CUADERNOS
DE LA FUNDACIÓN

C / 232

Implicaciones jurídicas en el desarrollo y uso de sistemas de inteligencia artificial en el sector asegurador

Alfonso Ortega Giménez
José Bonmatí Sánchez
Juan José Gonzalo Domenech

Fundación
MAPFRE

Área de Seguro y Previsión Social

Implicaciones jurídicas en el desarrollo y uso de sistemas de inteligencia artificial en el sector asegurador

Alfonso Ortega Giménez
José Bonmatí Sánchez
Juan José Gonzalo Domenech

Fundación MAPFRE

Paseo de Recoletos, 23
28004 Madrid (España)

www.fundacionmapfre.org

ISBN: 978-84-9844-792-7
Depósito Legal: M-33978-2021
Maquetación y producción editorial: Cyan, Proyectos Editoriales, S.A.

PRESENTACIÓN

Desde 1975 Fundación MAPFRE desarrolla actividades de interés general para la sociedad en distintos ámbitos profesionales y culturales, así como acciones destinadas a la mejora de las condiciones económicas y sociales de las personas y de los sectores menos favorecidos de la sociedad.

Dentro de estas acciones, el área de Seguro y Previsión Social trabaja con el objetivo de promover y difundir el conocimiento y la cultura del seguro y la previsión social. Para ello convoca anualmente las Ayudas a la Investigación "Ignacio H. Larramendi", que facilitan apoyo económico a quienes deseen desarrollar proyectos de investigación en su campo de actuación. Además, publica informes periódicos y monografías sobre diferentes ámbitos del seguro y la previsión social y organiza jornadas y seminarios.

En este marco se encuadra la presente publicación, ya que es fruto de una Ayuda a la Investigación "Ignacio H. de Larramendi" concedida en el año 2019 a Alfonso Ortega Giménez, José Bonmatí Sánchez y Juan José Gonzalo, para el desarrollo del trabajo de investigación titulado: *Implicaciones jurídicas en el desarrollo y uso de sistemas de inteligencia artificial en el sector asegurador,* tutorizado por Rafael Estévez, director general adjunto de Servicios Jurídicos y Secretaria General de MAPFRE Iberia.

En cuanto a las actividades orientadas a la sociedad en general, el área de Seguro y Previsión Social crea contenidos gratuitos y universales en materia de seguros que divulga a través de la página web Seguros y Pensiones para Todos, y organiza seminarios en universidades, talleres para escolares y visitas gratuitas para grupos al Museo del Seguro. Asimismo, esta área publica guías divulgativas para dar a conocer aspectos básicos del seguro.

Además, cuenta con un centro de documentación especializado que da soporte a todas sus actividades y que está abierto al público en general. Sus actividades se encuentran disponibles y accesibles en internet, para usuarios de todo el mundo, de una manera rápida y eficaz, a través de nuestra página web: www.fundacionmapfre.org.

Fundación MAPFRE

Alfonso Ortega Giménez

Doctor en Derecho, 2014 (calificación: sobresaliente *Cum Laude* por unanimidad); premio extraordinario de Doctorado, 2018; licenciado en Derecho, 2000, y máster en Comercio Internacional también por la Universidad de Alicante, 2001.

Profesor titular de Derecho internacional privado de la Universidad Miguel Hernández de Elche. Director del Observatorio Provincial de la Inmigración de Alicante. Vicedecano de grado en Derecho de la Facultad de Ciencias Sociales y Jurídicas de Elche. Académico de Honor de la Academia Internacional de Ciencias, Tecnología, Educación y Humanidades desde 2018 y vocal del Observatorio Valenciano de la Inmigración. Socio-director de COEX International Trade, *Spin-Off* de la Universidad Miguel Hernández de Elche, que se dedica al asesoramiento, consultoría y formación en internacionalización de la empresa y planificación jurídica internacional.

Es consultor de Derecho internacional privado de la Universitat Oberta de Catalunya (UOC) desde el segundo semestre del curso académico 2008/2009 y consejero académico del despacho de abogados Ara y Asociados, con sede principal en Alicante y oficinas en Murcia, Madrid y Pekín (China).

