



Universidad de Valladolid

Facultad de Ciencias Económicas y Empresariales

Trabajo de Fin de Grado

Grado en Finanzas, Banca y Seguros

El mercado del seguro: impacto de las nuevas tecnologías en el sector asegurador

Presentado por:

Tatiana A. Rodríguez Bailón

Tutelado por:

María Jesús Peñas Moyano

Valladolid, 13 de octubre de 2021

RESUMEN

A través de la lectura de este trabajo vamos a tratar de comprender y analizar el sector asegurador en todos sus ámbitos, la normativa vigente, elementos y clases, centrándonos en el impacto de las nuevas tecnologías en el seguro. Veremos como la biotecnología cada vez está más presente en la sociedad, poniendo de manifiesto los riesgos a los que nos enfrentamos y la forma de anticiparnos a ellos.

Asimismo, se defiende la necesidad de la existencia de mayor regulación en los casos de ciber-riesgos, analizando en profundidad las consecuencias que suponen a la sociedad.

PALABRAS CLAVE

Contrato de seguro, nuevas tecnologías, ciber-riesgo, sandbox, insurtech, blockchain, smart contracts, big-data, robótica, neuro derecho.

ABSTRACT

Through reading this paper we will understand and analyze the insurance sector in all its areas, current regulations, elements and classes. Focusing on the impact of new technologies on insurance. We will see how biotechnology is increasingly present in society, highlighting the risks we face and how to anticipate them.

I also defend the need for greater regulation in cases of cyber-risks, cyber-attacks, analyzing in depth the consequences they entail to society.

KEY WORDS

Insurance contract, new technologies, cyber-risk, sandbox, insurtech, blockchain, smart contracts, big-data, robotics, neuro right

CODIGOS DE CLASIFICACION JEL.

El siguiente trabajo lo podemos clasificar atendiendo a la relación de códigos JEL:

Dentro de la categoría de Administración de empresas y economía de la empresa; Marketing; Contabilidad, subcategoría M1. Administración de empresas:

- M15 Gestión de la tecnología de la información

Dentro de la categoría de Desarrollo económico, cambio tecnológico y crecimiento, subcategoría O3. Cambio tecnológico; Investigación y desarrollo (I+D).

- O32 Gestión de la innovación tecnológica y de la I + D
- O33 Cambio tecnológico: opciones y consecuencias; Difusión

Dentro de la categoría de Economía financiera, subcategoría G2. Instituciones y servicios financieros.

- G22 Seguros; Compañías de seguros

ÍNDICE

1. INTRODUCCIÓN AL SEGURO.....	5
2. EL CONTRATO DE SEGURO	8
2.1. CARACTERÍSTICAS.....	8
2.2. ELEMENTOS	10
2.2.1. <i>Elementos Formales</i>	10
2.2.2. <i>Elementos Materiales</i>	10
2.3. CLASES – RAMOS DE SEGUROS.....	11
2.3.1. <i>Ramos personales</i>	12
2.3.2. <i>Ramos patrimoniales</i>	12
2.3.3. <i>Ramos de prestación de servicios</i>	12
3. LAS NUEVAS TECNOLOGÍAS: AVANCES MÁS IMPORTANTES	13
3.1. <i>INSURTECH</i>	13
3.2. <i>BIG-DATA</i>	14
3.3. <i>BLOCKCHAIN</i>	16
3.4. <i>CONTRATOS INTELIGENTES (SMART CONTRACTS)</i>	17
4. RETOS REGULATORIOS.....	19
4.1. <i>SANDBOX</i>	19
4.2. <i>DERECHO DE PROTECCIÓN DE DATOS PERSONALES</i>	21
4.3. <i>NEURO – DERECHO DE SEGUROS</i>	22
5. CIBER – ESPACIO	25
5.1. EL SEGURO CIBERNÉTICO	28
5.2. CIBER-RIESGOS. RESPONSABILIDAD CIVIL. CONTENIDO DEL SEGURO.....	33
5.2.1. <i>Obligaciones del Asegurador</i>	34
5.2.2. <i>Obligaciones del Asegurado</i>	34
5.1.3. <i>Robótica</i>	34
6. CONCLUSIONES	42
7. REFERENCIAS BIBLIOGRÁFICAS.	44

1. INTRODUCCIÓN AL SEGURO.

El aumento de la competitividad, así como el crecimiento de la inflación y los cambios en las preferencias del cliente, han propiciado una innovación en el sector asegurador. Esta situación tiene sus ventajas e inconvenientes. Gracias a esta innovación, las entidades aseguradoras pueden mantener con facilidad su posición en el mercado, ya que se han reducido intensamente los riesgos intraficables y, por lo tanto, gracias a la tecnología el sector asegurador no está expuesto a siniestros sin tarificar.

Asimismo, dicha innovación permite variar el producto para adaptarse al cliente, lo que supone un aumento de la competitividad respecto a años anteriores. No hay que olvidarse de la parte primordial de los seguros, la prima, la cual se ve beneficiada de apenas variación, a consecuencia de la presión en los precios y la disminución de los márgenes. Este último dato, dependiendo del ramo del seguro en el que estemos, puede resultar de vital importancia, ya que el precio de la prima se va a ver como una obligación al ser el seguro de primera necesidad.

La incorporación al mercado de nuevos productos supone un desafío que está ligado a una innovación incremental de los productos para amoldarlos a las necesidades del cliente. Este tipo de desarrollo se puede ver como una flexibilización del producto, con el fin de preservar los riesgos asegurables y perfilar el conjunto de riesgos probables.¹

Desde el punto de vista de la sociedad, todas estas mejoras en el producto son de vital importancia para su contratación. Tiene que ir al unísono el precio, la cobertura y la utilidad. Velando por el equilibrio del seguro.

Un producto tiene que estar equilibrado hacia las necesidades del cliente en ese momento. De nada sirve, por ejemplo, tener un seguro del hogar con una prima

¹ Jimeno Muñoz, J. (2019). *Derecho de daños tecnológicos, ciberseguridad e insurtech*, Ed. Dykinson S.L, Madrid, p. 29.

asequible, si únicamente nos cubre un 25% del valor de la vivienda. Este seguro no daría utilidad al cliente, ya que, en el momento del siniestro, la indemnización por parte del seguro no le va a proporcionar ni siquiera la mitad del valor de la vivienda. Con todo esto y gracias a la innovación, es cada vez más frecuente la incorporación del seguro en sectores como por ejemplo la banca, en el que no solo se aseguran productos de primera necesidad, como pueden ser el hogar o el de vida.

Actualmente empezamos a ver riesgos asegurables como la inteligencia artificial. Este término está formado por las palabras *Insurance* y *Technology*, las cuales definen a la perfección el cambio que están sufriendo las aseguradoras en pleno s. XXI. La tecnología está impactando en el modelo de negocio del sector, aportando un mayor valor y eficiencia en el desarrollo del seguro.

Con mayor frecuencia vemos nuevas categorías asegurables, debido a que las necesidades del cliente han evolucionado. Resulta necesario entender mejor la nueva realidad y proteger en la medida de lo posible el ciber riesgo, que constituye una amenaza actualmente en expansión. Cada vez nos preguntamos más sobre la responsabilidad en el futuro del mundo tecnológico, más en concretamente de la inteligencia artificial. Por ello, las aseguradoras se ven obligadas a mantener dicha innovación como aspecto primordial en su trabajo, ya que tienen que ser capaces de anticipar todo riesgo causante provocado por la tecnología.

Preguntas como:

¿Quién va a ser el responsable jurídicamente hablando del riesgo de la inteligencia artificial?

¿Es el fundador o el propietario del objeto tecnológico el que debe responder ante un imprevisto?

Estas son un ejemplo de las preguntas que tienen que plantearse en la actualidad las compañías aseguradoras. Con el fin de predecir cualquier riesgo evitando los siniestros sin tarificar.

Bien es sabido que el comercio electrónico se ha centrado en bienes tangibles e intangibles, pero no se puede decir lo mismo en referencia a los servicios. Los seguros y su contratación se están incorporando de forma tardía al nuevo soporte contractual y es por ello, por lo que las compañías aseguradoras no pueden olvidarse del desarrollo de las tecnologías tales como el blockchain o los smart contracts, las cuales han plasmado la relevancia en el mundo de la importancia que está teniendo la tecnología en la sociedad.

2. EL CONTRATO DE SEGURO

2.1. CARACTERÍSTICAS

Si nos adentramos en el mundo doctrinal, el contrato de seguro está caracterizado según su finalidad y forma.² Posee una regulación legal en la “*Ley 50/1980, de 8 de octubre, de Contrato de Seguro*”, lo que facilita su trato independiente. Por el cual, según la Sección primera, artículo primero: “*El contrato de seguro es aquel por el que el asegurador se obliga, mediante el cobro de una prima y para el caso de que se produzca el evento cuyo riesgo es objeto de cobertura a indemnizar, dentro de los límites pactados, el daño producido al asegurado o a satisfacer un capital, una renta u otras prestaciones convenidas*”.³

Con anterioridad, la regulación del contrato de seguro estaba en el Código Civil y de Comercio, con carácter de derecho dispositivo. Y cuyo vacío legislativo fue completado por las condiciones generales de contratación y las diversas normas administrativas dictadas para el control de las entidades aseguradora y su actividad.⁴

Las características fundamentales del contrato de seguro son:

- **Aleatorio**. La existencia del siniestro, así como el lugar determinado y forma, es desconocida por las partes tomadoras del seguro. No se sabe con exactitud si va a tener lugar el hecho previsto, aunque la entidad aseguradora puede determinar de manera global los costes desencadenantes del siniestro, mediante cálculos estadísticos. Asimismo, en el momento de contratación del seguro no debe existir riesgo. En cuanto a esta definición, hay autores como el catedrático

² Pérez Bonachea, Mayren y Denis Lorenzo, Yuneidy. (2008). *Estudio teórico-doctrinal del contrato de seguro asociado a la perspectiva del ordenamiento jurídico cubano y la necesidad de afianzar la legislación en ese sentido*. Ed. Espacios Públicos, p. 5.

