como arquitectos o ingenieros— respondan respecto de los daños que su actuación pueda causar a terceros[454].

La responsabilidad de los administradores y directivos derivada de daños causados tanto al interés social como a terceros se contempla como una responsabilidad profesional. De tal forma, este régimen de responsabilidad ha ido evolucionando en la medida en que se han endurecido las normas que

453 Digby C. Jess, *A Guide to the Insurance of Profesional Negligence Risks*, Butterworths London, 1982, p. 1.

454 Rupert M. Jackson, *Professional Negligence*, London Sweet & Maxwell, 1987, pp. 4-15.

lo regulan[455], primeramente con la publicación del Texto Refundido de la Ley de Sociedades Anónimas y, posteriormente, con la Ley de Sociedades de Capital.

Así, se trata de una responsabilidad derivada de los errores o negligencias cometidas en el ejercicio de su cargo, que en el caso de los administradores engloba todas las actividades necesarias para alcanzar el fin social. En concreto, estas actividades están circunscritas al ámbito interno de la gestión de la sociedad y al ámbito externo de la representación de la misma. Así, frente a tales daños, surge la «acción social» para reclamar el perjuicio que el administrador haya causado al patrimonio social, y la «acción individual» de cualquiera de los socios o terceros como consecuencia de un perjuicio causado a su patrimonio individual (236.1 LSC).

El artículo 225 de la LSC impone el deber de desempeñar con diligencia el ejercicio de su cargo que, como mantenía Garrigues, se extiende a las dos funciones del cargo: representar a la sociedad con lealtad y fidelidad, y conducir los negocios sociales como un ordenado empresario[456], a lo que se refiere José Oriol como el deber fiduciario de esforzarse por la consecución del interés social[457]. Así, este deber genérico de diligencia constituye una obligación de medios, por lo que no responde del éxito de su gestión sino de las faltas que haya podido cometer en el desempeño de la misma[458]. Además, el artículo 225 establece la obligación de los administradores de obtener la información que resulte necesaria para el desempeño de su cargo, que en el caso de los ciberriesgos se llevará a cabo mediante la comunicación con los CIO y CISO.

Así, el desarrollo legislativo y doctrinal ha permitido individualizar y determinar la responsabilidad de cada uno de los sujetos que forman parte de una organización. No obstante, el principal problema con el que se enfrenta este régimen es la dificultad de probar qué sujeto es individualmente responsable de un acto ejercido por, o por cuenta de, una organización. De esta forma, se

455 Fernando Martínez Sanz, «Los administradores responsables», en Ana Belén Campuzano (coord.), *La responsabilidad de los administradores en las sociedades mercantiles*, Tirant lo Blach Tratados, Valencia, 4.ª edición, 2011, p. 60.

456 Garrigues y Uría, «Comentario de la Ley de Sociedades Anónimas», t. II, 3.ª ed., revisada y puesta al día por Menéndez y Olivencia, Civitas, 1976, en M.ª Ángeles Parra Lucán, «Lección 17.ª La responsabilidad civil de los administradores», en *Lecciones de responsabilidad civil*, 2013, Aranzadi, pp. 505-515.

457 José Oriol Llebot, «Los deberes y la responsabilidad de los administradores», en Ana Belén Campuzano (coord.), *La responsabilidad de los administradores en las sociedades mercantiles*, 4.ª edición, Tirant lo Blach Tratados, Valencia, 2011, p. 30.

458 M.ª Ángeles Parra Lucán, «Lección 17.ª La responsabilidad civil de los administradores», *Lecciones de responsabilidad civil*, 2013, Dykinson, pp. 505-515.

han aplicado diversas soluciones para aquellos casos en los que esta prueba resulte especialmente difícil, entre los que destaca la responsabilidad vicaria, conforme a la que se considera a la empresa como responsable principal (*respondeat superior*[459]) de los daños que cause aquel cuya actividad se encuentra bajo el control de la organización. Y otras soluciones como:

- Limitar este régimen de responsabilidad a la responsabilidad que sobrevenga del incumplimiento de las disposiciones penales;
- determinar de forma específica aquellas prácticas de las que pueda derivarse tal responsabilidad[460];
- o regular el nivel de diligencia que debe exigirse a una determinada profesión.

Así, el ordenamiento jurídico español ha optado por reconocer una relación de acciones de las que puede llegar a surgir la responsabilidad del administrador, que se han determinado en diversas disposiciones entre las que destacan los artículos 226 al 229 de la LSC. Y sobre la diligencia, las normas que determinan el estándar con el que deben actuar los administradores o directivos han tendido a proteger los intereses de los accionistas, por medio del reconocimiento de una serie de medidas que deben tomar estos sujetos para procurar el cuidado razonable del ejercicio de su cargo[461]. No obstante, debido a la amplitud del término y de sus obligaciones, mantiene Kraakman que la determinación del nivel de diligencia con el que debe actuar un directivo resulta mucho más difícil que en el resto de profesionales.

Tal práctica permitiría establecer una serie de límites con los que se podría determinar un régimen de responsabilidad razonable en el ciberespacio, e impediría atribuir la obligación de alcanzar objetivos de ciberseguridad a los que no se puede llegar con el actual estado de la ciencia.

En todo caso, se debe aplicar la doctrina general de la responsabilidad por daños conforme a la cual es preciso acreditar la concurrencia de una acción u omisión negligente o culpable; y que de tal acción tenga un efecto en el ámbito de la ciberseguridad de la que se haya derivado necesariamente un daño concreto, actual y determinado. Así, la acción individual de responsabilidad de los administradores «supone una especial aplicación de responsabilidad»

459 Shavell, 2004, p. 232 y Kraakman, 2008 en Maximilian K.P. Gaber, *The effect of D&O Insurance on managerial risk taking*, Intersentia Publish Ltd, Cambridge, 2015, p. 11.

460 Maximilian K.P. Gaber, *The effect of D&O Insurance on managerial risk taking*, Intersentia Publish Ltd, Cambridge, 2015, pp. 11-13.

461 Kraakman, 2009, p. 78 en Maximilian K. P. Gaber, *The effect of D&O Insurance on managerial risk taking*, Intersentia Publish Ltd, Cambridge, 2015, pp. 22-23.

extracontractual integrada en un marco societario, que cuenta con una regulación propia (art. 135 TRLSA, y en la actualidad, art. 241 LSC) que la especializa respecto de la genérica prevista en el art. 1902 CC (SSTS de 6 de abril de 2006, 7 de mayo de 2004, 24 de marzo de 2004, entre otras). Se trata de una responsabilidad por «ilícito orgánico», entendida como la contraída en el desempeño de sus funciones del cargo» (sentencias 242/2014, de 23 de mayo, y 737/2014, de 22 de diciembre).

Y como mantiene la inveterada jurisprudencia (sentencias 131/2016, de 3 de marzo; 396/2013, de 20 de junio; 395/2012, de 18 de junio; 312/2010, de 1 de junio; y 667/2009, de 23 de octubre, entre otras), para su apreciación será necesario el cumplimiento de los siguientes requisitos:

- la existencia de un comportamiento activo o pasivo de los administradores;
- que tal comportamiento sea imputable al órgano de administración;
- que la conducta del administrador sea antijurídica por infringir la ley, los estatutos o no ajustarse al estándar o patrón de diligencia exigible a un ordenado empresario y a un representante leal;
- que la conducta antijurídica, culposa o negligente sea susceptible de producir un daño;
- el daño que se infiere afecte de forma directa a un tercero, sin necesidad de lesionar los intereses de la sociedad;
- la relación de causalidad entre la conducta antijurídica del administrador y el daño directo ocasionado al tercero.

6.2. Concepto y obligaciones propias de los CTO, CIO y CISO

El Chief Technology Officer (CTO) es el individuo que supervisa el estado de las IT y las políticas tecnológicas que han sido implementadas en una determinada compañía o institución. Por ello, debe tratarse de un profesional con el conocimiento técnico adecuado para adoptar decisiones y gestionar los sistemas tecnológicos conforme a los objetivos generales de la compañía[462].

A mediados del siglo XX los avances científicos facilitaron la creación de centros de investigación, cuya dirección se dejaba en manos de un miembro de la compañía que se dedicaba a formar al equipo científico y proponer nuevas

462 Chief Technology Officer (CTO), Definition, *techtarget*, http://searchcio.techtarget.com/definition/Chief-Technology-Officer-CTO

ideas de investigación, pero no formaba parte de las decisiones estratégicas de la misma. Con el desarrollo de las IT a finales de 1980 aumentó el negocio y la dependencia tecnológica, por lo que se empezó a hacer partícipe a aquel director de las decisiones estratégicas de la sociedad[463], lo que permitió la creación del CTO y su inclusión en la dirección de las compañías.

Entre las obligaciones de este director se encuentran, según Paul O'Neill, la capacidad de identificar, acceder y determinar los sistemas de alto riesgo, y maximizar la eficiencia de los sistemas para los negocios existentes y potenciales[464]. De tal forma, los principales cometidos de los CTO son la monitorización, la evaluación y la aplicación a futuros negocios de los sistemas tecnológicos de la compañía[465]. Así, podemos considerar que el CTO tiene un ámbito de actuación transversal que va ganando amplitud con el desarrollo de las IT y su implementación en todos los procesos empresariales. De tal manera, este directivo interviene en todos los procesos de decisión con un alto componente tecnológico, entre los que el artículo «The Role of the Chief Technology Officer in Strategic Innovation» destaca: la adopción de políticas de innovación y estrategia, las operaciones de fusiones y adquisiciones, el marketing y las relaciones con los medios (en la medida en que cada día dependen más del ciberespacio y los sistemas tecnológicos).

Antes del desarrollo de la figura de los CTO solo se reconocía como director tecnológico al CIO, cuya labor se centra en la revisión de procesos y sistemas internos en los que se aplica algún medio tecnológico[466]. De esta forma, el CIO es responsable de la monitorización y el correcto funcionamiento de las IT desde un punto de vista más práctico, mientras que el CTO se encarga del desarrollo de nuevos sistemas y estrategias tecnológicas[467].

---

463 Lewis, W. W. y Lawrence, H. L., «A new mission for corporate technology», *Sloan Management Review*, 31 (1990), en Roger D. Smith, «The Role of the Chief Technology Officer in Strategic Innovation, Project Execution, and Mentoring», Princeton, 2002, p. 3, https://www.cs.princeton.edu/courses/archive/spring12/cos448/web/readings/smith.pdf

464 O'Neill, P. H. y Bridenbaugh, P. R., «Credibility between CEO and CTO — A CEO's perspective»; «Credibility between CEO and CTO — A CTO perspective». *Research Technology Management*, 35 (noviembre-diciembre de 1992), en Roger D. Smith, «The Role of the Chief Technology Officer in Strategic Innovation, Project Execution, and Mentoring», Princeton, 2002, p. 5, https://www.cs.princeton.edu/courses/archive/spring12/cos448/web/readings/smith.pdf

465 Thurlings, B. y Debackere, K. «Trends in managing industrial innovation — first insights from a field survey», *Research Technology Management* (agosto de 1996), en Roger D. Smith, «The Role of the Chief Technology Officer in Strategic Innovation, Project Execution, and Mentorin», Princeton, 2002, p. 6, https://www.cs.princeton.edu/courses/archive/spring12/cos448/web/readings/smith.pdf

466 Roger D. Smith, «The Role of the Chief Technology Officer in Strategic Innovation, Project Execution, and Mentoring», Princeton, 2002, p. 17, https://www.cs.princeton.edu/courses/archive/spring12/cos448/web/readings/smith.pdf

467 Mike Lata, «Reality Check: What's the Difference Between a CTO and CIO?», *Technopedia* (23 de noviembre de 2012), https://www.techopedia.com/2/28883/it-business/it-careers/reality-check-whats-the-difference-between-a-cto-and-cio

En 1982 la Society for Management Information Systems (SMIS) ya adelantó que la importancia de las IT para la estrategia de cualquier organización haría que se atribuyera a los CIO competencias de nivel estratégico y directivo[468]. De tal manera, durante los años 1990 esta posición empezó a participar de las labores propias de la dirección ejecutiva, lo que se ha ido consagrando tras el comienzo del siglo XXI con el potencial desarrollo estratégico de las IT. Actualmente, los CIO ostentan una posición tranversal que depende de los modelos de gestión de información. Así, por norma general, la gestión de la información incide sobre dos niveles: el nivel operativo, que se encarga de la estructura y sistemas de control y transmisión de información; y el nivel estratégico, centrado en la aplicación de aquellos sistemas para la resolución de aspectos propios de la comunicación y el negocio. De tal forma, los CIO son responsables de los sistemas de información[469] y se encargan, desde el punto de vista tecnológico, del desarrollo y mantenimiento de estrategias, estructuras y operaciones relacionadas con los procesos externos e internos de transmisión de información y comunicación[470].

El Chief Information Security Officer (CISO) es aquel directivo responsable de planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones encaminadas a mejorar la seguridad de las IT[471], y en ciertos casos su función se ejercita junto con la del CIO[472]. Así, este sujeto es el responsable directo de la seguridad de una organización en cualquier ámbito relacionado con las IT y al ciberespacio. Y conforme al modelo de CERT (Resilience Management Model), podemos identificar que la función de los CISO se circunscribe a[473]:

- La protección, defensa y prevención, para lo que deberá procurar que el personal, las políticas, los procesos y prácticas tecnológicas sirvan a tal fin. Y de tal manera impidan los cibereventos y mitiguen sus efectos.

468 David F. Feeny, Brian Edwards y Kep Simpson, «Understanding the CEO/CIO Relationship», Oxford Institute of Information Management Templeton College, 1992, http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1058&context=icis1992

469 *Guía terminológica de ciberseguridad*, AGERS, Madrid, 2017, p. 26.

470 Stefanos A. Strickland y Babis Theodoulidis, «Chief Information Officer: A Journey Through Time, Centre for Service Research Manchester Business School University of Manchester», pp. 2-16, http://www.citi.columbia.edu/B8210/read17/CIO.pdf

471 *Op. cit.*, AGERS, Madrid, 2017, p. 26.

472 CISO (Chief Information Security Officer), Definition Techtarget, http://searchsecurity.techtarget.com/definition/CISO-chief-information-security-officer

473 Julia H. Allen, Gregory Crabb, Pamela D. Curtis, Brendan Fitzpatrick, Nader Mehravari y David Tobar, «Structuring the Chief Information Security Officer Organization», Carnegie Mellon University (septiembre de 2015), https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf

- La monitorización de las operaciones y sistemas para detectar vulnerabilidades y posibles intromisiones y el proceso para reportar y advertir sobre su existencia.

- Los procesos de respuesta, recuperación y mantenimiento que se ponen en práctica después de la ocurrencia del ciberevento para tratar de mitigar los efectos del mismo.

- La formación, concienciación y gestión del riesgo, para lo que deberá desarrollar los procedimientos de gestión y prevención necesarios, entre los que destaca la aplicación de un sistema de Compliance que permita revisar la adecuada actuación de la organización.

En definitiva, aunque estas figuras se refieran al desempeño de diferentes cometidos, sus funciones giran en torno a procurar el correcto desempeño de los sistemas y protocolos relacionados con las IT. Por ello, en algunos casos estos cometidos se ejercen por una misma persona o el CISO forma parte del equipo del CIO, a quien reporta de forma directa[474].