Reconocidos dos sexenios de investigación correspondientes al tramo 2002-2007 CNEAI (fecha concesión: 23-10-19), al tramo 2009-2017 CNEAI (fecha concesión: 21-06-18) y al tramo 2010-2016 AVAP (fecha concesión: 18-01-18). Ha recibido numerosos premios en docencia e investigación.

Ponente habitual en numerosos cursos organizados en España y en el extranjero en materia de Derecho internacional privado, Derecho de la nacionalidad, Derecho de extranjería, Derecho del comercio internacional, Contratación internacional y Protección de datos de carácter personal, entre otros.

Autor de diferentes artículos, notas, recensiones y comentarios relacionados con dichas materias publicados en revistas científicas, técnicas y de divulgación, españolas y extranjeras; ha participado como autor, coautor, director y/o coordinador en más de 180 libros.

José Bonmatí Sánchez

Graduado en Derecho por la Universidad Miguel Hernández de Elche (2017) y máster de Acceso a la Abogacía, con especialidad en Derecho mercantil, en el Centro de Estudios Garrigues (2018). Abogado ejerciente colegiado en el Ilustre Colegio de Abogados de Madrid. Actualmente ejerce como abogado en el bufete de abogados Ayuela Jiménez Legal, en el aárea de Derecho mercantil y está cursando el máster en Data Science y Business Analytics impartido por el IMF Business School. Respecto a la actividad investigadora, esta se ha centrado principalmente en el sector de las nuevas tecnologías, destacando, entre otras, la realización del trabajo final de máster centrado en la inteligencia artificial y responsabilidad ("Inteligencia artificial y gestión de riesgos"), su coautoría en el libro *Comentario a la Ley Orgánica de Protección de Datos y garantía de los derechos digitales* y ganador de la II edición de Premios Secciones del ICAM en la sección 40 de robótica, inteligencia artificial y realidad virtual y aumentada con el trabajo de investigación "La automatización inteligente de la toma de decisiones y el principio de transparencia: el derecho de explicación" y la III edición de Premios Secciones del ICAM en la sección 26 de Derecho societario y gobierno corporativo con el trabajo de investigación "Discrecionalidad del órgano de administración y responsabilidad: la debida diligencia a través del uso de algoritmos".

Juan José Gonzalo Domenech

Analista de cumplimiento IT en servicios internos de Deloitte, ejerciendo labores de gestión de los diferentes marcos normativos sobre la seguridad de la información y continuidad de negocio, tales como ISO/IEC 27001, ISO 22301, NIS y SOC. Graduado en Derecho por la Universidad Miguel Hernández de Elche y máster en Derecho de las Telecomunicaciones, Protección de Datos, Sociedad de la Información y Comunicación Audiovisual, y grado superior en Administración de Sistemas Informáticos en Red - Ciberseguridad. Certificado CESCOM e IFCA sobre cumplimiento normativo y Lead Implementer ISO/IEC 27001:2013 por la British Standard Institution. Actualmente es consultor de protección de datos y seguridad de la información. En cuanto a la experiencia investigadora, destaca el trabajo final de grado "Big Data, protección de datos y Derecho internacional privado", por el cual fue premiado por el ISDE con el IX Premio Jurídico Internacional, en la categoría de Derecho internacional. Coautor del libro *Comentario a la Ley Orgánica de Protección de Datos y garantía de los derechos digitales.*

ABREVIATURAS

AEPD: Agencia Española de Protección de Datos.

ALTAI: Assessment List for Trustworthy AI.

EI: Evaluación de Impacto.

EIOPA: European Insurance and Occupational Pensions Authority.

FAQ: Frequent Answer and Questions.

HLEG: High Level Expert Group on AI

IA: Inteligencia Artificial.

IAF: Inteligencia Artificial Fiable.

IaaS: Infraestructure as a Service

IoT: Internet of Things.

ISO: Organización Internacional de Normalización o Estandarización.

LSSI: Ley de Servicios de la Sociedad de la Información.

ML: Machine Learning.

OCDE: Organización para la Cooperación y el Desarrollo Económicos.

PaaS: Platform as a Service.

PIB: Producto Interno Bruto.

RGPD: Reglamento General de Protección de Datos.

SaaS: Software as a Service.

TI: Tecnologías de la Información.

UE: Unión Europea.