³ Jimeno Muñoz, J., op.cit., p. 61.

⁴ Tortella Casares, G., Caruana de las Cagigas, L., García Ruiz, J.L., Manzano Martos Martos, A. M. (2012). *Claves del seguro español: una aproximación a la historia del seguro en España*, Ed. Fundación Mapfre, Madrid., p. 9.

mexicano Joaquín Rodríguez, no acepta esta aleatoriedad del contrato de Seguro.

- **Consensual**. Ambas partes deben de estar de acuerdo para su realización. materializándose el contrato cuando se unen la oferta y la aceptación, cualquiera sea la forma de su formalización, oral u escrita⁵.
- **Bilateral**. Ambas partes contratantes tienen obligaciones recíprocas, todo lo contrario, a los contratos unilaterales en los que la obligación es únicamente por una de las partes. Hay autores que defienden la idea de “bilateral perfecto”⁶, para otros es denominado como “bilateral imperfecto”, ya que una de las partes estaba obligada al abono de la prima desde la formalización del contrato y es la aseguradora quien recibe dicha prima.⁷
- **Oneroso**. Cada una de las partes intervinientes recibe algo a cambio de su colaboración⁸. La entidad aseguradora percibe la prima del asegurado y éste la cuantía económica una vez formalizado el siniestro. En este sentido, Rodrigo Uría, lo percibe como la obtención de la ventaja patrimonial perseguida por cada parte.⁹
- **De adhesión**. Por el cual la entidad aseguradora es la encargada de establecer las cláusulas del contrato y del tomador de aceptarlas. En la elaboración de las cláusulas el cliente no toma partido en ellas, es una labor única de la aseguradora. Dichas cláusulas hacen referencia a las

⁵ Pero a efectos probatorios, la ley exige según el artículo quinto de la LCS “El contrato de seguro y sus modificaciones o adiciones deberán ser formalizadas por escrito. El asegurador está obligado a entregar al tomador del seguro la póliza o, al menos, el documento de cobertura provisional. En las modalidades de seguro en que por disposiciones especiales no se exija la emisión de la póliza el asegurador estará obligado a entregar el documento que en ellas se establezca”

⁶ Rodrigo, Uría. (1994), *Derecho Mercantil*, Madrid, Editorial Marcial Pons, p. 55.

⁷ Pérez Bonachea, M. et al, *op. cit.*, p. 7.

⁸ Ley 50/1980 de 8 de octubre, de Contrato de Seguro (LCS). Tal y como recoge el artículo 1 de la LCS, el Contrato de Seguro se define como aquel por el que el asegurador se obliga, mediante el cobro de una prima y para el caso de que se produzca el evento cuyo riesgo es objeto de cobertura a indemnizar, dentro de los límites pactados, el daño

⁹ Busquets Roca, Francisco, Busquets Roca, F. (1988), *Teoría general del seguro*, Ed. Vicens-Vives, Barcelona, p. 50.

condiciones en las que prestara su servicio y por las que el tomador mediante una tarificación, es decir, una prima, debe aceptarlas.

- **De tracto sucesivo.** Los efectos del contrato persisten durante la vigencia de la póliza, debiendo de cubrir por parte de la aseguradora todos los siniestros que se produzcan dentro del plazo de cobertura de la póliza

2.2. ELEMENTOS

Se diferencian varios tipos de elementos en el contrato de seguro: los formales en los que se hallarían la póliza; los materiales donde se encuentran la prima y el riesgo.¹⁰

2.2.1. Elementos Formales.

Póliza, es la parte fundamentas por la que se caracteriza el contrato de seguro, sin ella el contrato no tendría validez alguna¹¹. A través de la póliza, se formaliza el contrato de seguro y en la que se establecen las obligaciones de ambas partes.

Asegurado, es la persona física o jurídica que hace frente a las obligaciones derivadas del contrato de seguro.

Tomador, es la persona física o jurídica que contrata la póliza con la entidad aseguradora, por el cual queda obligado a la realización del pago de la prima.

Beneficiario, aquel por el cual recaen los correspondientes beneficios establecidos en la póliza, por voluntad del tomador.

2.2.2. Elementos Materiales

Prima, es la cuantificación monetaria que realizan los asegurados a la entidad aseguradora, durante un tiempo determinado. Esta prestación puede satisfacerse por primas periódicas o únicas.

Riesgo, aspecto fundamental e idea central por la que se realiza el contrato, con el fin de dar cobertura al mismo.

¹⁰ Busquets Roca, F., *op. cit.*, p. 28.

¹¹ El documento emitido por la Entidad aseguradora, suscrito por ésta y el tomador, que tiene por objeto probar la existencia del contrato de seguro, concretando sus condiciones.

2.3. CLASES – RAMOS DE SEGUROS.

En la actualidad existen diferentes clasificaciones de seguros privados, pero la más extendida es la que les referencia según su naturaleza de riesgos. Es por ello por lo que distinguimos entre los seguros de personas, en los cuales el objeto asegurado es el ser humano; seguros de daños, cuya finalidad es reparar el daño acontecido en el patrimonio y los seguros de prestación de servicios, en los cuales la aseguradora se compromete a realizar el servicio descrito en la póliza.¹²

RAMOS DE SEGURO NO VIDA
<i>Accidentes</i>
<i>Enfermedad (asistencia sanitaria y dependencia)</i>
<i>Vehículos terrestres</i>
<i>Vehículos ferroviarios</i>
<i>Vehículos aéreos</i>
<i>Vehículos marítimos, lacustres y fluviales</i>
<i>Incendio y elementos naturales</i>
<i>Crédito</i>
<i>Caución</i>
<i>Pérdidas pecunarias diversas</i>
<i>Defensa Jurídica Asistencia</i>
<i>Decesos</i>

Fuente: Elaboración propia a partir de datos web

¹² Busquets Roca, F., *op. cit.*, p. 35.

RAMOS DE SEGURO VIDA

El seguro sobre la vida, tanto para caso de muerte como de supervivencia, o ambos conjuntamente, incluido en el de supervivencia el seguro de renta; el seguro sobre la vida con contraseguro; el seguro de nupcialidad, y el seguro de natalidad.

Las operaciones de capitalización basadas en técnica actuarial, que consistan en obtener compromisos determinados en cuanto a su duración y a su importe a cambio de desembolsos únicos o periódicos previamente fijados.

Las operaciones de gestión de fondos colectivos de jubilación, entendiendo por tales aquellas que supongan para la entidad aseguradora administrar las inversiones y, particularmente, los activos representativos de las reservas de las entidades que otorgan prestaciones en caso de muerte, en caso de vida o en caso de cese o reducción de actividades

Fuente: Elaboración propia a partir de datos web

A continuación, se detallan cada uno de estos ramos.

2.3.1. Ramos personales

Hacen referencia a los seguros de personas, cuyas modalidades más importantes son¹³:

- Seguro de vida
- Seguro de asistencia sanitaria
- Seguro de accidentes

2.3.2. Ramos patrimoniales

Engloban a varios seguros que aseguran objetos, ya sea un vehículo, automóvil, es decir, protegen el patrimonio.

2.3.3. Ramos de prestación de servicios

Se caracterizan por la obligación de la entidad asegurador en prestar servicio al asegurado.

¹³ Busquets Roca, F., *op. cit.*, p. 36.

3. LAS NUEVAS TECNOLOGÍAS: AVANCES MÁS IMPORTANTES

3.1. INSURTECH

El término *Insurtech* es muy amplio, actualmente se refiere a actividades muy diversas de la realidad. Más bien esta terminología forma parte de una composición más amplia denominada *Fintech*, que es el conjunto de actividades que gracias a la tecnología prestan servicios reservados a las entidades financieras, la cual también favorece la perfección de productos ya existentes. Asimismo, *Insurtech* se puede conocer de dos maneras, de forma amplia y concreta. En ésta última, puede dirigirse al desarrollo de nuevos operadores como son los *start-ups* tecnológicos, que aspiran a sustituir las entidades aseguradoras como prestadoras de servicios. En cuanto al término más amplio, las *Insurtech* permitirán añadir los cambios llevados a cabo por las entidades aseguradoras tradicionales, con el fin de mejorar su gama de productos e incrementar su eficiencia.¹⁴

Entre el mundo *Fintech* e *Insurtech*, se encuentran los casos que no pretenden sustituir a las compañías aseguradoras como prestadoras de servicios sino colaborar con ellas. No se trata de un modelo de B2C¹⁵ sino del modelo de negocio B2B¹⁶. Y desde un punto de vista *Insurtech*, existen diversas modalidades como son:

- Aparición de nuevos canales comunicativos
- Uso masivo de datos denominado *Big Data*
- Explotación de las facilidades del internet como asemejar aplicaciones por ejemplo del ámbito del seguro del automóvil al ámbito de la salud

Todo ello con el fin de ofrecer al cliente productos más adaptados a sus necesidades, pero que entrañan una dificultad para los organismos reguladores,

¹⁴García Mandaloniz, M. (2019). "Derecho de Seguros 4.0", *Revista española de seguros (publicación doctrinal de derecho y economía de los seguros privados)*, núm. 177. Ed. Española de Seguros, S.L, Madrid, p.9.