6.3. Responsabilidad de los CTO, CIO y CISO

En todo caso, el Chief Executive Officer o administrador es el principal responsable de la gestión y actividad que desempeña una sociedad, de tal forma nuestro ordenamiento jurídico regula en diversas normas el régimen de la responsabilidad —civil, penal, concursal y administrativa— que se atribuye a este sujeto. Actualmente, parece que a los tradicionales riesgos financieros y de gestión cuya responsabilidad era asumida por el administrador se les pueden añadir los daños y amenazas procedentes de los ciberevento a los que hemos ido haciendo referencia. Y en torno a tal responsabilidad se han ido desarrollando las obligaciones de los CIO y CISO, cuya función principal es ofrecer al administrador la información necesaria para poder tomar decisiones relacionadas con las IT. Así, el CIO y CISO facilitan la gestión de los sistemas tecnológicos de una compañía durante todo el ciclo del negocio: desde su implementación y desarrollo, hasta la respuesta y gestión de las situaciones de crisis producidas por los cibereventos.

En todo caso, el régimen de responsabilidad derivado de la actividad de gestión empresarial que se sanciona en la LSC (entre otras normas) se circunscribe exclusivamente al cargo de administrador. De esta forma, ha sido

474 Taryn Aguas, Khalid Kark y Monique François, «The new CISO», *Deloitte Review* (2016), p. 7, https://dupress.deloitte.com/content/dam/dup-us-en/articles/ciso-next-generation-strategic-security-organization/DR19_TheNewCISO.pdf

continua la controversia sobre la posibilidad de hacer extensivo este régimen a algunos sujetos que por su cargo desempeñan actividades propias de la gestión (apoderados universales, gerentes, directores generales y cualquier otro director). La jurisprudencia ha mantenido que la responsabilidad recae sobre los administradores, y para que se atribuya a un apoderado o director, deberá reconocerse que «bajo la apariencia de otras funciones se estaba ejerciendo como auténtico y verdadero administrador» de hecho (SAP La Coruña, 17 de enero de 2000)[475].

De tal manera, la gestión de la sociedad entendida desde la perspectiva orgánica de la LSC solo se puede atribuir al administrador «y por lo tanto el que asume la responsabilidad por los actos sociales» (STS, 30 de julio de 2001), «sin perjuicio de la posible repetición que pudiera tener lugar en el seno del ente social» (SAP Barcelona, 24 de enero de 2005). Así, aunque los CIO y CISO desempeñen verdaderas funciones de gestión, solo participarán del régimen de responsabilidad del CEO en aquellos casos en los que pueda atribuirse a estos parte de la responsabilidad de forma individual (como en los casos en los que el administrador incumpla su deber de estar informado de aquello a lo que el CIO o CISO estaban obligados a informar). Sin perjuicio de la responsabilidad que pueda surgir de la regulación especial, como en el caso de los responsables del tratamiento de datos, y de aquellos daños que surjan de una acción u omisión atribuible a estos.

Durante las primeras etapas a las que hemos hecho referencia los CIO asumían la dirección del mantenimiento de los centros de datos y las aplicaciones críticas, pero progresivamente se les ha ido atribuyendo responsabilidades y competencias propias de la gestión de ciertas áreas de la compañía. Así, actualmente se encargan de determinar y establecer las necesidades tecnológicas de la compañía, por lo que es responsable de que los sistemas IT se adecuen al funcionamiento y al negocio desempeñado por la misma. Y en relación con la seguridad de los sistemas, el CIO es responsable de que dentro de los procesos de la compañía se lleven a cabo estrategias que, a su vez, permitan garantizar la aplicación de medidas de ciberseguridad en el ciclo productivo y el funcionamiento de la organización relativas a:

- El análisis del impacto de los ciberriesgos en el negocio.
- Identificar los sistemas críticos.

475 Fernando Martínez Sanz, «Los administradores responsables», en Ana Belén Campuzano (coord.), *La responsabilidad de los administradores en las sociedades mercantiles*, Tirant lo blanch Tratados, Valencia, 4.ª edición, 2011, p. 83.

- Los objetivos de recuperación tras un ciberevento.
- Los procesos necesarios para asegurar que los servidores, sistemas y aplicaciones están configurados de acuerdo con las bases establecidas.
- Incentivar y comprobar la efectiva utilización de técnicas de codificación segura.
- Los procesos de control de acceso de terceros a las redes y sistemas de la compañía.
- Los procesos de seguimiento y auditoría de los sistemas IT.
- La utilización eficiente y la inversión en recursos tecnológicos que permitan proteger a la compañía de vulnerabilidades y fallos.

En definitiva, concluye el artículo «Clarifying the Roles of Information Security» que el CIO tiene la responsabilidad de: procurar que se realizan las oportunas inversiones en IT de acuerdo con el negocio y estrategia de la compañía; asegurar que la información solo es accesible para aquellos que están autorizados; y gestionar de manera adecuada los recursos tecnológicos para procurar el mayor grado posible de seguridad[476].

El departamento de Seguridad Tecnológica normalmente forma parte del departamento de IT liderado por el CIO, por lo que, como se ha dicho, el CISO suele depender del CIO. Así, el CISO se encarga de supervisar todos los asuntos relativos con la seguridad en las IT, y en concreto es responsable de:

- Facilitar la implementación de programas de *Compliance*.
- Revisar la correcta utilización de herramientas de seguridad.
- Controlar que se están siguiendo las políticas de seguridad.
- Analizar y recomendar que las medidas de seguridad se adecuen al riesgo y los medios existentes.
- Colaborar con el CIO en la gestión de las situaciones de crisis derivadas de un ciberevento.

476 Todd Fitzgerald, «Clarifying the Roles of Information Security», Taylor & Francis Group (2007), pp. 259-261.

En definitiva, el CISO se encarga principalmente de analizar e informar de los riesgos y de las posibles medidas de seguridad al CEO, que es quien toma las decisiones y asume los riesgos oportunos[477]. Y en particular, las normas en materia de protección de datos (la LOPD y el nuevo Reglamento 2016/679, de 27 de abril de 2016) reconocen como encargado y responsable del tratamiento de los mismos a cualquier «persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento» (artículo 4.7 del reglamento), lo que podría encajar con los cometidos del CIO o CISO.

De esta forma, la progresiva determinación de los cometidos que desempeñan los CIO y CISO permitirá individualizar la responsabilidad sobrevenida de los ciberevents con mayor facilidad. No obstante, en atención al contenido de aquellos cometidos, parece que la responsabilidad que procede de un ciberevento y que sea relativa al ámbito de administración y gestión empresarial seguirá recayendo de forma exclusiva sobre los miembros del consejo de administración, CEO o administradores.

Aunque como mantiene Parra Lucán[478], «fuera de los casos en los que la actuación del órgano excede de las funciones que le corresponden» resulta difícil asignar los criterios por los que se debe atribuir la responsabilidad a unos u otros miembros. Y ello refuerza la aplicación del criterio de la responsabilidad basada en la culpa «dirigida a imputar personalmente a quienes se encargan de la gestión las consecuencias derivadas de una actuación negligente». Además, este criterio de la responsabilidad por culpa permite reclamar de forma conjunta o directamente contra los CIO y CISO en aquellos casos en los que se puedan individualizar las causas del daño, y siempre que estas sean atribuibles a su ámbito de responsabilidad.

Así, Daniel Garrie ya mantenía en su artículo publicado en 2015[479] que cabe esperar un aumento de las reclamaciones dirigidas directamente contra los CIO y CISO como consecuencia de los daños y perjuicios causados por el incumplimiento o del defectuoso cumplimiento de sus funciones. De tal manera, considera que un buen ejemplo de ello había sido la demanda dirigida contra el CIO de U.S. Office of Personnel Management (OPM) como consecuencia de una brecha de seguridad que dejó desprotegida la información personal de millones de trabajadores y contratos públicos.

---

477 Todd Fitzgerald, *op. cit.*, Taylor & Francis Group (2007), pp. 261-262.

478 M.ª Ángeles Parra Lucán, «Lección 17.ª La responsabilidad civil de los administradores», *Lecciones de responsavilidad civil*, 2013, Dykinson, pp. 505-515.

479 Daniel Garrie, «Do CIOs and CISOs Get Covered in Cybersecurity Litigation?», Bloomberg (26 de agosto de 2015), https://bol.bna.com/do-cios-and-cisos-get-covered-in-cybersecurity-litigation/

En este sentido, el referenciado autor mantiena que los CIO o CISO son un objetivo «natural» de las reclamaciones dirigidas por quien se haya visto perjudicado como consecuencia de un ciberevento. Pues, en definitiva, responden del buen funcionamiento de las IT y de la seguridad implementada para su protección, ya que en la mayoría de casos se encargan de la creación e implantación de las políticas y prácticas de seguridad[480]. Así, se podrá reconocer la responsabilidad de los CIO y los CISO si finalmente resulta que la compañía ha sufrido un ciberevento como consecuencia de la falta de implantación de aquellas políticas o de la existencia de algún defecto en los procedimientos de ciberseguridad.

No obstante, conforme a la sentencia del Tribunal Supremo de 2 de marzo de 2009 «el nexo de causalidad no puede ser establecido únicamente en el plano fenomenológico atendiendo exclusivamente a la sucesión de acontecimientos en el mundo externo, sino que la causalidad física debe ser acompañada de una valoración jurídica en virtud de la cual, con criterios tomados del ordenamiento, pueda llegarse a la conclusión de que el daño causado se encuentra dentro del alcance de la conducta del agente, en virtud de lo que en nuestro ámbito científico suele llamarse imputación objetiva».

De tal manera que la existencia de un daño efectivamente causado no puede servir de pretexto (según mantiene el profesor Yzquierdo) para la extensión del régimen de responsabilidad objetiva a cualquier ámbito. Así, tal responsabilidad sin culpa dejaría a los CIO y CISO en una posición muy vulnerable, ya que responderían frente a cualquier daño causado por un ciberevento en un entorno ilimitado —el ciberespacio— y sin posibilidad material de prueba en contrario.

En este sentido, los ciberriesgos ponen de manifiesto que los planteamientos como la objetivización de la responsabilidad han quedado obsoletos en el mundo actual. Pues bien, circunstancias tales como la hiperconectividad impiden la estimación del riesgo en el ciberespacio y producirían una enorme acumulación de riesgo sobre determinados sujetos. Y si a esto le unimos la imposibilidad material de garantizar la seguridad plena de cualquier sistema relacionado con las IT, podría ocasionar una atribución automática y desmedida de los daños derivados de ciberevento a las compañías que operan en el ciberespacio, los CIO y los CISO, que, como hemos visto, ralentizaría el desarrollo socioeconómico global.

480 Daniel Garrie, *op. cit.*, *Bloomberg* (26 de agosto de 2015), https://bol.bna.com/do-cios-and-cisos-get-covered-in-cybersecurity-litigation/

6.4. Concurrencia de responsabilidades entre directivos

Los supuestos en los que de una u otra forma se puede llegar a apreciar la concurrencia de responsabilidad civil derivada de un ciberevento son múltiples y se encuentran en continua evolución. De esta forma, el resultado de la hiperconectividad y el continuo desarrollo de las IT han llevado a que una gran cantidad de decisiones empresariales tengan un efecto directo en el ciberespacio.

En este sentido, mantiene el informe «Cybersecurity and Corporate Liability: The Board's View» (Veracode, 2015)[481] que las decisiones relativas a la ciberseguridad han aumentado la presión de los equipos de dirección y gestión en relación con el funcionamiento de la sociedad y la responsabilidad derivada de su gestión. Así, parece que tal preocupación es además un deber inexcusable si consideramos el aumento generalizado de los cibereventos, las sanciones y reclamaciones que estos vienen produciendo y la abundante información sobre los ciberriesgos[482]. Además, tal deber puede aplicarse a cualquier sujeto que interactúe en el ciberespacio por medio de un sistema que pueda llegar a causar un daño a otro.

En el ámbito de la dirección y gestión empresarial, la responsabilidad se proyecta frente a la sociedad y sus socios, y cualquier tercero que pueda sufrir un daño derivado de tales acciones que se circunscriben a:

- La gestión de los sistemas de control de ciberseguridad.
- Las políticas de inversión y renovación de los sistemas de IT de la compañía.
- La promoción y control de la implantación de sistemas y políticas de prevención.
- El desarrollo y control de políticas de actuación frente a un ciberevento.
- La gestión eficaz de los cibereventos.

En todo caso, parece que los órganos de administración serán los últimos responsables de velar por el efectivo cumplimiento de estas acciones. Así, igual que vienen realizando en otros ámbitos, deberán emplear cuantos medios

481 «Cybersecurity and Corporate Liability: The Board's View», *Veracode*, 2015, p. 2, https://www.nyse.com/publicdocs/Veracode_Survey_Report_Cybersecurity_Corporate_Liability.pdf

482 *Op. cit.*, *Veracode*, 2015, p. 2, https://www.nyse.com/publicdocs/Veracode_Survey_Report_Cybersecurity_Corporate_Liability.pdf

sean necesarios para garantizar la integridad cibernética de la sociedad. Y ello, dentro de los límites de su actividad de gestión y coordinación de los medios empresariales, y superditado al estado de la ciencia y sistemas de los que se puede disponer en cada momento.

Sin perjuicio de la responsabilidad del órgano de administración de una sociedad que ha sido ampliamente desarrollada por el ordenamiento jurídico español, pueden concurrir diversos niveles de responsabilidad que dependerán de la estructura de cada compañía y de las funciones atribuidas a cada directivo.

Así, el desarrollo de las IT y los efectos que los ciberriesgos pueden llegar a causar sobre la actividad empresarial han llevado a la atribución de la responsabilidad y cometidos de los CIO y CISO, que se dedican de forma directa al control y aplicación de las políticas y actuaciones mencionadas. De esta forma, se encargan de informar al órgano de administración sobre la situación, riesgos, necesidades y oportunidades relacionados con los sistemas de las IT y la ciberseguridad de la compañía. Por ello, parece probable que después de que un ciberevento afecte a una compañía se revise y ponga en duda la actuación de estos directivos, ya que se tratan de los responsables directos de la gestión de las IT y el ámbito cibernético de la compañía.

En todo caso, deberá acreditarse que concurren los requisitos de la responsabilidad civil y que el daño no se produjo como consecuencia de una obligación propia del ámbito de la gestión empresarial que corresponda a su administrador. De tal forma, podrá derivarse la responsabilidad de un ciberevento a los CIO o CISO siempre que se acredite que el órgano de administración había asignado los medios suficientes y desarrollado las políticas organizativas tendentes a permitir la prevención de ciberevents y sus efectos.

7. CONCLUSIONES

La utilización de las IT se ha ido introduciendo en cada uno de los aspectos básicos de la vida diaria, las relaciones empresariales y el ámbito socioeconómico en general desde la creación de los primeros sistemas informáticos. Y en la actualidad, sus efectos se hacen más evidentes que en cualquier otro momento por medio de la hiperconectividad que entre otros sistemas se pone de manifiesto por medio del Internet of Things. De esta manera, los efectos generales del ciberespacio y de la evolución de las IT ha hecho que se les atribuya la calificación de Cuarta Revolución Industrial.