ÍNDICE

1. OBJETIVOS Y JUSTIFICACIÓN DEL PROYECTO Y METODOLOGÍA DE LA INVESTIGACIÓN

Durante los últimos años, el sector asegurador se encuentra inmerso en un proceso de transformación tecnológica para adaptarse a las nuevas necesidades del sector. El uso de las nuevas tecnologías en el sector asegurador se conoce actualmente con el término *insurtech*.

En un contexto marcado por la constante evolución tecnológica, como se puede observar en el estudio *Hype Cycle for Emerging Technologies 2018*[1] publicado por Gartner, cabe destacar que encontramos numerosas tecnologías que están siendo objeto de desarrollo y uso en el mercado, como el *blockchain*, el internet de las cosas (IoT) o la inteligancia artificial (IA).

El auge de las nuevas tecnologías está suponiendo la digitalización del mercado y de los operadores que intervienen en este. El uso de nuevas tecnologías como el *blockchain*, el IoT y la IA permiten a las empresas ofrecer servicios más personalizados y aprovechar las nuevas oportunidades que presenta el mercado. Pero el uso de estas tecnologías no solo acompaña nuevas oportunidades, sino que también comportan incertidumbres que deben ser gestionadas por la empresa.

Entre las tecnologías más utilizadas en el sector asegurador, debe destacarse el uso de la IA. Tanto por parte de las propias aseguradoras en la prestación de sus servicios (p. ej., automatización en la toma de decisiones, *profiling* de clientes, etc.), como por las personas y bienes objeto de aseguramiento (p. ej., la contratación de seguros en coches autónomos, drones inteligentes, etc.).

En este contexto, no se puede obviar la importancia de la IA en los diferentes modelos de negocios existentes y los beneficios que esto conlleva. En este sentido, y

[1] Disponible en: https://www.gartner.com/en/newsroom/press-releases/2018-08-20-gartner-identifies-five-emerging-technology-trends-that-will-blur-the-lines-between-human-and-machine (fecha de consulta: 22-03-2020).

según el informe de PWC *Sizing the Price*[2], en el año 2018 la IA aportó 2 billones de dólares al PIB mundial.

La IA es objeto de aplicación en una gran variedad de sectores, debido a la amplia variedad de funciones y tareas que puede cumplir. Entre los sectores afectados, el asegurador no es una excepción, y ya hay compañías aseguradoras que están empezando a aplicarla para analizar reclamaciones y efectuar el pago de indemnizaciones en un tiempo récord de tres segundos, analizando en ese espacio temporal el proceso de recepción de reclamaciones, referencia de políticas, detección de fraude, pago y notificación a los clientes, como es el caso de la entidad FRISS, que ha desarrollado un software de evaluación de riesgos y detección de fraude en el ámbito de las aseguradoras[3].

Es evidente la gran mejora de la productividad y el ahorro de costes derivados de la automatización de los procesos, pero el uso de herramientas basadas total o parcialmente en tecnologías de IA también implican una serie de riesgos de diversa índole:

a. En primer lugar, el cumplimiento de las obligaciones derivadas del propio uso de sistemas de IA como, por ejemplo, la gestión del cumplimiento en materia de privacidad, transparencia en la toma de decisiones, eliminación de sesgos discriminatorios, garantiza la fiabilidad y las implicaciones de ciberseguridad durante todo el ciclo de vida del sistema.

b. En segundo lugar, y dado que el sector asegurador es uno de los sectores con mayor carga regulatoria (con una clara orientación a la protección del consumidor), así como un marcado multinivel y dispersión normativa, debemos prestar atención a los riesgos de incumplimiento de la normativa específica aseguradora derivados del uso de sistemas de IA en el sector asegurador como, por ejemplo:

---

[2] Disponible en: https://www.pwc.es/es/publicaciones/tecnologia/sizing-the-prize.html (fecha de consulta: 22-03-2020).

[3] María Torrego, J. (20 de mayo de 2020). *El futuro del sector* Insurtech *en España*. Disponible en: https://elreferente.es/mas/el-futuro-del-sector-insurtech-en-espana/ (fecha de consulta: 17-09-2021).

– La denegación automática de reclamaciones solicitadas sobre la base de la existencia de cualquier enfermedad declarada del asegurado, como consecuencia de un sesgo discriminatorio (disposición adicional 5.ª de la Ley 50/1980 de contrato de seguro[4]).