¹⁵ B2C, modelo de negocio en el que las empresas están enfocadas a un consumidor final, sin intermediarios

¹⁶ B2B, modelo de negocio en el que se realizan transacciones entre dos empresas

ya que tienen que ser capaces de capturar esta nueva realidad tecnológica y adecuarla a las exigencias regulatorias.¹⁷

3.2. BIG-DATA

La tecnología ha permitido desde sus inicios mitigar las deficiencias e ineficiencias del mercado asegurador. En un futuro puede implicar un cambio más profundo en la forma de comprender la actividad del seguro, ya sea en el cambio de perspectiva de compensar daños a la prevención de estos o también implicando un cambio de vida social, ya el pago de las primas puede llegar a ser un incentivo para expandir determinados tipos de conductas, hábitos de vida, comportamientos deseables...etc.

Big data es un término tecnológico que para conocerlo tenemos que remontarnos a sus antecedentes históricos. La definición de referencia es la siguiente (conocido como “*las tres V*”) ¹⁸:

“Big data son datos que contienen una mayor variedad y que se presentan en volúmenes crecientes y a una velocidad superior”

Otra definición posible es *“el conjunto de datos de mayor tamaño y más complejos, especialmente procedentes de nuevas fuentes de datos”*.

- Volumen. Referido a que la cantidad de datos es relevante, *big data* procesara una gran cantidad de datos de baja densidad.
- Velocidad. Ritmo al que se perciben los datos, transmitida directamente a la memoria en vez de escribirse en un disco

¹⁷ Veiga Copo, Abel B. (2020). *Seguro y tecnología. El Impacto de la digitalización en el contrato de seguro*. Alianza Editorial, Madrid. p. 150.

¹⁸ Gartner, 2001. (Gartner Inc. es una empresa consultora y de investigación de las tecnologías de la información con sede en Stamford, Connecticut, Estados Unidos). Hasta 2001 era conocida como Gartner Group.

- Variedad. Diferentes tipos de datos disponibles se presentan en un tipo no estructurado a diferencia de los datos convenciones que eran estructurados y organizados.

Pero en los últimos años han surgido otras dos V:

- Valor. Los datos tienen un valor intrínseco, pero no poseen utilidad hasta que no se descubre su valor. Este proceso de hallar su valor es complejo, ya que requiere de la intervención de analistas los cuales tienen que predecir comportamientos y plantear las preguntas correctas.
- Veracidad. Referido a la alteración de los datos y su riesgo. Los analistas tienen que preguntarse si los datos obtenidos son los referidos al problema estudiado en concreto.

Existe una asimetría en la información, lo cual supone uno de los evidentes fallos del mercado del sector del seguro, y por todo ello la LOSSEAR en el siguiente artículo detallado a continuación responde detalladamente en materia de protección de datos. Según el artículo 99 Protección de datos de carácter personal de la LOSSEAR *“Las entidades aseguradoras podrán tratar los datos de los tomadores, asegurados, beneficiarios o terceros perjudicados, así como de sus derechohabientes sin necesidad de contar con su consentimiento a los solos efectos de garantizar el pleno desenvolvimiento del contrato de seguro y el cumplimiento de las obligaciones establecidas en esta Ley y en sus disposiciones de desarrollo”*.

Pero no hay que perder de vista lo previsto en el artículo 6.1 Reglamento (UE) 2016/679, por el cual para recabar información es obligatorio informar al interesado del objetivo del tratamiento de sus datos. De esta forma modelos de negocio como *Insurtech*, pueden estar recabando información personal de los usuarios (ya sea con relojes-pulseras inteligentes) de forma ilegal, al no poseer los consentimientos necesarios para su tratamiento. Por ello las empresas *Insurtech*, deberán introducir en sus páginas webs ventanas que permitan

recabar esta información, aunque sea mediante la marcación de una casilla, informando del fin de la captación de datos.¹⁹

3.3. BLOCKCHAIN

Los descubrimientos cuestionables producidos por la digitalización no se deben únicamente a la cantidad de datos tratados y a su análisis. Más bien, la encrucijada se encuentra en las cadenas de bloques, las cuales registran, intercambian y validan la información, mejor conocidas por su término inglés, “*blockchain*”.

Podemos ver un caso cercano, como es el de la compañía Mapfre, la cual creó un centro de excelencia de blockchain denominado B3i, con el fin de asegurar las operaciones de seguros. El presidente de esta compañía, durante su ponencia en un curso de economía, advirtió que: “*MAPFRE RE forma parte de las ALASTRIA que se presenta como el primer consorcio multisectorial promovido por empresas para el establecimiento de una infraestructura semipública presionada blockchain que soporte servicios con eficacia legal en el ámbito español y acorde con la regulación europea*”²⁰.

Tres de las principales características son:

- Independiente, siguiendo los principios de independencia y neutralidad
- Abierta, en lo que se refiere a espacio digital.
- Multisectorial

Actualmente, B3i, está representado aproximadamente el 70% de la capacidad mundial del reaseguro²¹. La funcionalidad del *Blockchain* para el sector asegurador se caracteriza por:

- Mejora en el tratamiento de datos

¹⁹Jimeno Muñoz, J., *op.cit.*, p. 107.

²⁰ García Mandaloniz, M., *op.cit.*, p.24.

²¹González Vargas, Maite., (2018). *Blockchain en el sector financiero y asegurador*, Center for Insurance Research del IE, Madrid. p. 5.

- Reducción de los costes administrativos derivados
- Aumento de la rentabilidad de las aseguradoras
- Establecimiento de patrones
- Eliminación de la reclamación del siniestro
- Predicción de indecencias

Por todo ello y gracias a la gran confianza y seguridad, el Plan de acción de la Comisión en materia de tecnología financiera prevé para esta tecnología un lugar primordial para la futura infraestructura de servicios financieros.

3.4. CONTRATOS INTELIGENTES (SMART CONTRACTS)

No sabemos con exactitud el desarrollo global que se va a producir con el *blockchain*, pero lo que es seguro es que su utilización tiene que ir unida a los *smart contracts*, ya que son piezas fundamentales de código informático que van aparejados al funcionamiento del *blockchain*, es decir, a la cadena de bloques.²²

Los *smart contracts*, son definidos como programas informáticos autoejecutables y automáticos siempre que se cumplan las condiciones previamente programadas en su código. Estos contratos son denominados como inteligentes, pero no por su coeficiente intelectual ya que únicamente reciben órdenes previamente determinadas, pero este no es el debate moral relevante, sino aquellos interrogantes que pueden ocasionar para el derecho. El marco regulatorio que deberá regularlos eficientemente tendrá que adaptarse a las características propias del *blockchain*, ya que es la base técnica de los *smart contracts*. Se sabe que la cadena bloques es imborrable, por lo que si hay un error humano en su codificación desencadenaría un error en la operación contractual. Por todo esto, el marco regulatorio debe resolver todos los interrogantes posibles para evitar cualquier catástrofe futura.²³

²² Illescas, R., (2017) *Revista española de seguros (publicación doctrinal de Derecho y Economía de los Seguros privados)*, núm. 169. Dedicado a: *Insurtech: retos y desafíos de cara a la nueva distribución y contratación de seguros*, Ed. Editorial Española de Seguros, S.L, Madrid, p. 38. (cita completa)

²³ Veiga Copo, Abel B., *op.cit.*, p. 178.

No todo son problemas, ya que una vez resuelto lo relativo a su regulación siguiendo el Código Civil, Código de Comercio y la Ley de Contratos de Seguro, se espera que reduzcan la necesidad de intervención de intermediarios en los seguros y desencadenen los siguientes sucesos:

- Menor número de formularios para su contratación y menores costes
- Mayor rapidez y menores costes (reducción de la prima en seguros)
- Aceleración en la gestión de los siniestros y ejecución de indemnizaciones

Este tipo de contratos cuyo funcionamiento depende de la cadena de bloques, tecnología que da soporte a las criptomonedas, son una solución aplicable a diferentes ámbitos, por ello es considerada como una de las mayores revoluciones tecnológicas y por lo tanto deberán de tenerse en cuenta las particularidades de un contrato de seguro, recogida de en la definición del artículo 1 de la LCS, teniendo así la misma naturaleza.