Tal importancia hace que cualquier sistema tecnológico que se encuentre conectado a otro pueda provocar o padecer algún daño, cuyos efectos se pueden poner de manifiesto sobre todo en aquello que dependa de manera directa o indirecta de ese sistema. Así, parece que la incidencia de las IT sobre una cantidad ilimitada de actividades públicas y privadas que se encuentran continuamente conectadas a internet determina los 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 «Risk and Responsibility in a Hyperconnected World» considera que este carácter ilimitado y abierto plantea tres cuestiones fundamentales con las que podemos definir, a grandes rasgos, el alcance de los ciberriesgos. De tal forma el informe considera:

- 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.

Por ello, hemos abordado el estudio de los ciberriesgos desde diversas perspectivas, que nos han permitido presentar los aspectos técnicos y definiciones

esenciales de este ámbito, y señalar los bienes y derechos que pueden resultar afectados por los mismos. 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, establece 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 en el que bienes y derechos de toda índole pueden llegar a resultar amenazados e incluso sufrir algún daño, menoscabo o deterioro, al que se ha denominado «ecosistema digital». Desde esta perpectiva, parece importante destacar que la ciberseguridad constituye una materia esencial para evitar los efectos adversos de los cibereventos tanto en el ámbito físico como en el propio ciberespacio. Y trata de impedir que de una u otra forma se ponga en riesgo la integridad de un número ilimitado de bienes y derechos.

En este sentido, nos hemos referido al conjunto de intereses individuales y colectivos que pueden resultar afectados por un ciberevento como aquellos que forman parte o que están relacionados con los elementos físicos o teleológicos del ciberespacio, por lo que constituyen una realidad cambiante que depende del estado y desarrollo de las IT. Así, resulta útil partir de unas pautas básicas que permitan identificar los elementos de los bienes y derechos afectados, que hemos clasificado en cuatro grupos:

1. Las cuestiones de interés general y seguridad nacional.

2. Los datos.

3. Las estructuras y sistemas.

4. Los daños de carácter inmaterial.

El primer grupo es particularmente relevante para nuestro estudio ya que nos ha permitido delimitar el ámbito del Derecho Privado en el ciberespacio. Así, resulta que la relevancia del ciberespacio hace que ante un ciberevento puedan concurrir las normas del derecho público y privado, lo que dependerá del interés jurídico que resulte afectado. De esta forma, hemos puesto de manifiesto diversas normas de carácter penal y administrativo que resultan de aplicación para supuestos tales como:

- La protección del interés público del ciberespacio, que permite situar a la ciberseguridad dentro del interés colectivo que pretende prevenir los daños procedentes de las acciones de guerra, terrorismo, el cibercrimen y

otros eventos susceptibles de ocasionar daños sobre elementos y sistemas que afectan al interés general como las infraestructuras críticas.

- El cibercrimen ocasiona un daño económico muy relevante y distorsiona el correcto funcionamiento y desarrollo del ciberespacio. De esta forma, la repercusión socioeconómica de los denominados ciberdelitos ha motivado la creación de disposiciones penales que regulan la responsabilidad penal aplicable a estos casos.

- El ciberterrorismo engloba aquellos actos y ataques que afectan a un Estado o que tienen por finalidad principal infundir terror a personas individuales, grupos de personas o al público en general. Este término se utiliza de forma generalizada para hacer referencia a la procedencia de un gran número de ciberataques, por lo que su delimitación y determinación conceptual ha sido un aspecto esencial en nuestro estudio. Así, esta calificación produce efectos de gran relevancia en relación con la responsabilidad y la cobertura de los seguros, ya que en muchos casos podrán encontrarse excluidos. Y ello, a pesar de que no hay consenso sobre una metodología concreta que posibilite calificar un acto con el carácter de ciberterrorismo. En la mayoría de los casos este calificativo no responde a un reconocimiento oficial de acto terrorista, lo que podría dar lugar a confusiones.

La posible responsabilidad derivada del desarrollo de una actividad o actuación concreta en el ciberespacio es muy amplia y despliega sus efectos en diversos ámbitos del ordenamiento jurídico. Así, el IoT y las infraestructuras críticas ponen de manifiesto la influencia que los ciberriesgos pueden llegar a tener sobre toda clase de bienes y derechos, desde aquellos que se circunscriben a las actividades individuales, industriales y corporativas (conectadas por medio del IoT), hasta el mantenimiento de las estructuras más relevantes para el ámbito socioeconómico (como las estructuras energéticas o los sistemas de transporte).

Los cibereventos están formados por diversas circunstancias esenciales que permitirán determinar los elementos de la atribución de la responsabilidad que puedan concurrir en el caso concreto, entre los que destaca:

- **La procedencia o acción que origina los cibereventos,** que puede derivar de un fallo en los sistemas o procesos, y en su caso ser consecuencia de una acción voluntaria o involuntaria.

  En la mayoría de casos resulta verdaderamente complejo determinar el origen del ciberevento, lo que dificultará la atribución de una responsabilidad concreta. Así, existe una gran cantidad de cibereventos que se transmiten entre los sistemas de terceros ajenos al origen del mismo, por lo que podría llegar a reconocerse la responsabilidad de estos sujetos intermedios.

Y también son numerosos los supuestos en los que se declara que el ciberevento proviene de un acto de cyberwar, ciberterrorismo, ciberactivismo o vandalismo, lo que permitiría atribuir al supuesto concreto el carácter de fuerza mayor, y excluir la responsabilidad de los sujetos intermedios.

- **La forma de manifestarse** y los sistemas que resultan afectados por un ciberevento determinan la causalidad que pueda existir entre el efecto que estos producen en el sistema propio y los daños que de este se derivan a terceros.

  En este sentido, parece esencial la determinación del grado de diligencia a la que resulta obligado cada sujeto o entidad, de manera que todos los sujetos que forman parte del ciberespacio se pueden encontrar obligados a mantener un mínimo de ciberseguridad. Y esto dependerá, entre otras circunstancias, del carácter y sensibilidad de los sistemas y datos que trata cada individuo. Entre ellos, destaca la responsabilidad de los CIO y CISO como directores responsables de los sistemas tecnológicos y de la ciberseguridad de las compañías, cuya labor ha superado el ámbito operativo al haberles atribuido competencias relativas a la gestión de recursos, políticas e incidencias.

- **Los efectos** que producen los ciberеventos sobre los elementos externos al sistema dañado son determinantes del verdadero riesgo, y permiten concretar los daños que los elementos y relaciones del ciberespacio pueden causar sobre bienes y derechos (concretos determinados y pertenecientes a la realidad material). Y para ello, será necesario que un evento que acontece en el ciberespacio produzca un daño real, cuyos efectos se deben desarrollar en el ámbito material, social, personal, empresarial, político, jurídico institucional o económico.

La responsabilidad civil es una consecuencia necesaria y esencial de los ciberеventos, por lo que se han estudiado sus elementos a la luz de las circunstancias y supuestos que concurren en el ciberespacio. De tal manera, el presente estudio permite aplicar los modelos tradicionales de la responsabilidad civil a las acciones dañosas procedentes del ciberespacio. Y, además, plantea las particularidades que la evolución del ciberespacio puede llegar a poner de manifiesto con relación a la determinación del sujeto causante del daño y la atribución de la responsabilidad. Todo ello vendrá necesariamente favorecido por el desarrollo de la ciencia y de los pronunciamientos jurisprudenciales sobre conclusiones tales como:

- La calificación de los bienes cibernéticos como bienes intangibles que en ciertos casos pueden ser determinables y valorables.

- La ratificación de que el criterio de la objetivación del daño se debe superar en favor del estudio de las circunstancias que coadyuvan al resultado

dañoso, la culpa, y el necesario estudio de la diligencia con la que el agente actuó en cada caso.

- La determinación de las circunstancias de especial riesgo, o de riesgo general para la vida en el ciberespacio, que dependerá tanto de la gravedad de las circunstancias, como de los efectos que pueden llegar a ocasionarse.

- La importancia de la aplicación restrictiva de la responsabilidad por daños ajenos, además de la atribución de la lógica exoneración para los casos en los que, cumplido con la diligencia debida, se pusieron todos los medios para evitar el daño.

Llegados a este punto ya solo queda hacer referencia a la importancia que tiene la adecuada gestión de los riesgos cibernéticos ya que, como hemos advertido, en ciertos casos los cibereventos son circunstancias insalvables e impredecibles.

Por ello, la implantación de sistemas de prevención adecuados permitirá acreditar que se actuó con la diligencia suficiente, y así evitar la atribución de responsabilidad. De esta misma forma, los métodos de gestión de incidencias que en muchos casos dependen de los CIO y CISO son una herramienta esencial para impedir que los daños se propaguen por los sistemas de la compañía y llegen a terceros. Además, permiten actuar de manera eficiente y cumplir con la regulación en materia de notificación de incidentes para evitar la imposición de sanciones y la consecución de daños de mayor entidad.

En definitiva, el carácter inevitable de los cibereventos determina la necesidad de transferir el riesgo derivado de los mismos a la industria aseguradora por medio de los nuevos productos que de manera específica se están desarrollando para la cobertura de estos daños.

Así, una vez que se ha analizado el entorno y características de los ciberriesgos, los bienes y derechos que pueden llegar a resultar afectados, y la responsabilidad que puede llegar a surgir de un ciberevento, será conveniente elaborar un estudio sobre el contenido y características de los seguros que cubren tal responsabilidad y daños. De tal forma, los medios de gestión del riesgo y los seguros son las herramientas de las que dispone la sociedad civil para lidiar con los efectos adversos del ciberespacio, y lo que permite mantener a este ámbito libre de la necesidad de una regulación excesivamente proteccionista.

La diversidad de intereses y objetos que pueden resultar afectados por los cibereventos a la que hemos hecho referencia nos permite advertir sobre la posible concurrencia de seguros, además de la aplicación de límites y exclusiones como consecuencia del origen o dinámica del ciberevento. En este

sentido, ya hemos advertido sobre los efectos que la calificación de ciberterrorismo o ciberguerra pueden causar sobre la atribución de la responsabilidad. Y esto, además, tiene una evidente consecuencia en cuanto a la cobertura aseguradora, ya que se tratan de riesgos extraordinarios que están generalmente excluidos por las pólizas, y de cuya cobertura se encargan instituciones como el Consorcio de Compensación de Seguros en España y los pools de aseguradoras y reaseguradoras en el resto de Europa.

En el ámbito de la responsabilidad civil, los daños a terceros derivados de una acción u omisión que se desarrolla o tiene lugar por medio del ciberespacio podrían ser atribuibles a las pólizas de responsabilidad civil general. Y ello, siempre que el objeto asegurado no cambie como consecuencia del carácter cibernético del medio, por lo que los ciberriesgos se han ido excluyendo y delimitando en dichas pólizas.

En definitiva, como continuación al presente estudio sería apropiado elaborar una ponderación de los ciberriesgos que puedan resultar cubiertos por las pólizas pertenecientes a este ramo, ya que, como hemos visto, en el ciberespacio concurren múltiples relaciones de las que pueden derivarse diversas obligaciones y responsabilidades.

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

BIBLIOGRAFÍA

Aberasturi Gorriño, Unai, *Revista Aragonesa de Administración Pública*, n° 41-42, Zaragoza, 2013, pp. 179-180, http://w.aragon.es/estaticos/GobiernoAragon/Organismos/InstitutoAragonesAdministracionPublica/Areas/03_Revista_Aragonesa_Formacion/04%20Unai%20Aberasturi.pdf

«Abkommen zwischen dem Schweizerischen Bundesrat und der Stiftung World Economic Forum zur Festlegung des Status der Stiftung World Economic Forum in der Schweiz, Privilegien und Immunitäten». Abk mit der Stiftung World Economic Forum, 2015, http://www.news.admin.ch/NSBSubscriber/message/attachments/38059.pdf

«Abuso del derecho», *Guías jurídicas*, wolterskluwer, http://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAEAMtMSbF1jTAAAUNDYwsLtbLUouLM_DxbIwMDCwNzA7BAZlqlS35ySGVBqm1aYk5xKgB-Pb9sNQAAAA==WKE

«Advanced Targeted Attacks: How to Protect Against the New Generation of Cyber Attacks,» *FireEye*, 2015, p. 4, http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-targeted-attacks.pdf

Aguas, Taryn, Kark, Khalid y François, Monique, «The new CISO», *Deloitte Review* (2016), p. 7, https://dupress.deloitte.com/content/dam/dup-us-en/articles/ciso-next-generation -strategic-security-organization/DR19_TheNewCISO.pdf

Albadalejo, M., *La responsabilidad por culpa extracontractual levísima*, Real Academia de Jurisprudencia y Legislación, Madrid, 2000, p. 15 y ss.

Albiol Montesinos, I., Alfonso Mellado, C. L., Blasco Pellicer, A., Goerlich Peset, J. M., *Derecho Procesal Laboral*, Tirant lo Blanch, Valencia, 1996, p. 38.

Alfaro, Jesús, «Derecho de la Propiedad Industrial: Patentes y Marcas», UAM, https://www.uam.es/personal_pdi/derecho/bbagooria/ADEPiloto/Leccion%205%20-%20Propiedad%20Industrial.pdf

Allianz Global Corporate & Specialty, *A Guide to Cyber Risk* (septiembre de 2015), https://www.allianz.com/v_1441789023000/media/press/document/other/Allianz_Global_Corporate_Specialty_Cyber_Guide_final.pdf

Alonso Soto, Ricardo, «Responsabilidad civil y seguros», https://www.uam.es/otros/afduam/pdf/4/Responsabilidad%20civil%20y%20Seguro%20Ricardo%20Alonso%20Soto.pdf

Álvarez Vizcaya, M., *Consideraciones político-criminales sobre la delincuencia informática: el papel del Derecho Penal en la red, en internet y Derecho Penal*, Consejo General del Poder Judicial, nº 10, 2001.

AMCC TF on Cyber Resilience and AMCC Working Group, *Cyber Security in Securities Markets An International Perspective*, IOSCO (abril de 2016), pp. 23 y 24, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf

Anderson, James M., Kalra, Nidhi, Stanley, Karlyn D., Sorensen, Paul, Samaras, Constantine y Oluwatola, Oluwatobi A., «Autonomous Vehicle Technology», RAND Corporation (2016), http://www.rand.org/content/dam/rand/pubs/research_repor ts/RR400/RR443-2/RAND_RR443-2.pdf

Andrés Domínguez, A. C., *El delito de daños: consideraciones jurídico-políticas y dogmáticas*, Ed. Universidad de Burgos, 1.ª edición, Burgos, 1999, p. 122.

Ángel Yágüez, R. de, *Tratado de responsabilidad civil*, Madrid, 1993, p.126.

Ángel Yágüez, R. de, *La responsabilidad civil*, Universidad de Deusto, Bilbao, 2.ª edición, 1989, p. 21.

Anderson, Ross, «Measuring the Cost of Cybercrime», 2012, http://www.econinfosec. org/archive/weis 2012/papers/Anderson_WEIS2012.pdf

«Annual U.S. Cybercrime Costs Estimated at $100 Billion», *The Wall Street Journal* (22 de julio de 2013), http://online.wsj.com/articles/SB10001424127887324328904578621880966242990.

Aparicio Salom, J.: *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Ed. Aranzadi, Cizur Menor, 2.ª edición, 2002, p. 167.

Aquino, Santo Tomás de. *Comentario a la ética a Nicómaco de Aristóteles*, trad. Ana Mallea, Eunsa, Pamplona, 2012, p. 304.