– Reducción de la calidad de los servicios de atención al cliente como consecuencia de la falta de supervisión humana en el aprendizaje y desarrollo de la IA (artículo 195.18 de la Ley 20/2015 de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras[5]).

– La no motivación de una denegación de contratación de un contrato de seguro cuya decisión ha recaído sobre un sistema de IA (artículo 22 del RGPD).

c. Por último, no hay que olvidar las importantes implicaciones éticas que, a la hora de desarrollar y desplegar los sistemas de IA, deben tenerse en cuenta, garantizando, entre otras cuestiones, una correcta transparencia entre el asegurado/tomador y el asegurador, así como evitando discriminaciones y opacidades.

Por otro lado, surgen nuevos retos en el negocio asegurador cuando el riesgo no lo posee una persona, sino una misma aplicación de IA que puede intervenir en la materialización del riesgo; por lo que se discute el régimen de responsabilidad e incluso el papel del asegurador en este tipo de casuística. No hay más que observar las complejas cuestiones legales que nacen tras el auge de los coches autónomos y cómo los siniestros producidos por estos vehículos deben ser abordados por el sector asegurador.

Para afrontar la dispersión e incertidumbre jurídica, marcada por la gran regulación existente en materia de seguros, protección del consumidor y protección de datos personales, así como las propuestas de regulación de los sistemas de IA, resulta necesario que la empresa aseguradora cuente con un modelo de gestión

[4] *BOE* núm. 250, de 17-10-1980.

[5] *BOE* núm. 168, de 15-07-2015.

que le permita tratar los riesgos incipientes del uso de esta tecnología. Por eso podemos asumir –por analogía– el modelo de gestión de riesgos derivado del RGPD, centrado en el uso de una "evaluación de impacto" (EI) sobre los riesgos que presenta el uso de la IA y el tratamiento de estos desde una doble perspectiva –técnica y jurídica–, planteando en el presente trabajo una metodología para el desarrollo de una EI sobre el uso de un sistema de IA por parte de la entidad aseguradora.

En consecuencia, este trabajo se justifica en la medida en que aporta una adecuada seguridad jurídica para la resolución de las importantes cuestiones legales que el desarrollo y despliegue de sistemas de IA puede suscitar al sector asegurador, fijando los siguientes objetivos a cumplir:

a. Determinar la aplicación práctica de la IA en el sector asegurador y los beneficios que implicarían su introducción en el modelo de negocio.

b. Determinar los riesgos legales que una entidad aseguradora asume como consecuencia del uso de sistemas de IA.

c. Encuadrar y analizar los riesgos que una entidad aseguradora asume con la implementación de sistemas de IA en modelo de negocio, desde el punto de vista de la regulación propia del sector asegurador.

d. Analizar los problemas éticos que pueden derivarse por la aplicación de la IA en el sector asegurador.

e. Analizar y desarrollar un régimen de responsabilidad adecuado para aquellas entidades aseguradoras que implementen en su modelo de negocio sistemas de IA.

f. Explicar y resolver situaciones prácticas donde se evidencien los problemas legales de la IA en el sector asegurador y su resolución desde el punto de vista jurídico.

2. EL USO DE LAS NUEVAS TECNOLOGÍAS EN EL MERCADO Y SU IMPACTO JURÍDICO

2.1. CUARTA REVOLUCIÓN INDUSTRIAL: LAS NUEVAS TECNOLOGÍAS Y SU IMPACTO EN EL MERCADO

Los operadores económicos siempre se han enfrentado a un mercado en constante cambio y, sin duda, ha sido en los últimos años, con el desarrollo y avance en tecnologías relacionadas con el IoT, el Big Data y la IA, así como la mejora en la conectividad, almacenamiento de información (p. ej., líneas 5G, *cloud computing,* etc.) y potencia de computación, que se ha propiciado uno de los cambios más disruptivos de las últimas décadas: la cuarta revolución industrial.

La revolución industrial 4.0 o cuarta revolución industrial se erige sobre el uso de las nuevas tecnologías, facilitando la unión del mundo real con el mundo digital y permitiendo a las empresas organizar mejor sus procesos, adaptándose con mayor agilidad a las necesidades de la demanda y gestionando de forma más eficiente sus recursos.