4. RETOS REGULATORIOS.

4.1. SANDBOX

Una vez definidos estos fenómenos tecnológicos, hay que plantearse la nueva regulación, ya que, si el modelo de las entidades aseguradoras ha sufrido un cambio, también lo hará en lo que se refiere a su régimen. El marco jurídico tendrá que ir variando en la medida que se produce la adaptación del sector al mundo tecnológico. Todo ello con el fin de acoplarse a la perfección a los diferentes requerimientos que plantea esta revolución.²⁴

Se demanda un nuevo desafío regulatorio, adaptado a una nueva necesidad tecnológica global. El pilar fundamental que sustenta estas propuestas es la Ley 7/2020, de 13 de noviembre, para la transformación digital del sistema financiero, Artículo 1, *“Esta Ley regula un entorno controlado de pruebas que permita llevar a la práctica proyectos tecnológicos de innovación en el sistema financiero con pleno acomodo en el marco legal y supervisor, respetando en todo caso el principio de no discriminación.”* En dicha ley se presentó un marco regulatorio para las *Insurtech* y *Fintech*, más bien conocido como *“regulatory sandbox”*, en el que se pretende adaptar el nuevo contexto digital del sector financiero, combinando la innovación con la seguridad por parte de las autoridades competentes. En concreto, se trata de:

- Facilitar el acceso a la financiación, siendo el motor de la economía
- Facilitar el acceso a la estabilidad financiera
- Facilitar el acceso a la integridad de los mercados.

Este modelo, *sandbox*, es similar al implantado en Reino Unido, supervisado por la *Financial Conduct Authority*. La ley 7/2020 del 13 de noviembre, prevé su implantación en España logrando así un entorno seguro de pruebas, en el que se puedan realizar ensayos controlados y delimitados en un proyecto que pueda aportar una innovación aplicable al sistema financiero.

²⁴ García Mandaloniz, M., op. cit., p. 10.

En definitiva, con el *sandbox*, se normaliza la ejecución de pruebas que mejoran al consumidor gracias al buen funcionamiento de los tres regímenes para las tres fases:

- Régimen de acceso. Caracterizada por dos vías
 - o Exención. Destinada para empresas financieras existentes con actividades reguladas y que pretendieran utilizar el *sandbox* para asegurar una viabilidad y potencialidad de la innovación financiera.
 - o No sujeción. Destinada a nuevas empresas sin actividades reguladas y que deseen probar sus productos con más seguridad.
- Régimen de garantía y protección al consumidor
- Régimen de salida

Estas tres fases son similares a las que experimenta un proyecto empresarial en la incubadora de empresas. Se trata de establecer un espacio controlado con un esquema jurídico, con el fin de aportar seguridad y garantías bajo vigilancia, y no de establecer una estructura física adaptada a las necesidades de cada proyecto antes y durante los primeros pasos en el mercado.

En un entorno leal y de libre de competencia, se quiere alcanzar la neutralidad tecnológica, para que los servicios prestados respeten la normativa con independencia del medio en el que se desarrolle. Pero eso sí, sin descuidar el principio de proporcionalidad que establezca que, a mayor dimensión empresarial, mayores requisitos legales. Se pretende compaginar el *sandbox* con la tecnología, configurando un Derecho 4.0.²⁵

²⁵ García Mandaloniz, M., op. cit., p.30.

4.2. DERECHO DE PROTECCIÓN DE DATOS PERSONALES.

Con todo este surgimiento tecnológico, no hay que olvidar la exposición del consumidor. Se debe preservar la seguridad de los datos personales y aportar esas garantías gracias al Reglamento general de protección de datos (RGPD) del 27 de abril de 2016²⁶.

*“ Un derecho claro y comprensible; un consentimiento claro y afirmativo, sin admisión del consentimiento de omisión; un derecho a ser informado en caso de pirateo; un derecho al olvido, y un derecho de traslado de los datos a otro proveedor de servicios son las bases que sustentan el nuevo marco jurídico europeo en el que los profesionales, también el sector asegurador, asumen un papel principal”*²⁷

Todas las medidas que habría de imponerse tendrían que calificarse según su naturaleza y tipología, además de distinguirse por los tipos de riesgos que pudieran presentarse²⁸. Pero la cuestión es:

¿Son las *Insurtech* un riesgo adicional en materia de protección de datos?

Las *Insurtech* tratan los datos del cliente de forma automatizada y son estas automatizaciones las que deben de cumplir las exigencias del nuevo RGPD y de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Según el artículo 99 de la Ley 20/2015, de 14 de julio, (LOSSEAR), *“Las entidades aseguradoras podrán tratar los datos de los tomadores, asegurados, beneficiarios o terceros perjudicados, así como de sus derechohabientes sin necesidad de contar con su consentimiento a los solos efectos de garantizar el pleno desenvolvimiento del contrato de seguro y el cumplimiento de las obligaciones establecidas en esta Ley y en sus*

²⁶ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales a la libre circulación de esos datos.

²⁷ García Mandaloniz, M., op. cit., p. 54.

²⁸García Mandaloniz, M., op. cit., p.17.

disposiciones de desarrollo.” “El tratamiento de los datos de las personas antes indicadas para cualquier finalidad distinta de las especificadas en el párrafo anterior deberá contar con el consentimiento específico de los interesados”

Ahora bien, hay que plantearse si ante estos nuevos competidores tecnológicos es conveniente la revisión de la norma con el fin de incrementar la supervisión en materia de seguridad y protección de datos. Numerosas dudas de operativas pueden surgir y por ello también en el ámbito legal. En las entidades aseguradoras, las medidas aplicables han de ser equitativas en cuanto al volumen de tratamiento de datos, siendo muchos de ellos sensibles para el cliente, como por ejemplos los datos facilitados para la redacción y cobro de las primas (números de cuenta), análisis de riesgo de tomadores, asesoramiento de la información, defensa de reclamaciones...etc. Siendo estos unos pocos ejemplos de la vulnerabilidad del cliente a consecuencia de sus datos.

4.3. NEURO – DERECHO DE SEGUROS

Más allá del avance tecnológico, existe el debate ético, social y legal entorno al empleo por parte de las entidades aseguradoras de la información genética que otorga la ciencia fácilmente. El mal uso de esto provocaría para el derecho a la no discriminación, ya que no existe un tratamiento diferenciado.²⁹

El Consejo de Europa aprobó el 26 de octubre de 2016, la Recomendación del Comité de ministros en la cual se trataba el procesamiento de datos sanitarios, suplicando en que las entidades aseguradoras no requieran pruebas genéticas a efectos del seguro, salvo previa autorización por la ley. El objetivo era conseguir que ningún individuo fuera discriminado por sus rasgos genéticos. El artículo 11 del Convenio para la protección de derechos humanos *“prohíbe toda forma de discriminación de una persona a causa de su patrimonio genético”*. Con estas actuaciones, ninguna entidad aseguradora podrá exigir la realización de pruebas genéticas, aunque bajo petición de reducción de la prima en seguros de salud, estén incluyendo en la oferta la realización de estudios genéticos del consumidor. A día de hoy no se sabe si en un futuro se puedan pedir.

²⁹ García Mandaloniz, M., op. cit., p. 20.

Otra de las dudas actuales es:

¿Puede la compañía aseguradora preguntar si el tomador conoce su genoma?

La finalidad es predecir enfermedades excluyendo así las más probables a padecer por el asegurado, o simplemente con el fin de reducir o aumentar la prima a pagar. Ante esta situación, el Parlamento europeo respondió negativamente, a través de la Resolución sobre los problemas éticos y jurídicos de la manipulación genética del 16 de marzo de 1989³⁰, en especial en los puntos 19³¹ y 20³². En el cual se prohibieron:

- La realización de pruebas genéticas
- La declaración de los resultados de las pruebas de ADN realizados

Pero con todo ello, el debate no finaliza sino todo lo contrario, se expande. Provocado por la Ley 4/2018 del 11 de junio por la que tiene lugar la modificación del texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias³³. La autonomía que poseen los consumidores sobre su voluntad, para realizar pactos y contratos, no deberá de utilizarse con un fin discriminatorio por el hecho de padecer una enfermedad. Por ello, es necesario aplicar una ley que establezca la nulidad de cualquier cláusula o pacto, que realice este tipo de discriminación. Por ejemplo, en la LCS, disposición adicional quinta, se establece que *“no se podrá discriminar a las personas que padezcan VIH/SIDA”*, es decir, se prohíbe la denegación de contratación por razón de esta enfermedad, salvo que se encuentre justificación.

³⁰ Doc. A 2-327/88, 16 de marzo del 1989. Diario Oficial de las Comunidades Europeas, 96/165, 17 de abril 1989.

³¹ Artículo 19 del Doc. A 2-237/88, *“Hace constar que las compañías de seguros no tienen ningún derecho a exigir que se realicen análisis genéticos antes o después de la firma de un contrato de seguro ni a que se comuniquen los resultados de análisis genéticos ya realizados y que los análisis genéticos no pueden convertirse en condición previa para la firma de un contrato de seguros”*.

³² Artículo 19 del Doc. A 2-237/88, *“Considera que la compañía de seguros no tiene ningún derecho a obtener información sobre los datos genéticos que el asegurado conoce”*.

³³ BOE nº 142, 12 de junio del 2018, págs., 60207-60208 (RCL 2018, 7832).

Definitivamente, el neuro-derecho de seguros, habrá de estar al corriente de los diversos peligros que desencadena los resultados genéticos de los asegurados, con el fin de no caer en la discriminación.