Arenas García, Rafael; Fernández Rozas, José Carlos y Miguel Asensio, Pedro Alberto de, *Derecho de los Negocios Internacionales*, Iustel, Madrid, 4.ª edición, 2013.

Arquillo Colet, Begoña, «Anotaciones al reglamento del seguro de riesgos extraordinarios», *InDret*, Barcelona (abril de 2004), http://www.indret.com/pdf/213_es.pdf

«Ashley Madison hack reveals IT 37 million users deepest sexual fantasies», *Independent* (20 de agosto de 2015), http://www.independent.co.uk/life-style/love-sex/ashley-madison-hack-reveals-IT-37-million-users-deepest-sexual-fantasies-10463985.html

Ashton, Catherine, «Plan de ciberseguridad de la UE para proteger una red abierta plena de libertad y de oportunidades en línea», Comunicado de prensa, Comisión Europea (7 de febrero de 2013), http://europa.eu/rapid/press-release_IP-13-94_es.htm

Asúa Batarrita, «Concepto jurídico del terrorismo y elementos subjetivos», en Echano Basaldua, J. (coord.), *Estudios jurídicos en memoria de José María Lidón*, Universidad de Deusto, Bilbao, 2002, pp. 41-85.

Bacaria Gea, Júlia, «Aspectos TIC en la reforma del Código Penal», GLD (3 de junio de 2015), http://legal-data.net/aspectos-tic-en-la-reforma-del-codigo-penal/

Badillo Arias, José A., «El dolo y la culpa en el contrato de seguros», http://www.asociacionabogadosrcs.org/doctrina/doct33-1.pdf

Bailard, Fred, Busony, Brian y Lilienthal, Gene, «Call the FED Cybercrime», FRBSF (14 de marzo de 2013), http://www.frbsf.org/banking/audioconf/031413/Call-the-Fed

Barlow, Jhon Perry, «A Declaration of the Independence of Cyberspace», *Electronic Frontier Fundatio EFF* (8 de febrero de 1996), https://www.eff.org/es/cyberspace-independence

Bartley, William Alan, «Valuation of Specific Crime Rates: Final Report» http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2835847/#R12 y https://www.ncjrs.gov/pdffiles1/pr/188070.pdf

Bendrath, Ralf, «The American Cyber-Angst and the Real World-any Link?», University of Bremen, New York, *The New Press* (2003).

Bercovitz Rodríguez-Cano, R., «Sentencia de 15 de abril de 1992. Derecho al honor. Extensión a las personas jurídicas», *Cuadernos Civitas de Jurisprudencia Civil*, nº 29 (1992).

Biener, Christian, Eling, Martin y Wirfs, Jan Hendrik, *Working papers on Risk Management and Insurance*, nº 151, University of St. Gallen (enero de 2015), http://

www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.pdf

«Big brother: a government or person in authority that tries to control people's behavior and thoughts», *Cambridge Dictionary,* http://dictionary.cambridge.org/us/dictionary /english/big-brother

«Big data: Changing the way businesses compete and operate», *EY* (abril de 2014), http://www.ey.com/Publication/vwLUAssets/EY_Big_data:_changing_the_way_businesses_operate/$FILE/EY-Insights-on-GRC-Big-data.pdf

Bishop, J., «Increasing participation in online communities: A framework for human-computer interaction», *Computers in Human Behavior*, Elsevier Science Publishers, 2007, https://trac.v2.nl/export/7500/andres/Documentation/Behaviour%20modification/Increasing%20participation%20in%20online%20communities.pdf

Blank, «The Commerce Blog», U.S. Department of Commerce (29 de noviembre de 2011).

Bogdanoski, Mitko y Petreski, Drage, «Cyber Terrorism-Global Security Theart, International Scientific Defence», *Security and Peace Journal,* http://eprints.ugd.edu.mk/6849/1/CYBER%20TERRORISM%E2%80%93%20GLOBAL%20SECURITY%20THREAT%20-%20Mitko%20Bogdanoski.pdf

Böhme, Rainer y Schwartz, Galina, «Modeling Cyber-Insurance: Towards a Unifying, the Economics of Information Security (WEIS)», Harvard (junio de 2010), http://www.econinfosec.org/archive/weis2010/papers/session5/weis2010_boehme.pdf Frameworhttp://static1.squarespace.com/static/53b2efd7e4b0018990a073c4/t/53c3daa5e4b056f825681c72/1405344421345/cyberinsurance_paper_pdf.pdf

Brad S. Karp, Paul y Weiss, Rifkind, «Federal Guidance on the Cybersecurity Information Sharing Act of 2015», Harvard Law School Forum on Corporate Governance and Financial Regulation (3 de marzo de 2016), https://corpgov.law .harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/#6b

Bradley, Tony, *Lifewire* (14 de octubre de 2016), https://www.lifewire.com/zero-day-exploIT-2487435

Brandom, Russell, «Is Microsoft to blame for the largest ransomware attacks in internet history?», *The Verge* (15 de mayo de 2017), https://www.theverge.com/2 017/5/15/15641198/microsoft-ransomware-wannacry-security-patch-upgrade-wannacrypt

Braun, Hans Werner, «The new NSFNET backbone network», *ACE ConneXions*, vol. 2, nº 12 (diciembre de 1988).

Briscoe, G. y De Wilde, P., «Digital Ecosystems: Evolving service-oriented architectures», Conference on Bio Inspired Models of Network, Information and Computing Systems. IEEE Press (2006), https://arxiv.org/abs/0712.4102

Brown, Eric, «Who Needs the Internet of Things?», *Linux.com* (13 de septiembre de 2016).

Busto Lago, José Manuel y Reglero Campos, Fernando L. (coord.), «Lección 2.ª Los sistemas de responsabilidad», en *Lecciones de responsabilidad civil*, Aranzadi, Navarra, 2013, p. 42.

Busto Lago, José Manuel, «La responsabilidad civil de los servidores y operadores de datos», Seminario sobre Protección de Datos, Ciudad Real (9 y 10 de noviembre de 2005), http://www.uclm.net/actividades0506/seminarios/proteccion_datos/pdf/busto.pdf

Butler, Jeremy G., *A History of Information Technology and Systems*, University of Arizona.

Buttarelli, G., *Banche dati e tutela della riservatezza (La privacy nella Società dell'Informazione)*, Giuffrè Editore, Milán, 1997, pp. 351 y 352.

Bux, Udo. «La propiedad intelectual, industrial y comercial. Fichas técnicas sobre la Unión Europea». Parlamento Europeo (octubre de 2016), http://www.europarl.europa. eu/atyourservice/es/displayFtu.html?ftuId=FTU_3.2.4.html

Cannar, Kenneth, *Liability Insurance Claims*, London Witherby & Co, 1978, p. 69.

Capita Remezal, M. «Análisis de la legislación», pp. 27-28 y 37-44.

Carbonell Mateu, J. C. *Derecho Penal: concepto y principios constitucionales*, Valencia, Tirant lo Blanch, 3.ª edición, 1999.

Cardona Llabrés, Carla y Miquel Rodríguez, Jorge, «La propiedad intelectual aplicada a internet y el efecto sobre la creatividad», Universitat Autònoma de Barcelona (15 de mayo de 2015), https://ddd.uab.cat/pub/tfg/2015/132932/TFG_ccardonallabres.pdf

Carr, Jeffrey, «Inside Cyber Warfare», O'really (2010), https://wikileaks.org/sony/docs/05/docs/eBooks/Inside_Cyber_Warfare.pdf

CASANOVAS YSLA, Alain (coord.), *Libro blanco sobre la función del* Compliance, Asociación Española de Compliance, Madrid (marzo de 2017), p. 5.

CASTELLS, M., *The Rise of the Network Society,* Oxford, Blackwell, 1996.

CASTELO MATRÁN, J. y GUARDIOLA LOZANO, A., *Diccionario MAPFRE de Seguros*, Ed. FME, Madrid, 1992.

CEBULA, James J. y YOUNG, Lisa R., «A Taxonomy of Operational Cyber Security Risks», Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 15213, (diciembre de 2010), http://bit.ly/1NEBcTU

CEREIJO, M., «Cuba the threat II: Cyberterrorism and Cyberwar» (16 de mayo de 2006), http://www.lanuevacuba.com/archivo/manuel-cereijo-110.htm

CHANG, E., QUADDUS, M. y RAMASESHAN, R. «The Vision of DEBI Institute: Digital Ecosystems and Business Intelligence», DEBII, 2006.

Chicago Mercantile Exchange, CME Group Confirms Cyber Intrusion (15 de noviembre de 2013), http://investor.cmegroup.com/investor-relations/releasedetail.cfm? ReleaseID=807750

Chief Economists Note, European Commission, Trade, *Issue* 2, 2012, http://trade.ec.europa

Chief Technology Officer (CTO), Definition, *Techtarget,* http://searchcio.techtarget.com/definition/Chief-Technology-Officer-CTO

Child Protection Act of 2012, Congressional Budget Office Cost Estimate (30 de julio de 2012), http://www.cbo.gov/sites/default/files/cbofiles/attachments/hr6063.pdf

«Ciberespacio», *Diccionario de la Lengua Española,* Edición del Tricentenario, RAE, http://dle.rae.es/?id=98Wdd57

«Ciberriesgo, seguridad, redes y privacidad, Finex Global», *Willis,* https://welcome.willis.com/finexeventcalendar/Shared%20Documents/FINEX%20PI/Cyber/Cyber%20Brochure%20-%20Spanish%20version.pdf,

«Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio», *Cuadernos de Estrategia*, nº 149, Ministerio de Defensa (diciembre de 2010), https://www.cni.es/comun/recursos/descargas/Cuaderno_IEEE_149_Ciberseguridad.pdf

«Ciberseguros», *Thiber* (abril de 2016), p. 52, http://www.thiber.org/ciberseguros.pdf

CISCO 2010. «The Evolving Internet: Driving Force, Uncertainties, and Four Scenarios to 2025». Disponible en http://newsroom.cisco.com/dlls/2010/ekIT/Evolving_Internet _GBN_Cisco_2010_Aug_rev2.pdf

CISO (Chief Information Security Officer), Definition, *Techtarget*, http://searchsecurity.techtarget.com/definition/CISO-chief-information-security-officer

COBIT 5 for Risk, ISACA, 2013, http://www.isaca.org/COBIT/Documents/COBIT-5-for-Risk-Preview_res_eng_0913.pdf

Cobo del Rosal, M. y Vives Antón, T. S., *Derecho Penal. Parte General*, Valencia, Tirant lo Blach, 5.ª edición, 1999.

Collin, B., «The Future of Cyberterrorism, Crime and Justice International» (marzo de 1997), pp. 15-18.

COM (2010) 521 final 2010/0275 (COD), Concerning the European Network and Information Security Agency (ENISA) (30 de septiembre de 2010), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0521:FIN:EN:PDF

«Communication and Information Systems Services Agency», NATO, http://www.ncsa.nato.int/topics/combating_cyber_terrorism.htm

Computer Science and Telecommunications Board, National Research Council, 1991. Computers at Risk: Safe Computing in the Information Age. National Academy Press, Washington, D. C.

«Computer-related crime: analysis of legal policy», en ICCP - Information, Computer and Communications Policy, Ed. OECD Publications and Information Centre, n° 10, Washington (31 de agosto de 1986).

Convention pour la prévention et de la répression du terrorisme/Convention for the Prevention and Punishment of Terrorism (16 de noviembre de 1937), https://www.wdl.org/es/item/11579/view/1/1/

Coraggio, Giulio, «Cyber risk insurance - a solution to cybercrime?», http://www.gamingtechlaw.com/2015/10/cyber-risk-insurance-cybercrime.html

Coraggio, Giulio, «The Internet of Things cannot be 100% secure?», *IoTLAW Law of the Internet of Things*, https://iotlaw.net/2015/11/02/the-internet-of-things-cannot-be-100-secure/

CORAGGIO, Giulio, «What is an adequate standard of security?», *IoTLAW Law of the Internet of Things*, https://iotlaw.net/2015/11/02/the-internet-of-things-cannot-be-100-secure/

CORTE IBÁÑEZ, Luis de la y BLANCO NAVARRO, José María, *Seguridad nacional, amenazas y respuestas*, LID Editorial Empresarial (noviembre de 2014).

Cost of UK data breaches 2010, Ponemon Institute (julio de 2010).

Counter-Terrorism Committee, UN Security Council, http://www.un.org/sc /ctc/index.html

CRABB, Gregory, CURTIS, Pamela D., FITZPATRICK, Brendan, MEHRAVARI, Nader y TOBAR, David, «Structuring the Chief Information Security Officer Organization», Carnegie Mellon University (septiembre de 2015), https://resources.sei.cmu.edu/asset _files/TechnicalNote/2015_004_001_446198.pdf

CREMADES GARCÍA, Javier, *El fraude de los servicios financieros* online, Estudios Jurídicos del Ministerio Fiscal II, Madrid, 2003.

CTO. «A CTO perspective», *Research Technology Management*, 35, en SMITH, Roger D., «The Role of the Chief Technology Officer in Strategic Innovation, Project Execution, and Mentoring», Princeton, 2002, p. 5, https://www.cs.princeton.edu /courses/archive/spring12/cos448/web/readings/smith.pdf

Cuadro Comparativo, Ley Orgánica 1/2015, de 30 marzo por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, ICAM, p. 195, http://web.icam.es/bucket/CUADRO%20COMPARATIVO%20DEL%20C%C3%93DIGO%20PENAL_%20LO%201-2015_%20CP.pdf

Cyber Explotation - Law Enforcement FAQs, State of California Department of Justice, Office of the Attorney General, p. 1, https://oag.ca.gov/sites/all/files/agweb/pdfs/ce/cyber-exploitation-law-enforcement-faqs.pdf

«Cyber insurance market set to reach $7.5 billion by 2020», PWC (16 de septiembre de 2015), p. 10, http://press.pwc.com/News-releases/cyber-insurance-market-set-to-reach--7.5-billion-by-2020/s/5CC3FA21-221C-43DF-A133-05435E365342

Cyber Risk - a Global Systemic Threat, a White Paper to the Industry on Systemic Risk, DTCC (octubre de 2014), Prólogo, https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjG7Ibqw-bPAhXCQBQKHUveB5UQFggcM AA&url=http%3A%2F%2Fwww.dtcc.com%2F~%2Fmedia%2FFiles%2FDownloads%2Fissues%-2Frisk%2Fcyber-risk.pdf&usg=AFQjCNHaLH eWuZLVBLjiw_2JwBAUCh4x-PA&sig2=QE0u1kerPcAwi_6NYsv-_w&bvm=bv. 136499718,d.d24

Cyber Risk, a global systemic threat, Depositary Trust & Clearing Corporation (octubre de 2014), http://www.dtcc.com/~/media/Files/Downloads/issues/risk/cyber-risk.pdf

Cyber Risk Pool, Europe Economics, Londres (21 de febrero de 2017), http://www.europe-economics.com/publications/cyber_risk_pool.pdf

Cyber Risk, The Institute of Risk Management, CGI, IRM (2014), https://www.theirm.org/media/883443/Final_IRM_Cyber-Risk_Exec-Summ_A5_low-res.pdf

«Cyber risks and government pools. Too soon?», *Artemis* (30 de marzo de 2017), http://www.artemis.bm/blog/2017/03/30/cyber-risks-and-government-pools-too-soon/

«Cyber Security and Risk Management», NCSC, 2013, p. 2, http://www.ncsc.govt.nz/assets/cyber-security-risk-management-Executive.pdf

«Cyber Security in Securities Markets», IOSCO (abril de 2016), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf

Cyber Security Market by Solutions, *marketsandmarkets.com* (julio de 2016), http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html

Cyber Warefare, Institute for Security Technology Studies at Dartmouth College (noviembre de 2004), http://www.ists.dartmouth.edu/docs/execsum.pdf

«Cybercrime», *J. Computer Virology,* nº 1 (2006), p. 14.