La digitalización del sector empresarial, tanto en la producción y distribución de bienes como en la prestación de servicios, está permitiendo compartir de forma más ágil grandes cantidades de información, cuyo análisis ofrece a los operadores una visión más exacta sobre su entorno, convirtiéndose así su uso en una pieza fundamental para las empresas que quieren acceder o mejorar su posición en el mercado y, en definitiva, mantener su capacidad competitiva.

Aunque la digitalización del mercado y sus operadores se construye sobre el uso de una gran variedad de tecnologías y procesos, entre ellas hay varias que han adquirido un papel clave con respecto al resto: el IoT, el Big Data y la IA.

La coordinación en el uso de estas tecnologías, pues debe matizarse que estas no son estancas e independientes, ha permitido a los operadores del mercado desarrollar una gran variedad de aplicaciones y herramientas como, por ejemplo, la adopción de decisiones más informadas, mediante la obtención, almacenamiento y análisis de datos con la finalidad de extraer *insights,* reduciendo así la incertidumbre y los riesgos derivados de la toma de decisiones. En definitiva, todas las tecnologías giran en torno al mismo concepto: los datos.

Por este motivo ya se ha acuñado la expresión de que los datos se han convertido en el "petróleo" del siglo XXI, y esto se debe, principalmente, a que la información que se puede extraer de ellos (también denominada *insights*) adquiere especial valor en la evolución de los operadores del mercado, permitiendo, entre otras, explicar las causas de un acontecimiento (descriptivo), orientar en la toma de decisiones a través de la extracción de patrones (predictivo) e incluso recomendar la apertura de nuevas líneas de negocio (prescriptivo).

Es en este punto donde aparecen las empresas *data-driven,* es decir, aquellas que, en la era del cambio y de la digitalización del mercado, centran sus procesos y la toma de decisiones en los datos. Tradicionalmente, las empresas han organizado su actividad conforme a las experiencias propias, el comportamiento del mercado e intuiciones, lo que dotaba al resultado de las decisiones de una incertidumbre que, en algunos casos, podía ser altamente perjudicial para el futuro del propio operador.

La integración de las nuevas tecnologías en el modelo y funcionamiento de una empresa le puede reportar, siempre que haga un uso adecuado y adaptado a cada actividad, de una gran cantidad de beneficios:

- *Cualitativos:* mejorando el rendimiento y eficiencia en sus procesos productivos, optimizando los recursos y reduciendo el tiempo de fabricación o prestación del servicio.

- *Cuantitativos:* reportando beneficios económicos, consecuencia directa del uso responsable de los recursos y la toma de decisiones informadas.

El impacto que tiene la digitalización del mercado crece anualmente de forma exponencial, siendo cada vez más las empresas que reportan el incremento de sus beneficios. En este sentido, las empresas que forman parte de Asociación Española para la Digitalización (DigitalES), como Telefónica, Accenture o Mastercard, generaron un total de 34.500 millones de euros de valor añadido bruto en la economía española, es decir, casi un 3,3 % del total, sustentaron más de 250.000 empleos totales en España, impulsaron una inversión de más de 3.500 millones de euros y destinaron más de 2.000 millones de euros a investigación, desarrollo e innovación (I + D + i) durante al año 2017[6].

La consultora IBM respalda los beneficios de la automatización de procesos, afirmando que los sistemas de automatización inteligentes analizan los datos hasta 25 veces más rápido que el cerebro humano, reduciendo los costes hasta en un 75 % en tareas repetitivas[7].

El impacto es aún mayor si se analizan las cifras más allá de nuestras fronteras. Así lo refleja el informe publicado por PWC[8], en el que se asegura que para el año 2030 el impacto económico derivado del uso de nuevas tecnologías, como los sistemas de IA, supondrá una contribución de hasta 15,7 billones de dólares a la economía global, materializándose la mayor parte de estas ganancias en los países que decidan invertir y desarrollar en el campo de la IA. El informe destaca que países como China se beneficiarán de un aumento del 26 % del PIB en 2030 y América del Norte con un aumento del 14,5 %, representando ambas casi el 70 % del impacto económico global.

Los operadores de mercado no son ajenos al potencial desarrollo y oportunidades que brinda el mercado digital, no solo por poder llegar a clientes y usuarios de todos los rincones del mundo, sino también por la posibilidad de implementar, a

---

[6] *Vid.* Deloitte, *El impacto de la digitalización en España. Contribución de las empresas DigitalES a la economía española,* 2019, p. 5.