5. CIBER – ESPACIO

El desarrollo de las IT (*Information Technology*) llegará a reducir la probabilidad de los siniestros gracias a los sistemas de gestión y anticipación al riesgo. A su vez, los daños derivados de los siniestros pueden ser solucionados gracias a la rapidez en la que se trasmite y procesa la información³⁴. Las infraestructuras más críticas que sostienen las acciones del día a día dependen cada vez mas de este desarrollo de las IT y a su vez de la hiperconectividad. Por ello es de vital importancia establecer un ciber ecosistema saludable, en la que la ciber seguridad se verá inmersa dentro del interés general con el fin de lograr una estabilidad social

Esta situación fomenta la inversión privada en materia de ciberseguridad, con el fin de reducir el aumento de ataques criminales en el ciberespacio, los cuales están en continua expansión. Es en estos casos, en el que los efectos de la IT hacen que las compañías deban considerar los ciber riesgos como un aspecto en el que es necesario realizar una política estratégica efectiva. Algunos países, ya han implantado este tipo de política con el fin de posicionarse en lugares más seguros para su economía digital.

Actualmente estamos adentrados en un mundo digital, la tecnología está teniendo un papel fundamental en nuestro día a día. Tal es así que ya se habla de una cuarta revolución industrial o más bien revolución 4.0, ya que la sociedad crece al mismo tiempo que se están desarrollando las tecnologías y por lo tanto pasan a formar parte de su vida diaria. Por ello, las empresas deben lograr adaptarse a este crecimiento tecnológico, porque de no ser así pueden llegar a quedarse obsoletas en la sociedad.

Cada vez se encuentran mayores retos para el sector asegurador, los clientes cambian, la demanda también y en consecuencia lo hace la oferta. Las compañías deben aprovechar el potencial de datos del cliente y del entorno con el fin de adaptar lo máximo posible el producto a cada mercado establecido.

Durante los últimos años, el mercado del seguro lleva utilizando la tecnología como medio de contratación, apertura a nuevos entornos, con el fin de mejorar sus productos ya existentes en el mercado. Esta importancia la vemos manifestada en el mercado *Insurtech*, el cual se encuentra en plena expansión. Pero antes haremos una breve referencia sobre este mercado, con el fin de entender la tendencia alcista que ha ido experimentando a causa de:

- La transformación en la mentalidad de la sociedad, gracias a la llegada de los denominados *millenials*
- Nuevas formas de aseguramiento más allá de objetos tradicionales
- Los gigantes tecnológicos.

Estos últimos, han ido aprovechando su potencial económico para poder competir con las entidades aseguradores tradiciones e incorporar nuevos modelos de negocio.

CAMBIOS CLAVE DE LA ERA DIGITAL EN LOS SEGUROS
<i>Social: Nuevo Paradigma</i>
<i>Movil: Canal ideal posventa</i>
<i>Pricing: Pólizas a medida</i>
<i>Analytics: La informacion es la base de la transformación</i>
<i>Insurtech: Operador financiero</i>

Fuente: Elaboración propia a partir de datos de Deloitte

La ciber seguridad de los sistemas privados contribuye al interés público en la medida en que las inversiones favorecen la implantación o creación de un ciber espacio saludable. En este sentido, cuando las entidades y usuarios implantan estas políticas se benefician cuatro puntos claves:

- El propio sistema
- Clientes y proveedores
- Ciber ecosistema en general

Y es por todo ello por lo que actualmente se diferencian tres niveles de interés que dependen del desarrollo de sistemas de la ciber seguridad:

- Interés corporativo
- Interés colectivo
- Interés individual

Si hablamos del interés general presente en el ciber espacio, es necesario hacer referencia a las acciones que tienden a debilitar la estabilidad del ciberespacio como es el caso de la terminología inglesa: *cyber crime*, *cyber attack* y *cyber terrorismo*.³⁵ De tal forma es entendible el interés nacional como la protección de los intereses políticos, culturales y sociales que se relacionan con el ciberespacio. Un ciber crimen es considerado como la realización de cualquier acción penada por la ley cuya manifestación se realiza a través de un sistema informático, careciendo de un interés político sin afectar a la nación. A pesar de esto, los ciber crímenes suelen llevarse a cabo por personas individuales y no por países en su conjunto.

De todas formas, el *cyber crime*, *cyber attack* y *cyber terrorismo* dan lugar a daños desarrollados a través del ciberespacio y con una consecuencia que depende de la acción voluntaria, con el objetivo de hacer daño o conseguir beneficiarse de la acción no consentida de la persona que lo sufre.

En referencia al interés general de establecer un ciberespacio saludable, la amenaza más destacable es la desencadenada por los “Riesgos globales”, denominados así por su naturaleza, ya que no respetan las fronteras de los estados³⁶. En diciembre de 2013, el departamento de Seguridad Nacional publica la Estrategia de Ciberseguridad Nacional, en la que se dotó en este documento de un plan estratégico a España en el que se reconoce los principios básicos de protección del ciber espacio, destacando:

- Principio de responsabilidad compartida
- Principio de proporcionalidad

³⁵ Jimeno Muñoz, J., *op. cit.*, p. 81.

³⁶ Schwab, K. (2013), *La cuarta revolución industrial*, World Economic Forum, Ed. Debate, p.8.

- Principio de racionalidad y eficacia
- La cooperación internacional

En esta dirección, ha sido importante la regulación encaminada a establecer sistemas que logren asegurar un nivel de ciber seguridad adecuado. Por todo esto, la Unión Europea durante estos últimos años han publicado diferentes estrategias y normas en las que destacan las siguientes:

“COM (2001) 209 “Seguridad de las redes y de la información. Propuesta para una política europea”

“COM (2006) 251 “Estrategia para una sociedad de información segura”

“2009/C 321.01 “De un enfoque europeo común sobre la seguridad de la información y de las redes”

“COM (2010) 245 “Una agenda digital para Europa”

No cabe la menor duda de que el ciber espacio es una realidad que aún está pendiente de explicar y definir completamente.

5.1. EL SEGURO CIBERNÉTICO

Es evidente que las nuevas tecnologías de la comunicación y el desarrollo de la informática han generado riesgos que desestabilizan la seguridad y confidencialidad de estas. Sin duda, es el campo que actualmente despierta mayor interés debido a su gran potencial de crecimiento en la rama de seguros.

La vigilancia de estos riesgos será el motor principal del sector asegurador y responder de forma dinámica a través de herramientas digitales permitirá esquivar los ataques cibernéticos y en consecuencia anticiparse a ellos. Estos riesgos son fruto del desarrollo tecnológico y de la hiperconectividad de la economía que abarcan desde los más simples como es el robo de un dispositivo electrónico desde un ordenador, hasta el robo de cuantiosos datos de valor incalculable.³⁷

³⁷ Jimeno Muñoz, J., *op. cit.*, p. 52.

El seguro con su metodología clásica de cobertura es insuficiente en este tipo de riesgos, ya que no solo afectan al tomador de la póliza, sino que pueden causar grandes daños que afecten a terceros. Por ello es necesario su renovación y actualización a la etapa en la que estamos inmersos, haciendo frente a desafíos extremos que no pueden ampararse bajo sistemas estadísticos clásicos, desencadenando así una nueva era en la canalización del seguro. El pirateo, el terrorismo informático, la ciber extorsión y otros múltiples actos vandálicos son los que conforman las diferentes amenazas que hoy sufre la sociedad a causa de la economía digitalizada.

- El pirateo, es el centro del riesgo en las pólizas que cubren el acceso malicioso al software informático confiscando datos o servicios.
- El terrorismo, hace referencia a la amenaza al riesgo del sistema asegurado actuando en nombre de una organización con el fin de provocar un acceso no autorizado a los datos.
- La ciber extorsión, es cualquier amenaza creíble que realice un tercero contra el asegurado con el objetivo de corromper información confidencial privada.

En cuanto a la cobertura de los seguros cibernéticos, existen dos tipos de protección, el primero frente a los riesgos directos como es la pérdida de datos y el segundo la responsabilidad frente a terceros, más bien ante los clientes o entidades regulatorias. Dichos riesgos se relacionan con las responsabilidades civiles semejantes al que la violación puede ocasionar a terceros.

Frente a la multitud de riesgos existentes, es importante a la hora de su tarificación establecer la forma de resarcimiento. No es lo mismo que el daño se efectúe en un medio tecnológico, cuyo resarcimiento habitual es la sustitución por otro equipo que el daño se materialice en la filtración o copia de datos privados, en este caso el resarcimiento no solo constara de la reparación del daño, sino que además habrá que establecer un marco nuevo de seguridad que evite este tipo de situaciones. Por otro lado, es fundamental distinguir entre riesgo real y el declarado, con el fin de evitar el desequilibrio entre ambos. La exigencia de medidas que deberán de ser llevadas a cabo por el asegurado tendrá como objetivo minimizar el impacto del riesgo y en consecuencia

provocaran que el asegurado realice prestaciones periódicas de mantenimiento de dispositivo.

El daño no solo interrumpe la seguridad informática de una empresa, sino que genera unos costes adicionales de renovación y obtención de esa información, como por ejemplo la petición de ayudas de asesoramiento de expertos, aplicación de nuevas murallas de acceso, indemnización de daños...etc.