Cybercrime, UNODC, https://www.unodc.org/documents/data-and-analysis tocta/10. Cybercrime.pdf

Cybercrime trends report, RSA, 2011.

«Cyber-Insurance Metrics and Impact on Cyber Security, The White House, Washington, D. C., GPO, s. f., www.whitehouse.gov/files/documents/cyber/ISA%20-%20CyberInsurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf, en «La transferencia del ciberriesgo en España», *Thiber* (2016).

«Cyberpower and National Security: Policy Recomendations for a Strategic Framework», en Kramer, F. D., Starr, S. y Wentz, L. K. (ed.), *Cyberpower and National Security*, National Defense University Press, Washington, D. C., 2009.

«A cybersecurity call to action», Marsh & McLennan y Cherthoff Group, Nueva York, 2014, https://chertoffgroup.com/files/docs/2e8e875a-78e9-4b5f-b537-7722b1826137.pdf

«Cybersecurity and Corporate Liability: The Board's View», *Veracode* (2015), p. 2, https://www.nyse.com/publicdocs/Veracode_Survey_Report_Cybersecurity_Corporate_Liability.pdf

«Cybersecurity industry, Digital Single Market Digital Economy & Society», European Commission (2016), https://ec.europa.eu/digital-single-market/en/cybersecurity-industry

«Cybersecurity Insurance», The department of Homeland Security (30 de junio de 2016), https://www.dhs.gov/cybersecurity-insurance#

«Cybersecurity National Action Plan», The White House Office of the Press Secretary, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national action-plan

Cybersecurity Strategy of European Union, An Open, Safe and Secure Cyberspace, JOIN (2013) 1 final, Join Communication to the European Parliament, the council, The European Economic and Social Committee and the Commettee of the Regions, Referencia legal: Pub. L. n° 98-473.

«Cyberspace», *Oxford Living Dictionaries*, Oxford University, http://www.oxforddictionaries.com/us/definition/american_english/cyberspace

Daintith, John (ed.) (2009), «IT», *A Dictionary of Physics*, Oxford University Press.

Danchev, Dancho, «How many people fall victim to phishing attacks?» (4 de diciembre de 2009), http://www.zdnet.com/blog/security/how-many-people-fall-victim-tophishing-

«Dañar», *Diccionario de la Lengua Española*, RAE, http://dle.rae.es/?id=BrdY6Ro

«DDoS attacks against Global Markets» (febrero de 2014): http://www.Prolexic.com/kcresources/whitepaper/global-market/DDoS_attacksagainst_Global_Markets_whitepaper_US_020314.pdf

De Esteban Alonso, J. y González-Trevijano Sánchez, P., *Tratado de Derecho Constitucional II*, Ed. Universidad Complutense de Madrid, Madrid, 2.ª edición, 2004.

De La Mata Barranco, N. J., *Derecho Penal Informático*, Ed. Thomson Reuters, Navarra, 1.ª edición, 2010 pp. 161-162, 164.

De La Mata Barranco, Norberto Javier y Hernández Díaz, Leyre, «El delito de daños informáticos. Una tipificación defectuosa», *Estudios Penales y Criminológicos*, nº 29 (2009), p. 165.

De Verda y Beamonte, J. R. *Veinticinco años de aplicación de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen*, ed. Thomson-Aranzadi, Cizur Menor (Navarra), 2007, p. 288.

«Defending against cyber attacks: what does this mean in practice?», NATO (31 de marzo de 2008), http:// www.nato.int/issues/cyber_defence/practice.html

Definition «antimalware», TechTarget, *SearchSecurity*, http://searchsecurity.techtarget .com/definition/antimalware

Definition «data loss prevention (DLP)», *Whatls*, http://whatis.techtarget.com/definition/data loss-prevention-DLP

Definition «disaster recovery», TechTarget, *SearchSecurity*, http://searchdisasterrecovery .techtarget.com/definition/disaster-recovery

Definition «encryption», TechTarget, *SearchSecurity*, http://searchsecurity.techtarget.com/definition/encryption

Definition «firewall», TechTarget, *SearchSecurity*, http://searchsecurity.techtarget.com/definition/firewall

Definition «identity access management (IAM) system», TechTarget, *Search Security*, http://searchsecurity.techtarget.com/definition/identity-access-management-IAM-system

Definition «vulnerability management planning», *whatls.com*, http://whatis.techtarget .com/definition/vulnerability-management

Definition «Web filter», TechTarget, *SearchSecurity*, http://searchsecurity.techtarget.com/definition/Web-filter

Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination, Digital Agenda for Europe, European Commission DG Communications Networks, Content & Technology, p. 9, http://ec.europa.eu/newsroom/dae /document.cfm?doc_id=9472

DENNING, D., «Cyberterrorism», Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives (23 de mayo de 2000), http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

DENNING, Dorothy E., «Activism, Hacktivism, and Cyberterrorism», 2000, p. 241, https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf

DENNING, Dorothy E., «Cyberterrorisim», Georgetown University (23 de mayo de 2000), p. 4, http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf

«Denuncia a una empresa de juegos *online* por 'robarle sus armas biológicas», *EFE*, Navegante.com, http://www.elmundo.es/navegante/2003/11/20/juegos/1069320761.html

DEVOST, M. G., HOUGHTON, B. K. y POLLARD, N. A. «Information terrorism: Political violence in the information age», 1998, http://www.terrorism.com/Denning.html

DÍEZ BALLESTEROS, Juan Alberto, «Riesgos cibernéticos: daños propios, responsabilidad civil, pérdida de beneficio», XVIII Congreso de RC y Seguro, INESE (27 y 28 de junio de 2016).

DÍEZ-PICAZO, L. M. *Sistema de derechos fundamentales*, Thomson-Civitas, Cizur Menor (Navarra), 3.ª edición, 2008, p. 310.

DÍEZ-PICAZO, L. y GULLÓN, A., *Sistema de derecho civil*, vol. II, Tecnos, 1989, p. 591.

Digital Ecosystem Community: Envisioning the future of the Digital Ecosystem, World Economic Forum (2007), http://www3.weforum.org/docs/WEF_Digital Ecosystem _Scenario2015_ExecutiveSummary_2010.pdf

Digital Ecosystem Convergence between IT, Telecoms, Media and Entertainment: Scenarios to 2015, WEForum (3 de noviembre de 2007), http://www3.weforum.org/docs/WEF_DigitalEcosystem_Scenario2015_ExecutiveSummary_2010.pdf

Digital Ecosystems, DG-Cnect of the European Commission, http://www.digital-ecosystems.org/

DINI, P., RATHBONE, N., VIDAL, M., HERNÁNDEZ, P., FERRONATO, P., BRISCOE, G. y HENDRYX, S. «The digital ecosystems research vision: 2010 and beyond», European

Commission (julio de 2005), http://www.digital-ecosystems.org/events/2005.05/de_position_paper_vf.pdf

«Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad», OCDE (2004), http://www.oecd.org/internet/ieconomy/34912912.pdf, p. 7

2015 Cost of Cyber Crime Study: United Kingdom, Ponemon Institute (octubre de 2015), pp. 4 y 5.

«Do you need an IDS or IPS, or both?», TechTarget, *SearchSecurity*, http://searchsecurity.techtarget.com/Do-you-need-an-IDS-or-IPS-or-both

Douligeris, C y Mitrokotsa, A., «DDoS Attacks and Defense Mechanisms: Classification and State-of-theart», *Comp. Networks, vol.* 44 (2004), pp. 643-666.

Eide, E. B. y Kaspersen, A., «Cyberspace: The new frontier in warfare» (24 de septiembre de 2015), https://agenda.weforum.org/2015/09/cyber space-the-new-frontier-inwarfare/

«Emerging Risks in the 21st Century», An Agenda For Action, OECD (2003), p. 12, https://www.oecd.org/futures/globalprospects/37944611.pdf

Emissions Trading, Q & A following the suspension of transactions in national ETS registries for at least one week from 19:00 CET on Wednesday 19 January 2011, Comisión Europea (21 de enero de 2011), http://europa.eu/rapid/press-release_MEMO-11-34_en.htm

«Enemies of the Internet 2014: Entities at the heart of censorship and surveillance», *Reporters Without Borders* (París) (11 de marzo de 2014).

«Estas son las razones por las que el coche autónomo 'siempre' va a tener la culpa en caso de accidente», *El blog de Mapfre* (14 de diciembre de 2016), http://blogmapfre.com/motor/estas-son-las-razones-por-las-que-el-coche-autonomo-siempre-va-tener-la-culpa-en-caso-de-accidente/#sthash.ISWBLwSz.dpuf

«Estimated Potential Economic Impact of Technologies, US$ trillion, annual», Global Risks Report, World Economic Forum (2016), p. 18.

«Estrategia de Ciberseguridad Nacional», Seguridad Nacional (diciembre de 2013), pp. 16-28, http://www.dsn.gob.es/es/file/146/download?token=Kl839vHG

«EU ministerial conference in Estonia initialized 'Tallinn process' to secure critical information infrastructure», Republic of Estonia Ministerio of Economic

Affairs and Comunications (29 de abril de 2009), https://www.mkm.ee/en/news/eu-ministerial-conference-estonia-initialized-tallinn-process-securecritical-information

European Commission, A New Framework for Electronic Communications Services COM, 539 final (10 de noviembre de 1999), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l24216.

Evans, Dave, «The Internet of Things How the Next Evolution of the Internet Is Changing Everything», CISCO, https://www.cisco.com/c/dam/en_us/about/ac79/ docs/innov/ IoT _IBSG_0411FINAL.pdf

Evans, Steve, «Pool Re cyber risk coverage to incentivise cyber-resilience», Reinsurancene (17 de marzo de 2017), https://www.reinsurancene.ws/pool-re-cyber-risk-coverage-incentivise-cyber-resilience/

Eynde Adroer, Andreu Van den, «Análisis jurídico del sabotaje informático», ENATIC, Consejo General de la Abogacía Española, http://www.abogacia.es/2015/03/09/analisis-juridico-del-sabotaje-informatico/

«El FBI investiga una estafa millonaria a través de los videojuegos 'FIFA' », *El Mundo*, (16 de noviembre de 2016), http://www.elmundo.es/tecnologia/2016/11/16/582c289046163f820d8b460b.html

«Federal Information Security Market 2015-2020», *Deltek*, http://more.deltek.com/Federal-Information-Security-Market-2015-2020

Feeny, David F., Edwards, Brian y Simpson, Kep, «Understanding the CEO/CIO Relationship», Oxford Institute of Information Management Templeton College, 1992, http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1058&context=icis1992

Fernández Avilés, José Antonio, «La responsabilidad civil en el ámbito de la jurisdicción social: puntos críticos», pp. 27 y 28, http://www.asociacionabogadosrcs.org/ponencias/pon2-4.pdf

Fernández Santiago, A. y Castro Fuertes, M., «Comentario al artículo 197 CP», en Amadeo Gadea, S., *Código Penal. Doctrina Jurisprudencial. Parte especial*, Ed. Factum Libri Ediciones, Madrid, 2009, http://0-vlex.com.cisne.sim.ucm.es/vid/comentario-articulo-codigo-penal-69108467

Fernández, J. Raúl, «La responsabilidad en vehículos autónomos», *Derecho y Nuevas Tecnologías* (5 de julio de 2016), http://www.jraulfernandez.es/la-responsabilidad-vehiculos-autonomos/

Fernández, J. Raúl, *El Blog de J. Raúl Fernández*, http://www.jraulfernandez.es/la-responsabilidad-vehiculos-autonomos/

Filkins, Barbara, «IT Security Spending Trends», SANS Institute (febrero de 2016), p. 1, https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697

«Fitch: UK Cyber Security Report Flags Insurers' Important Role», *Reuters* (23 de marzo de 2015), http://www.reuters.com/article/idUSFit91767020150323

Fitzgerald, Todd, *Clarifying the Roles of Information Security*, Taylor & Francis Group, 2007, pp. 259-261.

Floresca, Lauri, «Cyber Insurance 101: The Basics of Cyber Coverage», www.wsandco.com/about-us/news-and-events/cyber-blog/cyber-basics

Frey, Carl Benedikt y Osborne, Michael A., «The Future of Employment: How Susceptible are Jobs to Computerisation?» Oxford Martin School, University of Oxford (13 de septiembre de 2013), http://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf

Gaber, Maximilian K. P., *The effect of D&O Insurance on managerial risk taking*, Intersentia Publish Ltd, Cambridge, 2015, pp. 11-13.

Gandel, Stephen, «Lloyd's CEO: Cyber attacks cost companies $400 billion every year», *Fortune* (23 de enero de 2015), http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/

García, J. e Illescas Ortiz, R. (coords.), *Régimen jurídico de internet*, Ed. La Ley, Madrid, 1.ª edición, 2001.

Garrie, Daniel, «Do CIOs and CISOs Get Covered in Cybersecurity Litigation?», *Bloomberg* (26 de agosto de 2015), https://bol.bna.com/do-cios-and-cisos-get-covered-in-cybersecurity-litigation/

Garrigues, J. y Uría, R., «Comentario de la Ley de Sociedades Anónimas, t. II, 3.ª ed., revisada y puesta al día por Menéndez y Olivencia», Civitas, 1976, en Parra Lucán, M.ª Ángeles, «Lección 17ª. La responsabilidad civil de los administradores», en *Lecciones de responsavilidad civil*, Aranzadi, 2013, pp. 505-515.

«Global Risk», *Cambridge Dictionary*, http://dictionary.cambridge.org/es/diccionario/ingles/global-risk

Global Risk Landscape 2013 *versus* 2012, Global Risks Report, World Economic Forum (2013).

Global Risks Report 2006, World Economic Forum (2006).

Global Risks Report 2007, World Economic Forum (2007).

Global Risks Report 2008, World Economic Forum (2008).

Global Risks Report 2009, World Economic Forum (2009).

Global Risks Report 2010, World Economic Forum (2010).

Global Risks Report 2011, World Economic Forum (2011).

Global Risks Report 2012, World Economic Forum (2012).

Global Risks Report 2013, World Economic Forum (2013).

Global Risks Report 2014, World Economic Forum (2014).

Global Risks Report 2015, World Economic Forum (2015).

Global Risks Report 2016, World Economic Forum (2016).

Gómez Garrido, J., «Derecho al honor y persona jurídica-privada», *REDUR 8* (diciembre de 2010), p. 207, http://www.unirioja.es/dptos/dd/redur/numero8/gomez.pdf

Gómez Garrido, J., «Derecho al honor y persona jurídica-privada», *REDUR 8*, (diciembre de 2010), p. 218, http://www.unirioja.es/dptos/dd/redur/numero8/gomez.pdf

González Cussac, J. L. y Fernández Hernández, A., «Sobre el concepto jurídico penal», *Teoría y Derecho: Revista de Pensamiento Jurídico*, nº 3 (2008), p. 35.