[7] *Vid.* IBM Institute for Business Value, *La evolución de la automatización de procesos.* Informe ejecutivo, 2018, p. 8.

[8] *Vid.* PWC, *Sizing the prize. What is the real value of AI for your business and how can you capitalize.* Informe ejecutivo, 2017.

su actuación en el mercado, las soluciones que las nuevas tecnologías ofrecen, buscando adquirir mayores niveles de competencia.

Adicionalmente, cabe destacar que las empresas no solo se enfrentan a una transformación del mercado sin precedentes, sino también al cambio de mentalidad de los usuarios y consumidores de los bienes y servicios, que se han transformado en clientes caracterizados por la información, la comparativa, la agilidad y la disminución de la fidelidad.

Por otro lado, no podemos obviar la inversión pública de la cual es protagonista la Unión Europea mediante el programa de inversión NextGeneration EU, aprobado en junio de 2020, y materializado en el Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo de 12 de febrero de 2021 por el que se establece el mecanismo de recuperación y resiliencia, como un mecanismo financiero generado por la UE y distribuido entre los Estados miembros con el fin de que estos realicen reformas e inversiones estructurales ante los estragos generados por la covid-19 en el mundo, incluyendo la transición digital como uno de los ejes fundamentales del plan.

En el terreno nacional, España aprobó el Plan de Recuperación, Transformación y Resiliencia. Uno de los programas tractores de inversión del plan es la Estrategia Nacional de Inteligencia Artificial, que va a movilizar 500 millones de euros en el periodo de 2021 a 2023; y recientemente, en julio de 2021, fue creado el fondo Next Tech, impulsado por el Ministerio de Asuntos Económicos y Transformación Digital, cuyo fin es fomentar el desarrollo de proyectos digitales de alto impacto y la inversión en empresas en crecimiento mediante el refuerzo de instrumentos públicos de financiación, la atracción de fondos internacionales y la potenciación del capital riesgo, todo dentro de los programas estratégicos aprobados como estrategia España Digital 2025, el Plan de Recuperación, Transformación y Resiliencia, y la Estrategia Nacional de Inteligencia Artificial.

La inversión en IA se encuentra en un momento "dulce" donde todos los actores públicos y privados reconocen su potencial de generación de valor, añadido a la creación de certidumbre legal con la creación de nuevos instrumentos legales europeos, que se pretenderá desarrollar a lo largo de este trabajo.

2.2. RETO REGULATORIO: RIESGOS EN EL USO DE LAS NUEVAS TECNOLOGÍAS

Sin perjuicio de lo anterior, no todo son beneficios respecto al desarrollo y uso de las nuevas tecnologías, su implantación por los operadores del mercado conlleva la aparición de nuevos escenarios jurídicos que deben tenerse en cuenta a la hora de determinar el plan de adaptación y uso, debido a la actual incertidumbre regulatoria que genera: por un lado, la ausencia de normas específicas aplicables al desarrollo y uso de las nuevas tecnologías; y por otro, la dispersión de normas aplicables en función del contexto en el que se haga uso de la tecnología (p. ej., normativa de protección de datos, defensa de los consumidores, sectores regulados, etc.).

Centrándonos en los riesgos normativos actuales, podemos destacar la incidencia de la normativa de protección de datos personales, debido a que, como ya se ha citado previamente, el sustento funcional de las nuevas tecnologías se basa fundamentalmente en el uso de datos y, mayormente, el tratamiento de datos personales, lo que supone la aplicación de la normativa de protección de datos y, en consecuencia, de sus límites y obligaciones.

En este sentido se puede citar, respecto de la toma de decisiones automatizadas, los límites que impone la ley y las obligaciones relativas al cumplimiento del deber de información y el derecho de explicación, dado que en la toma de decisiones automatizadas se considera fundamental que el destinatario de esta se encuentre informado sobre el tipo tratamiento que se está llevando a cabo y la estructura en la toma de las decisiones.

También tiene impacto en la seguridad de la información el uso de sistemas que traten datos personales, sin perjuicio del resto de información que estos utilicen, a raíz de las obligaciones impuestas, por ejemplo, por 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 Europea, o el propio RGPD. No son pocas normas las que imponen como obligación la adopción de una serie de medidas técnicas y organizativas que aseguren un nivel mínimo de protección, atendiendo a los riesgos que implica, entre otras cuestiones, la finalidad del tratamiento.