La detección del riesgo es una de las grandes dificultades que indican en la valoración del riesgo real. Un riesgo, que como bien se ha señalado con anterioridad, es susceptible de agravarse a causa de la robotización. Esto multiplica de manera exponencial el daño ocasionado en el tiempo y su dificultad valorativa puede incidir en el cálculo del coste de la prima. Pensemos en no solo la cobertura global de tantos riesgos asociados a la tecnología sino en la particularidad de uno solo de estos riesgos, el robo. ¿Cómo podemos asegurar los bienes, programas fruto de la tecnología frente al robo de estos? Estos riesgos producidos provocarían un daño reputacional y en caso de materializarse en siniestro pueden ocasionar la interrupción en continuar el trabajo u objetivo.³⁸

PRINCIPALES MEDIOS CAUSANTES DE PERDIDAS DE DATOS
<i>Actos maliciosos informáticos</i> <i>Malware</i> <i>Hacking</i> <i>Acceso no autorizado</i> <i>Error humano</i> <i>Error de programación</i>

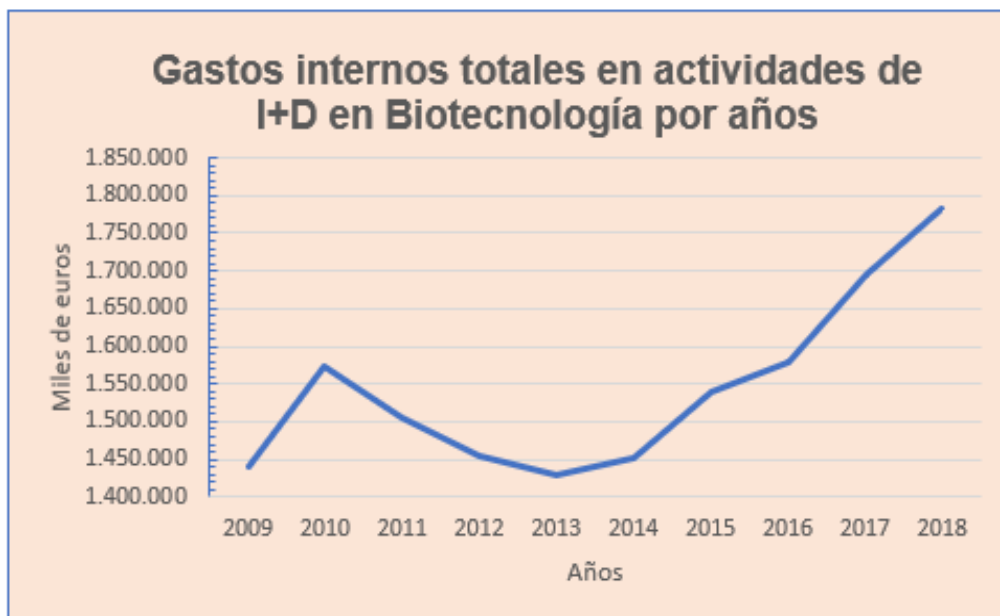
Fuente: Elaboración propia a partir de datos bibliográficos (Seguro y Tecnología. El impacto de la digitalización en el mundo del seguro)

Frente a la realidad de esta ciber extorsión o cibercriminalidad, la garantía que se asegura es concretada para riesgos como el robo, no siendo una noción física

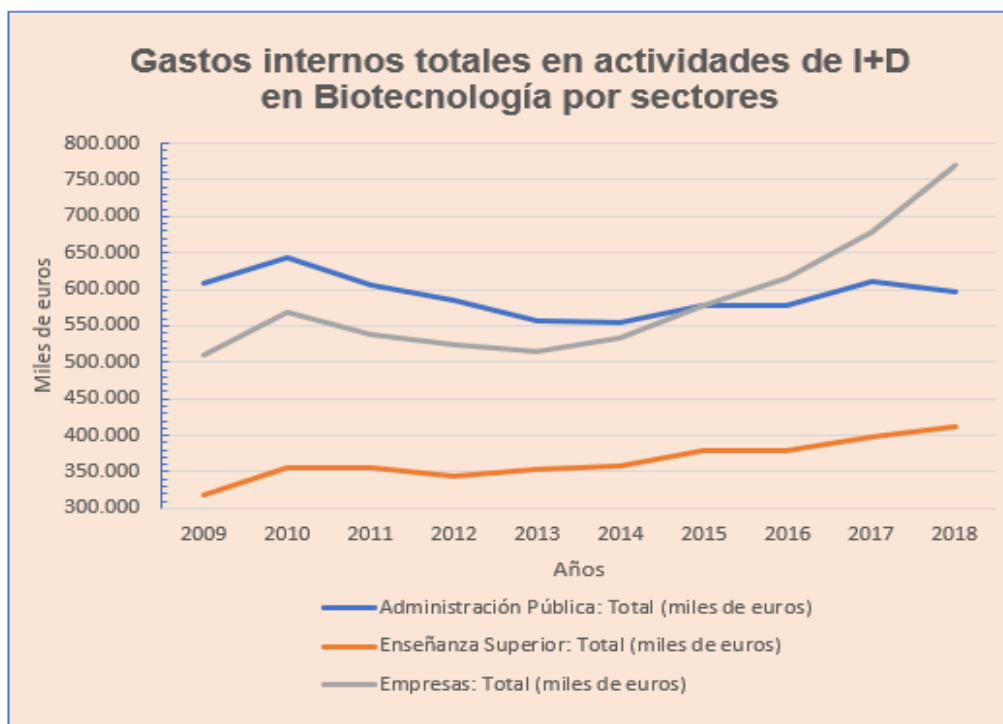
³⁸ Veiga Copo, Abel B., *op. cit.*, págs. 401 y ss.

de sustracción por parte de un tercero, sino de elementos informáticos que son inmateriales. Asimismo, además de la malversación de valores en beneficio propio, existe la malversación de programas software. Pero finalmente uno de los riesgos más ejecutados es del fraude de contenido mediante la colaboración de medios informáticos. Es por todo ello, por lo que el seguro debe confeccionar y ofrecer pólizas que garanticen frente a este tipo de riesgos, los cuales desgraciadamente tienen que afrontar tanto las empresas como los particulares.

En el siguiente gráfico podemos ver el avance en la incorporación de la biotecnología en la actualidad, así como su evolución en los últimos años.



Fuente: Elaboración propia a partir de datos del INE



Fuente: Elaboración propia a partir de datos del INE.

Como se puede ver, en el primer grafico se aprecia un gran avance en los últimos nueve años, destacando como el mundo tecnológico se ha ido desarrollando en el medio e influenciando al conjunto de la sociedad. Los grandes cambios se notan de manera más creciente en las empresas, que han duplicado los gastos en actividades en biotecnología respecto al 2009. Es un claro ejemplo de cómo la tecnología se ha adaptado extremadamente bien en nuestro día a día.

Era impensable pensar que en tan solo unos pocos años se duplicaría el porcentaje de gasto dedicado en un sector tecnológico que en aquella época no tenía más que la mínima importancia. Quién sabe si en un futuro, o dentro de unos otros pocos años, en vez de duplicar la tasa la triplicamos con respecto a otros años, siendo cada vez menor la diferencia en el tiempo.

5.2. CIBER-RIESGOS. RESPONSABILIDAD CIVIL. CONTENIDO DEL SEGURO.

El ciberespacio es un mundo digital en el que pueden suceder actuaciones que ocasionan un daño a un tercero. Las IoT (*Internet Of Things*)³⁹ es un ejemplo claro de las consecuencias que pueden formarse en cualquier ámbito. Por ello es necesario que las instituciones de toda índole diseñen políticas para garantizar un ciberespacio responsable. Esta responsabilidad es muy amplia y se deriva en cuatro tipos:

1. CIVIL. A su vez se distingue la responsabilidad contractual y extracontractual.
2. PENAL. En referente a los particulares y a las empresas, ya sea por propia actuación o a consecuencia de un tercero.
3. LABORAL. Respecto a los trabajadores de las compañías afectados por un ciber incidente.
4. ADMINISTRATIVA. Derivada frente a organismos regulatorios por el incumplimiento de obligaciones.

Asimismo, el contrato de seguro establece unas obligaciones entre la parte aseguradora y del asegurado, centradas en el pago de la prima y la cobertura cuando tiene lugar el suceso definido en la póliza. En el caso del punto 1 anterior, el de responsabilidad civil, el suceso definido es el hecho imprevisto cuyas consecuencias sea responsable el asegurado, y por tanto la cobertura consistirá en la indemnización a un tercero por la que está obligado el asegurado.

Más allá de los elementos generales del contrato de seguro, se derivan varias obligaciones de forma particular que permiten el buen funcionamiento de las pólizas, como por ejemplo el deber del asegurado de reducir el riesgo/daño, notificando así las variaciones posibles del objeto asegurado.⁴⁰

³⁹ Jimeno Muñoz, J., *op. cit.*, págs. 110 y ss.

⁴⁰ Tortella Casares, G. et al, *op. cit.*, p. 14.