González Hurtado, Jorge Alexandre, *Delincuencia informática: daños informáticos del artículo 264 del Código Penal y Propuesta de Reforma*, Tesis Doctoral, UCM, 2013, http://eprints.ucm.es/23826/1/T34976.pdf

González Hurtado, Jorge Alexandre, *Daños informáticos del artículo 264 del Código Penal y propuesta de reforma*, Universidad Complutense de Madrid, Madrid, 2013.

González Rus, J. J., «El *cracking* y otros supuestos de sabotaje informático», *Estudios Jurídicos. Ministerio Fiscal*, nº 2 (2003).

González Rus, J. J., «Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos», en Díez Ripollés, J. L., Romeo Casabona, C. M., Gracia Martín, L. e

González Rus, Juan José, «Daños a través de internet y denegación de servicios», en Jorge Barreiro, A. (coord.), *Homenaje al profesor Dr. Gonzalo Rodríguez Mourullo*, Ed. Thomson Civitas, Navarra, 1.ª edición, 2005, p. 1472 y ss.

Goodin, Dan, «NSA-leaking Shadow Brokers just dumped IT most damaging release yet», Arstechnica (14 de abril de 2017), https://arstechnica.com/security/2017/04/nsa-leaking-shadow-brokers-just-dumped-IT-most-damaging-release-yet/

Gordon, Sarah y Ford, Richard, «Cyberterrorism?», *Symantec Security Response* (2003), p. 8, https://www.symantec.com/avcenter/reference/cyber terrorism.pdf

«Growing a Digital Social Innovation Ecosystem for Europe DSI Final Report», DG-Cnect of the European Commission (2015), pp. 22-34, http://ec.europa.eu/newsroom/ dae/document.cfm?doc_id=8907

Gudín Rodríguez-Magariños, Faustino, «Nuevos delitos informáticos: *phising*, *pharming*, *hacking* y *cracking*», http://web.icam.es/bucket/Faustino%20Gud%C3%ADn%20-%20Nuevos%20delitos%20inform%C3%A1ticos.pdf

«Guía sobre cobertura de los ciberriesgos», Willis Towers Watson (18 de marzo de 2016).

Guía terminológica de ciberseguridad, AGERS, Madrid (2017), p. 14.

«Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities Under the Cybersecurity Information Sharing Act of 2015», The Department of Homeland Security The Department of Justice (15 de junio de 2016), https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity _Sharing_Guidance_(Sec%20105(a)).pdf

«Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security», OCDE, 2002, http://www.oecd.org/internet/internet economy/34912912.pdf

«Hacker targets Tel Aviv bourse and El Al» (16 de enero de 2012); «Hackers attack Arab stock markets», *Financial Times* (17 de enero de 2012).

HAHN, Saul, «Networking In Latin America and the Caribbean and the Caribbean», OAS/RedHUCyT Project, ISOC (1995).

HALL, Shanique, «Recent Regulatory Initiatives to Tackle the Growing Threat of Cyber Risk», CIPR, NAIC (diciembre de 2015), http://www.naic.org/cipr_newsletter_ar chive/vol17_cyber_threat.pdf

HANSMAN, S. y HUNT, R., «A taxonomy of network and computer attacks». *Computer and Security* (2005).

HEALEY, J. 2011. «The Five Futures of Cyber Conflict and Cooperation». *Atlantic Council Issue Brief* (2001), http://www.atlanticcouncil.org/publications/issue-briefs/the-five-futures-of-cyber-conflict-and-cooperation.

HEFENDEHL, R.; HIRRSCH, A. V.; WOHLERS, W. (coord.) *Die Rechtsgutstheorie legitimationsbasis des Strafrechts oder dogmatisches Glasperlenspiel?*, Baden-Baden, 2003.

HEINTZE, Hans-Joachim y THIELBÖRGER, Pierre, «From Cold War to Cyber War», Springer (2016), https://books.google.es/books?id=l8JOCgAAQBAJ&pg=PA39&lpg=PA39&dq=cyber+cold+war&source=bl&ots=_TIzSdlDG D&sig=mjGNzXUt6aLg Zj8hrxKRHOe Kwfw&hl=es&sa=X&ved=0ahUKEwiwj- _2svvTAhXD2xoKH d4OBy c4ChD oAQgiMAA#v=o nepage&q=cyber%20cold%20war&f=false

HEREDERO HIGUERAS, M., *La Ley Orgánica 5/1992, de Regulación de Tratamiento Automatizado de Datos Personales*, Ed. Tecnos, Madrid, 1996, p. 140.

HERNÁNDEZ FERNÁNDEZ, Abelardo. «El honor, la intimidad y la imagen como derechos fundamentales», *Codex* (24 de febrero de 2009).

HERRERO DE CASTRO, Rubén, *Evolución del concepto de interés nacional*, Centro Superior de Estudios de Defensa Nacional, Monografías del CESEDEN (abril de 2010), p. 19, http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/115_EVOLUCION_DEL_CONCEPTO_DE_INTERES_NACIONAL.pdf

HERSH, Seymour M., «The Online Threat: Should We Be Worried About a Cyber War?», *The New Yorker* (1 de noviembre de 2010), http://www.newyorker.com/reporting /2010/11/ 01/101101fa_fact_hersh?

HIGUERA GUIMERÁ, J. F. (coords.), *La ciencia del Derecho Penal ante el nuevo siglo. Libro homenaje al profesor doctor don José Cerezo Mir*, Ed. Tecnos, Madrid, 1.ª edición, 2002, p. 248.

Hildreth, Steven A. «Cyberwarfare», *Congressional Research Service*, 16 (19 de junio de 2001).

Historia, Agencia Española de Protección de Datos, AGPD, https://www.agpd.es/p ortalwebAGPD/LaAgencia/informacion_institucional/conoce/historia-ides-idphp.php

History and way ahead, CCD-CoE, http://www.ccdcoe.org/12.html

«A History of Excellence and Innovationç», *Merit*, https://www.merit.edu/about-us/merIT-history/

Holzmann, V. y Dubnov, S. «Understanding the Collaboration Enigm», *The International Journal of Knowledge, Culture & Change Management* (julio de 2011), https://www.researchgate.net/publication/235872389_Understanding_the_Collaboration_Enigma

«How to prepare for the emerging threats to your systems and data, essential guide», *Techtarget*, http://searchsecurity.techtarget.com/essentialguide/How-to-prepare-for-the-emerging-threats-to-your-systems-and-data

Howard, John D. y Longstaff, Thomas A. «A Common Language for Computer Security Incidents», *Technical report*, Sandia National Laboratories, 1998.

Huete Nogueras, Javier, «La reforma de los delitos informáticos», *Diario La Ley*, nº 7.534 (2010).

Hussain, Farooq, «Historic Role of the Commercial Internet eXchange Rounter and IT Impact on the Development of Internet eXchange Points (IXs)» (octubre de 2003).

«ICT Facts & figure the world in 2015» (mayo de 2015), https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf

«Industrial Control Systems Cyber Emergency Response Team», US Department of Homeland Security, https://www.dhs.gov/sites/defaultt/files/publications/DHS% 20Federal%20Government_4.7.edIT__0.pdf

Information Security Breaches Survey 2004 Technical Report, Department of Trade and Industry, 2004.

Informe general del 10.º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Viena, Austria (10 a 17 de abril de 2000).

Los informes del proyecto Information Warfare Monitor: «Tracking GhostNet: investigating a Cyber Espionage Network» (2009) y «Shadows in the Cloud: Investigating Cyber Espionage 2.0» (2010).

«Insurance Cyber Risk», Tine Olsen, Willis (18 de julio de 2013), http://www.pwc.dk/ da/arrangementer/assets/cyber-tineolsen.pdf

«¿Internet con fronteras electrónicas y límites geográficos?», *BBC Mundo*, 14 enero 2014, http://www.bbc.com/mundo/noticias/2014/01/140110_tecnologia_limites_internet_censura_kv

Internet Security Threat Report 2014, vol. 19, http://www.sec.gov/ocie/announcement /Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf

«IoT: La revolución silencioso» (11 de julio de 2016), https://www.t-systems.com/es/es/newsroom/pers pectives/internet-of-things/iot/iot-the-quiet-revolution-344724

ISO/IEC 27005:2011, Terms and definitions, ISO, Online Browsing Platform (OBP), https://www.iso.org/obp/ui/#iso:std:56742

ISO/IEC 27032:2012 Information Tecnology Security Techniques, Guidelines for Cybersecurity, ISO, http://www.iso.org/is o/iso_catalogue/catalogueetc/catalogue_ detail. htm?csnumber=44375

ITU Global Cybersecurity Agenda, GCA, Framework for International Cooperation in Cybersecurity (2007), http://www.ifap.ru/library/book169.pdf

Jackson, Rupert M. *Professional Negligence*, London Sweet & Maxwell (1987), pp. 4-15.

Jess, Digby C., *A Guide to the Insurance of Profesional Negligence Risks*, Butterworths London, 1982, p. 1.

Jimeno, Jesús, «¿Quién es responsable de WannaCrypt?», *Boletín Rc y Seguros*, INESE (1 de junio de 2017), http://boletinrc.inese.es/apendice-n36.html

«Jobs Supported by Exports: An Update», *International Trade Administration* (12 de marzo).

Jones, Sam, «UK prime cyber attack target of Europe and Middle East», *Financial Times* (16 de octubre de 2014).

Kahn, Robert E. «The Role of the Government in the Evolution of the Internet, Revolution in the US Information Infrastructure» (National Academy Press 1994).

Kallenbach, Paul y Lloyd, Anthony, «Perspectives on cyber risk», MinterEllison, (enero de 2016), p. 2, http://www.minterellison.com/files/uploads/Documents/Publications/Reports %20Guides/RG_2016_Cyber-Report[150189].pdf

Kaplan, R.S. y Mikes, A. «Managing Risks: A New Framework», *Harvard Business Review* (2012).

Kaspersen, A. «Can you have both security and privacy in the internet age?», Forum Agenda 21 July 2015, https://agenda.weforum.org/2015/07/can-you-have-bothsecurity- and-privacy-in-the-internet-age/

Kaspersen, A. «What will militaries of the future look like?», Forum Agenda 12 August 2015, https://agenda.weforum.org/2015/08/what-will-militaries-of-the-futurelook - like/

Kaspersen, A. y Hagan, A. «8 emerging technologies transforming international security». Forum Agenda 8 September 2015, https://agenda.weforum.org/2015/09/8-technologies-transforming-international-security/

Kaufman, G. G. y Scott, K. E., «What Is Systemic Risk, and Do Bank Regulators Retard or Contribute to It?», *Independent Review*, 7 (2003), pp. 371-391.

Kelly, D. J. y Mastrocola, P. R., «The Economic Espionage Act of 1996», *New England Journal on Criminal and Civil Confinement*, nº 26 (2000).

Kennedy, John, «Attack of the machines: Internet's biggest meltdown caused by Mirai Botnet» (23 de octubre de 2016), https://www.siliconrepublic.com/machines/internet-meltdown-mirai-botnet

Kesan, J, Majuca, Rupterto y Yurcik, William, «The Economic Case for Cyber-insurance», *University of Illinois College of Law Working Papers*, nº 2 (2004).

Kesan, Jay P. y Shah, Rajiv C., «Fool Us Once Shame on You - Fool Us Twice Shame on Us: What We Can Learn from the Privatizations of the Internet Backbone Network and the Domain Name System», *Washington University Law Quarterly*, vol. 79 (2001).

Kjaerland, M., «A taxonomy and comparison of computer security incidents from the commercial and government sectors». *Computers and Security*, 25, pp. 522-538 (octubre de 2005).

Koch Merino, Sebastián, «Libertad en el ciberespacio», Centro de Estudios Estratégicos, Academia General del Ejército de Chile, *Revista de Ensayos Militares*, vol. 1, nº 2 (2015), http://www.ceeag.cl/wpcontent/uploads/2016/05/libertad-en-el-ciberespacio.pdf

Kortuem, Gerd, Kawsar, Fahim, Fitton, Daniel y Sundramoorthy, Vasughi, «Smart Objects as Building Blocks for the Internet of Things», the IEEE Computer Society (febrero de 2010), pp. 46-49, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5342399

Kraakman 2009, p. 78, en Maximilian K. P. Gaber, *The effect of D&O Insurance on managerial risk taking*, Intersentia Publish Ltd, Cambridge, 2015, pp. 22-23.

Krebs, Brian, «IoT Device Maker Vows Product Recall, Legal Action Against Western Accusers» (24 de octubre de 2016), https://krebsonsecurity.com/

Lacruz Berdejo, J. L., «Elementos de Derecho Civil», Tomo III, Derechos Reales. Librería Bosch, Barcelona, 1980, pp. 339-344, en Miró Echevarne, Manuel, «Sessió 5: Els intangibles i la seva importancia jurídica», IAFI-IX Seminari en Finances (24 de febrero de 2006), p. 1, http://www.ub.edu/iafi/Recerca/Seminaris/miro.pdf

Lascuraín Sánchez, Juan Antonio, «Bien Jurídico y objeto protegible», *ADPCP*, vol. LX (2007).

Lata, Mike, «Reality Check: What's the Difference Between a CTO and CIO?», *Technopedia* (23 de noviembre de 2012), https://www.techopedia.com/2/28883/it-business/it-careers/reality-check-whats-the-difference-between-a-cto-and-cio

Lawson, F. H. *Negligence in the civil law*, Oxford, 1950, p. 29.

Leavitt, Harold J.; Whisler, Thomas L., «Management in the 1980s», *Harvard Business Review* (1958), p. 11.

Lejarza Illaro, Eguskiñe, «Ciberguerra, los escenarios de confrontación», *Instituto Español de Estudios Estratégicos*, nº 14 (febrero de 2014), pp. 2-4, http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO18-2014_Ciberguerra_EscenariosConfrontacion_EguskineLejarza.pdf

León Barandiarán, José, «Comentarios al Código Civil Peruano». *Rev. Derecho y Ciencias Políticas*, Año XII, nº 2, en Cuentas Ormachea, Enrique, «El abuso del derecho», p. 469, https://dialnet.unirioja.es/ descarga/articulo/5085322.pdf

Lewis, James, *United States. Center for Strategic and International Studies. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Washington, D. C., 2002.

Lewis, W. W. y Lawrence, H. L., «A new mission for corporate technology». *Sloan Management Review*, 31 (1990), pp. 57-67.

Licklider, J. C. R., «Man-Computer Symbiosis», IRE Transactions on Human Factors in Electronics (marzo de 1960), http://worrydream.com/refs/Licklider %20-%20Man-Computer %20Symbiosis.pdf.

López Cerezo, Luján, *Ciencia y política del riesgo*, Madrid, 2000.

López Gil, Mar, «Estrategia de Ciberseguridad Nacional», astic, *boletic 73* (mayo de 2015), http://www.astic.es/sites/default/files/articulosboletic/monografico2marialopezgil.pdf

Lough, Daniel, *A Taxonomy of Computer Attacks with Applications to Wireless Networks*, PhD thesis, Virginia Polytechnic Institute and State University, 2001.

Luening, E., «Clinton launches plan to protect IT infrastructure», *CNET* (7 de enero de 2000).

Maciá Góme, Ramón, «La dualidad del daño patrimonial y del daño moral», *Revista de Responsabilidad Civil y Seguro*, p. 22, http://asociacionabogadosrcs.org/doctrina/rc36 doctrina2.pdf

«Man arrested for £1m online tax fraud», *The Register* (4 de septiembre de 2009), http://www.theregister.co.uk/2009/09/04/pceu_hmrc/

«Manual de las Naciones Unidas sobre prevención y control de delitos informáticos», *Revista Internacional de Política Criminal*, Naciones Unidas, nº 43 y 44 (1994).

Martínez Sanz, Fernando, «Los administradores responsables», en Campuzano, Ana Belén (coord.), *La responsabilidad de los administradores en las sociedades mercantiles*, Tirant lo blach Tratados, Valencia, 4.ª edición, 2011, p. 60.

Mata y Martín, Ricardo Manuel, «Criminalidad informática: una introducción al cibercrimen», *Actualidad Penal* (2003).

Medina Crespo, Mariano, «La fuerza mayor como circunstancia exoneradora de la responsabilidad civil automovilística», http://www.asociacionabogadosrcs.org/congreso /6congreso/ponencias/Mariano%20Medina%20Crespo%20parte2.pdf

MENÉNDEZ, Aurelio y ROJO, Ángel, *Lecciones de Derecho Mercantil*, 2014.

«Microsoft Security Intelligence Report», Microsoft (2016) http://download.microsoft. com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft_ Security _Intelligence_ Report_Volume_21_English.pdf

«Mission and Vision», CCD-CoE, http://www.ccdcoe.org/11.html

MILL, John Stuart, *On Liberty*, Bantam Classics, New York, 2008, pp. 13-14.

MILLÁN-PUELLES, A. *III. Obras completas: La función social de los saberes liberales (1961), Persona humana y justicia social (1962), La formación de la persona humana (1963), Asociación de Filosofía y Ciencia Contemporánea*, Rialp, Madrid, 2013, p. 145.

MILLIGAN, Jhon, «The Expiry of the EU Insurance Block Exemption Regulation» (15 de febrero de 2017), https://www.clydeco.com/insight/article/the-expiry-of-the-eu-insurance -block-exemption-regulation

MIRÓ LLINARES, Fernando, «Delitos informáticos: Hacking. Daños», p. 161.

MIRÓ LLINARES, Fernando, «Delitos contra bienes inmateriales, corrupción y receptación: análisis y consideraciones críticas ante la nueva reforma penal», 2015, p. 161.

MOLINA MATEOS, José María, «Ciberdilema», *Instituto Español de Estudios Estratégicos*, nº 115 (noviembre de 2013), p. 1, http://www.ieee.es/Galerias /fichero/docs_opinion/2013 /DIEEEO115-2013_Cyberdilemma_JM.MolinaMateos.pdf

«Money laundering in cyberspace», *BBC* (2 de febrero de 2001), http://news.bbc.co.uk/2/hi/business/1149984.stm

MORGAN, Steve, «Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020» (diciembre de 2015), http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#526a3f592191

MORGAN, Steven C., «The Cybersecurity Market Report, Q3 2016», *Cybersecurity ventures*, 2016, http://cybersecurityventures.com/cybersecurity-market-report/

MORNINGSTAR, Chip y FARMER, F. Randall. *The Lessons of Lucasfilm's Habitat. The New Media Reader*. Ed. Wardrip-Fruin and Nick Montfort, The MIT Press, 2003.

Motero Aaroca, J., Iglesias Cabero, M., Martín Correa, J. M., Sampedro Corral, M., *Comentarios a la Ley de Procedimiento Laboral, t.* I, Civitas, Madrid, 1993, p. 38; cfr. también Montoya Melgar, A., Galiana Moreno, J. M., Sempere Navarro, A. V. y Ríos Salmerón, B.: *Curso de Procedimiento Laboral,* Tecnos, Madrid, 5.ª ed., 1998, pp. 36-37.

Nachira, Francesco, «Towards a network of digital business ecosystems fostering the local development», European Comission DG INSFO, Bruselas, septiembre de 2002.

Nagamine, K. «Worldwide Smartphone Market Expected to Grow 55% in 2011 and Approach Shipments of One Billion in 2015». *International Data Corporation* (2011), http://www.idc.com/getdoc.jsp?containerId=prUS22871611

«Net Losses: Estimating the Global Cost of Cybercrime», McAfee (junio de 2014), p. 16, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

«Networking for tomorrow», National Science Fundation, https://www.nsf.gov/news /special_reports/cyber/futurenetworks.jsp

«New Estimate of Cost of Identity Fraud to the UK Economy», Identity Fraud Steering Group (IFSC), 2008.

«NIST Cybersecurity Framework, Cyber Security in Securities Markets - An International Perspective», IOSCO, p. 25, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf

Noam, Eli, «Interconnecting the Network of Networks», *MIT Press* (2001).

Noman, Helmi y York, Jillian C., «West Censoring East: The Use of Western Technologies by Middle East Censors, 2010-2011», *OpenNet Initiative* (marzo de 2011).

Nye, J.S. Jr., «The Paradox of American Power. Why the World's Only Superpower can't go it Alone». Cap. 5: Redefining the Nacional Interest, 2002.

O'Connell, Kelly, «Online Casinos Will Experience Cyber-Extortion During SuperBowl Betting», *Internet Business Law* (28 de enero de 2008), http://www.ibls.com /internet _law_news_portal_view.aspx?id=1967&s=latestnews

O'Halloran, Derek, «Tech utopia or cybergeddon?» (22 de enero de 2013), https://www.weforum.org/agenda/2013/01/tech-utopia-or-cybergeddon/

O'Neill, P.H. y Bridenbaugh, P. R. «Credibility» (noviembre-diciembre de 1992).

OHLIN, Jens David, FINKELSTEIN, Claire Oakes y GOVERN, Kevin, *Cyber War: Law and Ethics for Virtual Conflicts*, Oxford, 2015.

«Open Philosophies for Associative Autopoietic Digital Ecosystems (OPAALS)», Information Society Technologies, http://www.lse.ac.uk/media@lse/research/OPAALS/D9.4.pdf

Open Source Definition, Open Source Iniciative, https://opensource.org/osd

«Organised Crime in Europe: The Threat of Cybercrime», Council of Europe (marzo de 2005).

«Organised gangs deceive web users into downloading malicious anti-virus software», *Get Safe Online* (15 de noviembre de 2010), https://www.helpnetsecurity.com/2010/11/16/web-users-deceived-into-downloading-malicious-anti-virus-software/

ORIOL LLEBOT, José, «Los deberes y la responsabilidad de los administradores», en CAMPUZANO, Ana Belén (coord.), *La responsabilidad de los administradores en las sociedades mercantiles*, Tirant lo blach Tratados, Valencia, 4.ª edición, 2011, p. 30.

ORTÍ VALLEJO, A., *Derecho a la intimidad e informática (Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada)*, Ed. Comares, Granada, 1994, p. 170.

PANTALEÓN, A. F., *Causalidad e imputación objetiva: criterios de imputación*, Asociación de Profesores de Derecho Civil, Centenario del Código Civil, t. 2, Madrid, 1990, p. 1561 y ss.

PARRA LUCÁN, M.ª Ángeles, «Lección 17.ª La responsabilidad civil de los administradores», en *Lecciones de responsabilidad civil*, Dykinson, 2013, pp. 505-515.

PERDICES. A., «La muerte juega al gin rummy (La parodia en el derecho de autor y de marcas)», *Revista de Propiedad Intelectual*, 1999.

PERLROTH. H y HARRIS, E. A., «Cyberattack insurance a challenge for Business», *The New York Times* (8 de junio de 2014), https://www.nytimes.com /2014/06/09/business /cyberattack-insurance-a-challenge-for-business.html?_r=0

POLAINO NAVARRETE, M. *El bien jurídico en el Derecho Penal*, Universidad de Sevilla, Sevilla, 1974.

Poncela González, Ángel, *La Escuela de Salamanca*, Verbum, Madrid, 2015, p. 199.

«Prague Summit Declaration Article 4(f)», NATO (21 de noviembre de 2002), http://www.nato.int/docu/pr/2002/p02-127e.htm

Puyol, Javier, «El ejercicio del derecho la indemnización derivado del art. 19 de la LOPD», ECIXGROUP (3 de diciembre de 2014), http://ecixgroup.com/el-grupo/el-ejercicio-del-derecho-la-indemnizacion-derivado-del-art-19-de-la-lopd/

«¿De quién es la culpa del accidente cuando hay un coche autónomo de por medio?» *Tecvolución volvo* (3 de diciembre de 2016), http://tecvolucion.com/quien-es-responsabilidad-legal-accidente-cuando-hay-coche-autonomo-de-por-medio/

Racz, Nicolas, Weippl, Edgar y Seufert, Andreas, «A process model for integrated IT governance, risk, and compliance management, TU Vienna, Institute for Software Technology and Interactive Systems», Favoritenstr. 9-11, 1040, Vienna, Austria, http://www.grcresource.com/resources/racz_al_grc_process_model_balticdbis2010.pdf

Raven, Ellie, «Cyber insurance market set to reach $7.5 billion by 2020», *PwC report*, PWC (14 de septiembre de 2015), p. 1, http://press.pwc.com/News-releases/cyber-insurance-market-set-to-reach--7.5-billion-by-2020/s/5cc3fa21-221c-43df-a133-05435e365342

«Reflexiones en torno al llamado ramo de Contingencias», Mapfre (octubre de 2004), p. 16, http://www.mapfre.com/ccm/content/documentos/mapfrere/fichero/es/trebol-num33-completo.pdf

Reinares, F., ¿Coinciden el Gobierno y los ciudadanos en qué medidas adoptar contra el terrorismo internacional?, *Análisis del Real Instituto El Cano, ARI*, nº 34/2006 (2006).

«Report of the Counter-Terrorism Committee to the Security Council on the implementation of resolution 1624», UN Security Council (15 de septiembre de 2006), pp. 6, 16 y 43, http://daccessdds.un.org/doc/UNDOC/GEN/N06/520/37/PDF/N0 652037.pdf?OpenElement

«Research Findings, Identity Fraud - What About The Victim?», CIFAS (marzo de 2006), https://www.cifas.org.uk/secure/contentPORT/uploads/documents/External-Identity%20Fraud%20%20What%20About%20the%20Victim%20Research%20Findings.pdf

«Responsabilidad civil del fabricante por daños causados por productos defectuosos», Universidad Pompeu Fabra, p. 6, https://www.upf.edu/dretcivil/_pdf/mat _fernando/T82008.pdf

Restivo, Kevin, Llamas, Ramón T. y Shirer, Michael, «Worldwide Smartphone Market Expected to Grow 55% in 2011 and Approach Shipments of One Billion in 2015», *International Data Corporation*, http://www.businesswire.com/news/home/20110609005403 /en/Worldwide-Smartphone-Market-Expected-Grow-55-2011

«Risk and Responsibility in a Hyperconnected World», World Economic Forum (febrero de 2014), http://www3.weforum.org/docs/WEF_IT_Pathways ToGlobalCyber Resilience _Report _2012.pdf

Roca Trías, E., Navarro Michel, M. *Derecho de Daños*, Tirant lo Blanch, Valencia, 6.ª edición, 2011, p. 199.

Rodríguez Guitián, Alma María, *El derecho al honor de las personas jurídicas*, Montecorvo, Madrid, 1996, pp. 103-104.

Romeo Casabona, C. M. (dir.), *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Ed. Comares, Granada, 2006, p. 248 y ss.

Rovira Sueiro, María E. *La responsabilidad civil derivada de los daños ocasionados al derecho al honor, a la intimidad personal y familiar y a la propia imagen*. Cedecs Editorial S.L., Barcelona, 1999, p. 112 y ss.

Rovira Sueiro, María, *la responsabilidad civil derivada de los daños ocasionados al derecho al honor, a la intimidad personal y familiar y a la propia imagen*, CEDECS, Barcelona, 1999.

Salaberry, Agustín, «Robo de bienes virtuales genera condena en vida real», Hipertextual.com (31 de enero de 2012), https://hipertextual.com/2012/01/robo-de-bienes-virtuales-genera-condena-en-vida-real

Sánchez Bravo, A. A., «Una política comunitaria de seguridad en internet», *Diario La Ley*, nº 5.414 (2001), p. 1 y ss.

Sánchez García, I., «El principio constitucional de proporcionalidad del Derecho Penal», *La Ley* (1999).

Sánchez Rojas, Emilio, «¿Ciber… qué? La ciberseguridad», *Ejército*, vol. 837 (2010).

Scarfone, K., Souppaya, M. *et al.*, «Technical Guide to Information Security Testing and Assessment», *NIST (*septiembre de 2008), http://web.nvd.nist.gov/view/vuln/detail ?execution=e7s1

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

Shanghai Cooperation Organisation, NATO Corporative Cyber Defence Centre of Excellence (16 de junio de 2009), https://ccdcoe.org/sco.html

Shavell 2004, p. 232 y Kraakman 2008 en Maximilian K.P. Gaber, *The effect of D&O Insurance on managerial risk taking*, Intersentia Publish Ltd, Cambridge, 2015, p. 11.

Simmons, Chris, Ellis, Charles, Shiva, Sajjan, Dasgupta, Dipankar y Wu, Qishi, Department of Computer Science University of Memphis Memphis, TN, USA, http: //ais.cs. memphis.edu/files/papers/CyberAttackTaxonomy_IEEE_Mag.pdf

Smith, John y Sulmeyer, Michael, «Touring the World of Cybersecurity Law», RSA Conference 2016 (marzo de 2016), https://www.rsaconference.com/writable /presentations/file_upload/law-w04-global_cybersecurity_laws_regulations_and_liability.pdf

Smith, Roger D. «The Role of the Chief Technology Officer in Strategic Innovation, Project Execution, and Mentoring», *Princeton*, 2002, p. 3, https://www.cs.princeton.edu/ courses/archive /spring12 /cos448/ web/readings/smith.pdf

Smith, Roger D., «The Role of the Chief Technology Officer in Strategic Innovation, Project Execution, and Mentoring», Princeton, 2002, p. 17, https://www.cs.princeton. edu/courses/archive/spring12/cos448/web/readings/smith.pdf

Stone, V., «Social interaction and social development in virtual environments», *Teleoperators and Virtual Environments*, vol. 2. (1993), pp. 153-161.

Stoneburner, Gary, Goguen, Alice y Feringa Risk, Alexis, «Management Guide for Information Technology Systems», National Institute of Standards and Technology NIST SP 800-30 (julio de 2002), http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Strickland, Stefanos A. y Theodoulidis, Babis, «Chief Information Officer: A Journey Through Time», Centre for Service Research Manchester Business School University of Manchester, pp. 2-16, http://www.citi.columbia.edu/B8210/read17/CIO.pdf

SYMANTEC, *Report on Rogue Security Software* (2009).

Systemic Risk Barometer, *DTCC* (2014), http://www.dtcc.com/~/media/Files/Downloads/issues /risk/Systemic_Risk_Summary_Report.ashx

«Ten Key Questions on Cyber Risk and Cyber Risk Insurance», *The Geneva Association* (noviembre de 2016), https://www.genevaassociation.org/media/954708/cyber-risk-10-key-questions.pdf

The Economic Impact of Cyber Crime and Cyber Spionage, McAfee, 2014.