5.2.1. Obligaciones del Asegurador

En el seguro de responsabilidad civil tienen lugar dos obligaciones para la entidad aseguradora:

- Pago indemnización
- Defensa Jurídica del asegurado. Las ciber pólizas se ha centrado en el carácter asistencial, pero en el caso de las de responsabilidad civil sería necesario introducir el carácter de asistencia técnica, con el objetivo de facilitar la recuperación del sistema después de sufrir un ciber evento.⁴¹

5.2.2. Obligaciones del Asegurado

Según el artículo 1 *“El contrato de seguro es aquel por el que el asegurador se obliga, mediante el cobro de una prima y para el caso de que se produzca el evento cuyo riesgo es objeto de cobertura a indemnizar, dentro de los límites pactados, el daño producido al asegurado o a satisfacer un capital, una renta u otras prestaciones convenidas”* y el 14 *“El tomador del seguro está obligado al pago de la prima en las condiciones estipuladas en la póliza. Si se han pactado primas periódicas, la primera de ellas será exigible una vez firmado el contrato. Si en la póliza no se determina ningún lugar para el pago de la prima, se entenderá que éste ha de hacerse en el domicilio del tomador del seguro”* de la LCS, la obligación principal del tomador es del pago de la prima.

Por otra parte, el tomador del seguro está obligado la prestación de tres deberes con relevancia en los seguros de responsabilidad civil, que son la comunicación del siniestro, el deber de salvamento y la colaboración jurídica.

5.1.3. Robótica

No cabe duda de que el sector asegurador tiene establecido a la perfección ambas responsabilidades tanto del asegurado como de la compañía aseguradora. Pero habría que plantearse si se mantuviese esta situación en lo referente al mundo robótico. La robótica es hoy la manifestación más desarrollada de la inteligencia artificial, y por ello es necesario establecer una regulación adecuada a la misma. Este es uno de los debates que se están

⁴¹ Jimeno Muñoz, J., *op. cit.*, págs. 234 y ss.

produciendo en la actualidad, ya que es uno de los mayores retos al que se va a enfrentar el mundo asegurador.

En la vida cotidiana cada vez es más frecuente la presencia de robots, máquinas inteligentes...etc. Ya sea en las actividades del mundo empresarial, automoción, hogar, las cuales están quebrando la comunicación entre los seres humanos. También es verdad que la robótica supone riesgos hasta ahora desconocidos o que anteriormente estaban más o menos controlados, como por ejemplo la pérdida de la privacidad.

Los robots replican comportamientos humanos, que quizás en un futuro tengan la capacidad de decidir por sí mismos, lejos de cualquier control por parte del ser humano. Por ello es necesario preguntarse como habrá que asegurar los daños que puedan llegar a causar los robots, como sesgar los riesgos y sobre todo decidir quién es el responsable, a quien se le imputan esos riesgos. Si el ser humano ha sido capaz de crear virus e infectar diversos programas informáticos, ¿Un robot no podrá hacerlo también?

Es por ello por lo que debemos contemplar un debate jurídico para buscar mecanismos que mitiguen el daño, los cuales tienen que partir desde la premisa del seguro ya sea obligatorio o voluntario, ya que este es primordial para diluir el riesgo, consiguiendo su posterior eliminación. Los mercados asegurados están innovando a causa de esta revolución, ya que rompe con la estructura tradicional.

Otra de las preguntas claves es, ¿Quién responde ante un siniestro, el poseedor del robot o su programador? Por esto mismo se están enfocando directrices a efectos de la inteligencia artificial y el potencial daño que pueden ocasionar. Se desarrolló el *“Informe sobre la responsabilidad derivada de la inteligencia artificial y otras tecnologías emergentes”* del Grupo de Expertos de la Comisión Europea⁴², esta responsabilidad se sustancia en la siguiente premisa:

⁴² Sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza, tal como se contempla en el informe final y el Plan de Acción del Grupo de Expertos en datos FAIR de la Comisión, de 2020, [COM(2020) 65 final]

“En situaciones que exponen a terceros a un riesgo incrementado de datos, un seguro de responsabilidad civil obligatorio podría darles a las víctimas un mejor acceso a la compensación y proteger a los potenciales causantes contra el riesgo de responsabilidad”

Otra de las cuestiones es el pago de la prima, ¿Quién tendrá que pagarla y en que concepto? Cuando es el propio robot quien actúa y toma decisiones automáticas, ¿Quién responde inicialmente? Para todo esto, el informe anterior⁴³ establece una serie de sugerencias, tituladas como *“key findings”*

“Cuanto más frecuente o grave sea el daño potencial resultante de la tecnología digital emergente y cuanto menos probable sea que el operador pueda indemnizar a las víctimas; más adecuado será obligar a contar con un seguro de responsabilidad civil para la cobertura de tales riesgos”

“Los fondos de compensación se pueden usar para proteger a las víctimas de daños que tienen derecho a indemnización de acuerdo con las normas de responsabilidad aplicables, pero cuyas reclamaciones no pueden ser satisfechas”

La Resolución del Parlamento Europeo, de 16 de febrero de 2017, en la que se establecen recomendaciones sobre normas de Derecho civil sobre robótica (2015/2103 (INL)) se centra en el aseguramiento de robots y en la creación de un fondo de garantía, muy similar al existente en el seguro de responsabilidad civil de circulación de vehículos, en el cual se garantiza que todas las víctimas de siniestros ocasionados por robots sean compensadas correctamente. La norma europea establece una obligatoriedad en el aseguramiento, y es la creación de un fondo de garantía *mutatis mutandis*, en la que se compensen daños producidos por un robot. Se producirá un cambio con respecto a la ubicación del artículo 75 de la LCS, trasladado a la LOSSEAR, en la disposición

⁴³ Sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza, tal como se contempla en el informe final y el Plan de Acción del Grupo de Expertos en datos FAIR de la Comisión, de 2020, [COM(2020) 65 final]

adicional segunda, *“Establecimiento e información sobre seguros obligatorios. 1. Se podrá exigir a quienes ejerzan determinadas actividades que presenten un riesgo directo y concreto para la salud o para la seguridad de las personas, incluida la seguridad financiera, la suscripción de un seguro u otra garantía equivalente que cubra los daños y perjuicios que puedan provocar y de los que sean responsables. La garantía exigida deberá ser proporcionada a la naturaleza y alcance del riesgo cubierto.”*

Existen otras dos resoluciones adicionales en la cuales la primera de ellas ⁴⁴ se delimita a quien se le imputa la responsabilidad de los daños producidos, en función de si el robot tiene autonomía o no:

“Determinar a quién incumbe realmente la responsabilidad de los daños o perjuicios causados por un robot, las competencias adquiridas a través de la formación de un robot no deberían confundirse con las competencias estrictamente dependientes de su capacidad de aprender de modo automático”

Y la segunda resolución⁴⁵ en la que se propugna un sistema de gestión de riesgos en la cual:

“no se centra en la persona que actuó de manera negligente como personalmente responsable, sino en la persona que es capaz, en determinadas circunstancias, de minimizar los riesgos y gestionar el impacto negativo”

5.2.3.1. Regulación aplicable.

Actualmente no tenemos un marco regulatorio definido ante la responsabilidad de las acciones de un robot. Pero ¿Hasta qué punto podemos considerarlos con

⁴⁴ Artículo 56, Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica, (2015/2103(INL)).

⁴⁵ Artículo 55, Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica, (2015/2103(INL))

respecto a nuestro código civil los responsables de las acciones que puedan causar a terceros? Y, en consecuencia, ¿Qué régimen de responsabilidad civil hay que aplicar a los robots que no encajan en estos cánones reales?

Lo que, sí que está claro que ante un siniestro hay detrás un responsable, ya sea el robot, el propietario o el fabricante de éste, ya que puede darse la situación de que la materialización del siniestro haya tenido lugar por una mala práctica de su poseedor o por un error en la ejecución.

El Anexo A de la Comunicación de la Comisión de 16 de febrero de 2017 establece respecto a la responsabilidad civil de los robots lo siguiente:

AA *“Considerando que, cuanto más autónomos sean los robots, más difícil será considerarlos simples instrumentos en manos de otros agentes (como el fabricante, el operador, el propietario, el usuario, etc.); que esta circunstancia, a su vez, suscita la cuestión de si la normativa general sobre responsabilidad es suficiente o si se requieren normas y principios específicos que aporten claridad sobre la responsabilidad jurídica de los distintos agentes y su responsabilidad por los actos y omisiones de los robots cuya causa no pueda atribuirse a un agente humano concreto, y de si los actos u omisiones de los robots que han causado daños podrían haberse evitado”.*

AB *“Considerando que, en última instancia, la autonomía de los robots suscita la cuestión de su naturaleza y de si pertenecen a una de las categorías jurídicas existentes o si debe crearse una nueva categoría con sus propias características jurídicas”*

AC *“Considerando que, en el actual marco jurídico, los robots no pueden ser considerados responsables de los actos u omisiones que causan daños a terceros; que las normas vigentes en materia de responsabilidad contemplan los casos en los que es posible atribuir la acción u omisión del robot a un agente humano concreto —como el fabricante, el operador, el propietario o el usuario—, y en los que dicho agente podía haber previsto y evitado el comportamiento del robot que ocasionó los daños; que, además, los fabricantes, los operadores, los propietarios o los usuarios podrían ser*

considerados objetivamente responsables de los actos u omisiones de un robot”

AD *“Considerando que, según el marco jurídico vigente, la responsabilidad por daños causados por productos defectuosos —en la que el fabricante de un producto es responsable de un mal funcionamiento— y las normas que rigen la responsabilidad por una actuación que ocasiona daños —en la que el usuario de un producto es responsable de un comportamiento que deriva en un perjuicio— se aplican a los daños ocasionados por los robots o la inteligencia artificial”*