«The Cost Of Cyber Crime», DETICA y The Office of Cybersecurity and Information Assurance in the Cabinet Office (enero de 2011), p. 7, https://www.gov.uk /government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

«The Dangers of Germany's Dependence on China», *Spiegel online*, http://www.spiegel.de/international/world/0,1518,713478-6,00.html

«The definitions of company sizes are consistent with those used in the BERR 2008 Information Breach Survey».

«The Evolving Internet: Driving Force, Uncertainties, and Four Scenarios to 2025», CISCO (2010), http://newsroom.cisco.com/dlls/2010/ekIT/Evolving_Internet_GBN_Cisco_2010_Aug_rev2.pdf

«The Global Information Technology Report», ICTs for Inclusive Growth (2015).

«The Global State of Iformation Security Survey,» *PWC* (2016), http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

«The hyperconnected economy: Phase 2 Hyperconnected organisations», The Economist Intelligence (2015), https://www.eiuperspectives.economist.com/sites/default/files/EIU-SAP%20Hyperconnected%20Economy%202%20-%20Briefing%20Paper%20PDF.pdf

«The Internet of Things Backgrounder», *Intel*, 2011, http://newsroom.intel.com/servlet /JiveServlet/download/2297-55895/The%20Internet%20of%20Things%20Backgrounder.pdf

«The Internet of Things: Making sense of the next mega-trend», *The Goldman Sachs Group*, Inc. (3 de septiembre de 2014), http://www.goldmansachs.com/our-thinking /outlook /internet-of-things/iot-report.pdf

«The IT Security Spending Survey», *SANS Institute* (febrero de 2016), https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697

Thurlings, B., y Debackere, K. «Trends in managing industrial innovation – first insights from a field survey. Research Technology Management» (agosto de 1996), en Smith, Roger D., «The Role of the Chief Technology Officer in Strategic Innovation, Project Execution, and Mentoring», Princeton, 2002, p. 6, https://www.cs.princeton. edu/courses/archive/spring12/cos448/web/readings/smith.pdf

Tiao, Paul M. y Hutchins, Eric M. «Congress Surprisingly Passes Several Cybersecurity Bills», *Law360* (18 de diciembre de 2014), https://www.hunton.co m/files/Publication/52ef4325-17ac-4e55-85661a27f3e9ad62/Presentation/PublicationAttachment/bf004202-1e11-4c23-ad4b31484c3cb657/Congress_Surprisingly_Passes_ Several_Cybersecurity_Bills_Dec2014.pdf

Tikk, Eneken, «Ten Rules for Cyber Security», *Survival*, vol. 53, nº 3 (2011).

«Top 5 Risk Identified, Risk to Broader Economy, Systemic Risk Barometer», DTCC (2014), http://www.dtcc.com/~/media/Files/Downloads/issues/risk/Systemic_Risk _Summary _Report.ashx

«La transferencia del ciberriesgo en España», *Thiber* (abril de 2016), p. 34, http://www. thiber.org/ciberseguros.pdf

«Trial lawyers circle Ashley Madison», *The Hill* (29 de agosto de 2015), http://thehill.com/policy/cybersecurity/252203-trial-lawyers-circling-ashley-madison

Tufekci, Zeynep, «The World Is Getting Hacked. Why Don't We Do More to Stop It?», *The New York Times* (13 de mayo de 2017), https://www.nytimes.com/2017/05 /13/opinion/the-world-is-getting-hacked-why-dont-we-do-more-to-stop-it.html?r=1

Tuhr, A. von, *Tratado de las obligaciones*, t. II, Madrid, 1934.

Tyson, J. «How Internet Infrastructure Works» (9 de febrero de 2011), p. 5.

Urbano Castrillo, Eduardo de, «El terrorismo como forma de organización delictiva», *La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario*, nº 49 (2008), p. 14.

USA Today, AP Twitter Feed Hacked; No Attack at White House (23 de abril de 2013), http://www.usatoday.com/story/theoval/2013/04/23/obama-carney-associated-press-hack whitehouse/2106757/

VACCA, Alexander W., «Military Culture and Cyber Security», *Survival*, vol. 53, nº 6 (2012), p. 159.

VARONA MARTÍNEZ, Gema, «Evolución jurisprudencial en la interpretación de los diversos elementos integrantes de los principales tipos delictivos aplicados respecto del terrorismo de ETA», http://www.ehu.eus/documents/1736829/2067438/05+-+Evolucion+jurisprudencial+I.pdf

VEIGA COPO, A. B., *Tratado del contrato de seguro*, Aranzadi, 2016.

VERDA Y BEAMONTE, José Ramón de, *Veinticinco años de aplicación de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho Al Honor, a la Intimidad*, Aranzadi, 2007.

«Vida», *Diccionario de la Lengua Española*, Edición del Tricentenario, RAE, http://dle.rae.es/?id=blw7uSa

VIDE, Rogel, *La responsabilidad civil extracontractual*, ed. Civitas, Madrid, 1976, p. 76.

VITORIA, Francisco de, *Comentarios a la secunda secundae de Santo Tomás*, Salamanca, vol. 2, 1932, p. 55.

WAMALA, Frederick, «The ITU National Cybersecurity Strategy Guide», *CISSP* (septiembre de 2011).

WATERMAN, Shaun, «Survey: U.S. insurers earned $1B in cyber premiums last year, fedscoop» (26 de agosto de 2016), https://www.fedscoop.com/cyber-insurance-premiums-fitch-report-august-2016/

WEBER, Joscha, «Industrial espionage threatens German companies and Jobs», *DW.com* (29 de junio de 2016), http://www.dw-world.de/dw/article/0,,5645869,00.html; y FITANAKIS, Joseph, «German security group sees rise in industrial, commercial spying», Intelnews.org (26 de mayo de 2009), http://intelnews.org/tag/berthold-stoppelkamp/

WEBER, Rolf H. «Internet of Things - New security and privacy challenges», *Computer Law & Security Review*, 26 (2010), p. 25, https://www.researchgate.net /profile/Rolf_ Weber3/publication/222708179_Internet_of_Things_-_New_security_and_privacy_ challenges/links /0c96053cab03fee371000000.pdf

WEGENER, Henning, «La ciberseguridad en la Unión Europea», *ieee.es* (14 de julio de 2014), http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO77bis2014_CiberseguridadProteccionInformacion_H.Wegener.pdf

Weimann, Gabriel, «Cyber Terrorism: How real is the threat» (13 de mayo de 2004), p. 4, https://www.usip.org/sites/default/files/sr119.pdf

Weimann, Gabriel, «Cyberterrorism: The Sum of All Fears?», Taylor & Francis Inc (mayo de 2004), https://www.princeton.edu/~ppns/Docs/State%20Security/Cyberterrorism%20%20sum%20of%20all%20fears.pdf

Werbach, Kevin, «Digital Tornado: The Internet and Telecommunications Policy», FCC Office of Plans.

«What is a Zero-Day Vulnerability?», *Pctools*, http://www.pctools.com/security-news/zero-day-vulnerability/

«What is hacktivism?», *Stanford*, https://cs.stanford.edu/people/eroberts/cs181/projects/ 2010-11/Hacktivism/what.html

«What is Intellectual Property?», *World Intelectual Property Organization*, Geneva, Switzerland, http://www.wipo.int/edocs/pubdocs/en/intproperty/450/wipo_pub_450.pdf

«What is Zero Day Exploit?», *Kaspersky*, https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

«Why cybersecurity is so important», *BI Intelligence* (5 de abril de 2016), http://www.businessinsider.com/cybersecurity-report-threats-and-opportunities-2016-3

«World Intellectual Property Report 2011», WIPO Economics & Statistics Series (2011), http://www.wipo.int/edocs/pubdocs/en/intproperty/944/wipo_pub_944_2011.pdf

«World Telecommunication/ICT Indicators Database 2010», *International Telecommunication Union*, http://www.itu.int/ITU-D/ict/publications /world /world.html, 2011.

«World Telecommunication/ICT Indicators database 2017», 21.ª edición, *ITU* (3 de julio de 2017), http://www.itu.int/ITU-D/ict/publications/world/world.html

Wright, Richard W., «Rigth, Justice and Tort Law», *Moral Foundations of the law of Torts*, Oxford University Press, 1995.

Yzquierdo Tolsada, Mariano, *Responsabilidad civil extracontractual. Parte general: Delimitación y especies. Elementos. Efectos o consecuencias*, Dykinson, 2015.

ABREVIATURAS

ACM: Association for Computing Machinery.

AN: Audiencia Nacional.

AP: Audiencia Provincial.

ARPANet: The Advanced Research Projects Agency Network.

AVOIDIT: Attack Vector, Operational Impact Defense, Information Impact, and Target.

BYOD Security: Bring Your Own Device.

CC: Código Civil.

CCD-CoE: Cooperative Cyber Defence Center of Excellence.

CCN: Centro Criptológico Nacional.

CCN CERT: Centro Criptológico Nacional-Computer Emergency Reaction Team.

CDMA: Cyber Defence Management Authority.

CEO: Chief Execitive Officer.

CERN: Centro Europeo de Investigación Nuclear.

CERT: Computer Emergency Readiness Team.

CERT-EU: Computer Emergency Response Team of European Union.

CIA: Central Inteligence Agency.

CIFAS: Centro de Inteligencia de las Fuerzas Armadas.

CIO: Chief Information Officer.

CISO: Chief Information Security Officer.

CME: Chicago Mercantile Exchange.

CNA: Computer Network Attack.

CND: Computer Network Defence.

CNE: Computer Network Explotation.

CNI: Centro Nacional de Inteligencia.

CP: Código Penal.

CSIRT: Computer Security Incident Response Team.

CTO: Chief Technology Officer.

DDoS: Distributed Denial of Service.

DEST: International Conference on Digital Ecosystems and Technologies.

DETICA: BAE Systems Applied Intelligence.

DG-Cnect of the European Commission: Directorate General for Communications Networks, Content & Technology.

DLP: Data Loss Prevention.

DTCC: Depositary Trust & Clearing Corporation.

DVD: Digital Versatile Digital.

EC3: Centro Europeo de Lucha contra la Ciberdelincuencia.

ENISA: Agencia Europea para la Seguridad de las Redes y de la Información.

ETA: Euskadi Ta Askatasuna.

EXE: executable.

FBI: Federal Bureau of Investigation.

FIX: Financial Information Exchange.

FSISAC: Financial Services Information Sharing and Analysis Center.

GDP: Gross Domestic Product.

GLEX: Global Exchange.

GPS: Global Positioning System.

GRC: Governance, Risk & Compliance.

IAM: Identity and Access Management.

IC: Infraestructura Crítica.

ICANN: The Internet Corporation for Assigned Names and Numbers.

IDS: Intrusion Detection System.

IETF: The Internet Engineering Task Force.

IFSC: International Financial Services Commission.

IIROC: Investment Industry Regulatory Organization of Canada.

INTECO: Instituto Nacional de Tecnologías de la Comunicación.

IoT: Internet of Things.

IP: Internet Protocol.

IPS: Intrusion Prevention System.

ISACA: Information Systems Audit and Control Association.

ISO: International Organization for Standardization.

ISP: Internet Service Provider.

IT: Information Technology.

ITC: Information Technology and Comunication.

ITU: International Telecommunication Union.

LEC: Ley de Enjuiciamiento Civil.

LHC: Large Hadron Collider.

LOPD: Ley Orgánica de Protección de Datos.

LOPDCP: Ley Orgánica de Protección de Datos de Carácter Personal.

LSC: Ley de Sociedades de Capital.

MDM: Mobile Device Management.

MEDES: Management of Emergent Digital EcoSystems.

NAC: Network Access Control.

NASDAQ: National Association of Securities Dealers Automated Quotation.

NCIRC: Computer Incident Response Capability.

NCSA: Communication and Information Systems Services Agency.

NCSN: New Zealand National Cyber Security Centre.

NIAOC: Information Assurance Operations Centre.

NIST: National Institute of Standards and Technology.

NYSE: New York Stock Exchange.

OECD: Organization for Economic Cooperation and Development.

OPAALS: Open Philosophies for Associative Autopoietic Digital Ecosystems.

OPM: Office of Personnel Management.

OSS: Open Source Software.

OTAN: Organización del Tratado del Atlántico Norte.

PIN: Personal Identification Number.

PYMES: Pequeña y Mediana Empresa.

RED SARA: Sistemas de Aplicacion y Redes para las Administraciones.

RIR: Regional Internet Registries.

RPO: Recovery Point Objective.

SANS Institute: SysAdmin Audit, Networking and Security Institute.

SCADA: Supervisory Control And Data Adquisition.

SIEM: Sintrusion Prevention Systems.

SIFMA: Securities Industry and Financial Markets Association.

SME Software: Subject-Matter Expert Software.

SMIS: Society for Management Information Systems.

SSAN: Sentencias de la Audiencia Nacional.

SSTC: Sentencias del Tribunal Constitucional.

SSTS: Sentencias del Tribunal Supremo.

STC: Sentencia del Tribunal Constitucional.

STS: Sentencia del Tribunal Supremo.

TCP/IP: Transmission Control Protocol/Internet Protocol.

TIC: Tecnologías de la Información y la Comunicación.

TRLSA: Texto Refundido de la Ley de Sociedades Anónimas.

TSX: Toronto Stock Market.

U.S. NIST: United States National Institute of Standards and Technology.

UNODC: United Nations Office on Drugs and Crime.

W3C: The World Wide Web Consortium.

WEForum: World Economic Forum.

WIPO: World Intellectual Property Organization.

SOBRE EL AUTOR

Jesús Jimeno Muñoz

Es abogado especialista en Derecho de Seguros y Responsabilidad Civil. Licenciado en Derecho (2013). Actualmente, se encuentra cursando los estudios de Doctorado en Derecho en la UAH, que completa con una estancia de investigación en la Universidad de Glasgow. Su tesis está siendo patrocinada por la Fundación MAPFRE (Beca I. H. Larramendi) y se enmarca dentro del ámbito de la Responsabilidad Civil y los Seguros. En ella se plantea una visión general y básica de la responsabilidad civil procedente de las ciberamenazas, y los elementos del contrato de seguro en relación con la cobertura de las mismas.

CENTRO DE DOCUMENTACIÓN

Todas nuestras publicaciones a tu alcance

Acceso gratuito a nuestro fondo documental especializado en:

- Seguros
- Gerencia de riesgos
- Prevención

Fundación MAPFRE

Centro de Documentación

www.fundacionmapfre.org/documentacion

P.V.P.: 30 €
ISBN: 978-84-9844-667-8

El riesgo cibernético se ha definido como el riesgo asociado con el uso de las tecnologías de la información y está relacionado con la propiedad, la operatividad, la influencia, la participación y la implementación de las mismas.

Los riesgos cibernéticos podrían afectar a un amplísimo panorama de intereses públicos y privados, por lo que resulta necesario estudiar las acciones que puedan concurrir al daño y la distribución de la responsabilidad entre todos los agentes que participan del ciberespacio.

Así, el presente trabajo plantea un análisis pormenorizado de los elementos de la responsabilidad civil y el derecho de daños en el ciberespacio, con lo que pretendemos establecer las bases de la responsabilidad derivada de la utilización de sistemas tecnológicos y cibernéticos.

Fundación
MAPFRE

www.fundacionmapfre.org
Paseo de Recoletos, 23
28004 Madrid