AE *“Considerando que también son manifiestas las deficiencias del marco jurídico vigente en el ámbito de la responsabilidad contractual, ya que la existencia de máquinas concebidas para elegir a sus contrapartes, negociar cláusulas contractuales, celebrar contratos y decidir sobre su aplicación hace inaplicables las normas tradicionales; considerando que esto pone de relieve la necesidad de adoptar nuevas normas eficientes y actualizadas, acordes con los avances tecnológicos y las innovaciones recientemente aparecidas y utilizadas en el mercado”*

AF *“Considerando que en materia de responsabilidad extracontractual podría no ser suficiente el marco ofrecido por la Directiva 85/374/CEE que solo cubre los daños ocasionados por los defectos de fabricación de un robot a condición de que el perjudicado pueda demostrar el daño real, el defecto del producto y la relación de causa a efecto entre el defecto y el daño (responsabilidad objetiva o responsabilidad sin culpa)”*

AG *“Considerando que, pese al ámbito de aplicación de la Directiva 85/374/CEE, el marco jurídico vigente no bastaría para cubrir los daños causados por la nueva generación de robots, en la medida en que se les puede dotar de capacidades de adaptación y aprendizaje que entrañan cierto grado de imprevisibilidad en su comportamiento, ya que un robot podría aprender de forma autónoma de sus experiencias concretas e interactuar con su entorno de un modo imprevisible y propio únicamente a ese robot”*

Por todo ello, en otros supuestos y en última instancia, quien adquiere un robot tendrá que responder de los daños causados a terceros. La clave será saber separar la indemnización del daño y de la responsabilidad. Pero ¿Pueden

aplicarse las normas de responsabilidad civil sobre un producto defectuoso? Son muchos los supuestos que encajarían bajo la connotación de actividades arriesgadas, como es el caso de la gestión de una fábrica nuclear, pero al igual que son peligrosas son lícitas, como todo lo que tiene que ver con la biotecnología.

Lo que sí está claro es que no debemos de pasar por alto el daño causado por una decisión, una auto ejecución del propio programa, ya que no sabemos si el creador de este debe responder por la conducta que ha generado el daño o por el contrario debería imputarse a quienes emplean estos algoritmos. Por ejemplo, pensemos en quien dirige un dron, el marco jurídico actual no puede dar solución ante la acción de este robot, aunque se comporte de forma autónoma. Es por ello por lo que deberíamos avanzar un paso más, hablando no solo de responsabilidad civil contractual, sino también extracontractual. No es desorbitado pensar en los daños que se puedan producir en el ámbito patrimonial del propietario del robot, los cuales son retornables a los expuestos en el Código Civil.⁴⁶ En este cuerpo legal existen diversos artículos en los cuales se establecen normativas sobre bienes y servicios defectuosos.⁴⁷

O que decir si es la propia máquina quien establece la norma a aplicar y perfecciona un contrato. A órdenes de la Unión Europea empieza toda una explosión a través de informes de por donde se debería de avanzar ante los daños de esta inteligencia artificial⁴⁸.

⁴⁶ Artículo 1101 del CC, “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 aquéllas”.

⁴⁷ Artículo 128. La legitimación podrá ser impugnada por los que se crean perjudicados en sus derechos, cuando se otorgue a favor de los que no tengan la condición legal de hijos naturales o cuando no concurren los requisitos señalados en este capítulo

⁴⁸ El 8 de abril de 2019, se promulga la CCEPE (Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones denominadas “Generar confianza en la inteligencia artificial centrada en el ser humano” (Bruselas, 8.4.2019. COM (2019) 168 final)

Definitivamente la dualidad de los robots es una realidad, en la que debemos avanzar jurídicamente para asegurar un entorno confortable, seguro y eficaz.

6. CONCLUSIONES

En la actualidad, el contrato de seguro está muy presente dado el tipo de sociedad en la que vivimos, estando expuestos a diferentes riesgos. El sector asegurador está en un ámbito que se encuentra en continuo crecimiento, y cuya relevancia está más que demostrada, ya que desde hace tiempo existen diversos tipos de seguros cuya contratación es obligatoria. Tanto la estructura como el funcionamiento del mercado asegurador posee ciertas peculiaridades, como es el CCS (consorcio de compensación de seguros) y el CESCE (agencia española de crédito a la exportación) ya que al formar parte de la UE y exceptuando casos como los dos anteriores, posee un sector similar al resto de mercados europeos.

Con respecto al objetivo principal del trabajo – el impacto de las nuevas tecnologías en el sector asegurador – es necesario dejar claro que las compañías aseguradoras deben de implementar estos avances tecnológicos en su día a día si no quieren quedarse atrás, ya que vivimos en una era digital en la que la tecnología ha protagonizado un papel fundamental en nuestras vidas. Actualmente las personas nacen, crecen y conviven con la tecnología, desde un simple aparato electrónico para monitorizar al recién nacido durante la noche, hasta drones teledirigidos que salvan vidas. Es por ello por lo que el mundo empresarial debe adaptarse a esta nueva forma de vida, amoldándose a este contexto digital, ya que de no hacerlo estarían abocadas al fracaso.

Esta implantación de los avances tecnológicos trae consigo varios beneficios tanto para los clientes como las aseguradoras. El foco principal de estas últimas es gestionar eficientemente el riesgo, permitiendo la eliminación de intermediarios y reduciendo los costes operativos de tiempos anteriores. Todas estas ventajas permiten a las aseguradoras reducir el precio de las pólizas, ajustándolas a un riesgo real, el cual gracias a estos avances tecnológicos es más fácil de cuantificar y estudiar. En consecuencia, de esto se consigue aumentar la competitividad y solvencia de estas compañías.

Una vez más, gracias al uso de estas nuevas tecnologías como las tratadas en el trabajo – big data, smart contracts, blockchain – las aseguradoras pueden

ofrecer productos personalizados a los clientes, aumentando su satisfacción derivando así en el incremento de ingresos de las aseguradoras. El enfoque en el cliente de forma individual se ha convertido en fundamental para asegurar el éxito en los diferentes mercados.

Aunque no todo conlleva ventajas, al mundo de la robótica todavía le queda mucho por desarrollar, el poseedor de cualquier producto autómatas está expuesto a varios riesgos, como son el de la responsabilidad del automatismo de la máquina, estudiando hasta qué punto es responsable o no el dueño del robot del riesgo que pueda ocasionar a un tercero, en quien recae la responsabilidad y muchas otras preguntas que actualmente no tienen una respuesta firme.⁴⁹

Como vemos, la implementación de las nuevas tecnologías por parte de las aseguradoras ya no es una opción, sino una necesidad para estar actualizada y mantenerse competitivamente en el mercado asegurador. Estamos viviendo una de las transiciones sociales más importantes que se ha conocido en el tiempo, basada en los efectos de la revolución tecnológica, los nuevos modelos económico y las nuevas revoluciones tecnológicas. Por ello, la agilidad en entender esta nueva realidad es clave para avanzar en el sector asegurador. Habrá de saber cómo afrontar eficazmente las oportunidades del momento, las cuales seguirán avanzando con el paso de los años y por ello debemos de anticiparnos a ellas, desencadenando así una mejora en nuestra posición en el mercado.

⁴⁹Veiga Copo, Abel B. *op. cit.*, p. 305.

7. REFERENCIAS BIBLIOGRÁFICAS.

Busquets Roca, Francisco (1988). *Teoría General del Seguro*, Vicens-Vives, Barcelona.

Comisión Europa (2020). Sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza. https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf

García Mandaloniz, M. (2019). "Derecho de Seguros 4.0", *Revista española de seguros (publicación doctrinal de derecho y economía de los seguros privados)*, núm. 177. Ed. Editorial Española de Seguros, S.L, Madrid

González Vargas, Maite, (2018) *Blockchain en el sector financiero y asegurador*, Center for Insurance Research del IE, Madrid.

Illescas, R. (2017) *Revista española de seguros (publicación doctrinal de Derecho y Economía de los Seguros privados)*, núm. 169. Dedicado a: Insurtech: retos y desafíos de cara a la nueva distribución y contratación de seguros, Ed. Editorial Española de Seguros, S.L, Madrid

Jimeno Muñoz, J. (2019). *Derecho de daños tecnológicos, ciberseguridad e insurtech*. Dykinson S.L, Madrid

Pérez Bonachea, Mayren y Denis Lorenzo, Yuneidy (2008). *Estudio teórico-doctrinal del contrato de seguro asociado a la perspectiva del ordenamiento jurídico cubano y la necesidad de afianzar la legislación en ese sentido*. Espacios Públicos, México.

Rodrigo, Uría (1994). *Derecho Mercantil*, Madrid, Editorial Marcial Pons.

Schwab, K. (2013). La cuarta revolución industrial, World Economic Forum, Ed. Debate

Tortella Casares, G., Caruana de las Cagigas, L., García Ruiz, J.L., Manzano Martos Martos, A. M. (2012). *Claves del seguro español: una aproximación a la historia del seguro en España*. Ed: Fundación Mapfre, Madrid.

Veiga Copo, Abel B. (2020). *Seguro y tecnología. El Impacto de la digitalización en el contrato de seguro*. Alianza Editorial, Madrid.