Además, la utilización de dichas tecnologías puede generar riesgos legales respecto a las obligaciones jurídicas específicas impuestas en un sector regulado, como pueden ser el sector sanitario, bancario, financiero o asegurador. Por ejemplo, la incertidumbre que genera la aplicabilidad del principio de proporcionalidad en el uso de un sistema de registro distribuido para mejorar el cumplimiento de las obligaciones en materia de prevención del blanqueo de capitales respecto a la hora de cumplir con la obligación de doble identificación, o incluso las cuestiones que suscita, para principios como el de transparencia, el uso de sistemas de IA que permitan determinar el riesgo de las transacciones con clientes sobre la base de los datos obtenidos y su tratamiento automatizado.

Por tanto, los reguladores se enfrentan al reto de abordar la disrupción que provoca el uso de estas nuevas tecnologías, buscando un equilibrio de todos los intereses y bienes jurídicos puestos en común, véase: por un lado, la necesidad de dotar al ordenamiento jurídico con un marco que reduzca los riesgos y proteja a los usuarios finales, permitiendo resolver, entre otras cuestiones, las que suscita la responsabilidad por los daños y perjuicios; y por otro, incentivar el desarrollo y uso de estas tecnologías a través de un marco regulatorio flexible y adaptativo.

De esta manera, el tipo de regulación que se adopte respecto de estas nuevas tecnologías tendrá un efecto directo sobre el desarrollo y uso de estas y, por tanto, en la consecución de los beneficios que tanto las entidades como la propia sociedad puedan obtener de estos. A modo de ejemplo, se puede destacar el Real Decreto-Ley 14/2019, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, a través del cual el legislador optó por prohibir a la Administración pública utilizar sistemas de registro distribuidos *(blockchain)* para entablar relaciones con los interesados.

Este es tan solo un ejemplo, entre otros muchos, que refleja la importancia que la conducta del legislador y el contenido de la regulación tendrá en el desarrollo, oferta y uso de estas nuevas tecnologías en el mercado, pues el citado real decreto implica la imposición de una traba para el desarrollo del *blockchain* en un sector tan relevante para la economía como la contratación pública. Por tanto, es evidente que los operadores del mercado se encuentran así ante más riesgos e

incertidumbres a los que enfrentarse a la hora de utilizar o prestar servicios sobre la base de sistemas o herramientas basadas en nuevas tecnologías.

El regulador debe optar por estrategias y medios que le permitan alcanzar un equilibrio regulatorio que beneficie a todos los intervinientes: evitando la desprotección y falta de garantías de los usuarios finales, que podrían verse afectados por sesgos discriminatorios o prácticas que vulneren su privacidad, y reduciendo la rigidez y carga regulatoria que afecta a los desarrolladores y usuarios de dichas tecnologías, ya que puede traducirse en un alto riesgo de verse afectados por situaciones de responsabilidad que decanten la balanza de la ponderación entre los beneficios que supone la adopción de estas tecnologías y los riesgos inherentes al mismo. Por ello, surgen modelos basados en la autorregulación de los propios operadores, o incluso la corregulación de los operadores con la Administración pública, mediante instrumentos flexibles que no encorseten el progreso y desarrollo de la tecnología con el paso del tiempo.

Este problema-dualidad planteado es típico de los regímenes jurídicos estrictos o con una gran predominancia del *Hard Law* en ellos, cuyo efecto en la sociedad y en la economía es estar a la retaguardia de la innovación. Ante un proceso legislativo caracterizado por ser largo y tedioso, y una tecnología que evoluciona y presenta nuevos retos diariamente, la probabilidad de que el texto jurídico regulador no se corresponda con las características y necesidades de la tecnología es evidentemente alto[9]. En consecuencia, surgen las herramientas de *Soft Law,* tales como directrices, recomendaciones o guías, que son emitidas por reguladores o comités técnicos que permiten a los operadores del mercado cumplir con las obligaciones marcadas por los instrumentos normativos tradicionales, los cuales deben tener un eminente componente "marco", fijando los objetivos de cumplimiento que las organizaciones deben alcanzar. De esta forma resulta más fácil poder actualizar las herramientas regulatorias para adecuarse a la realidad en cada momento, pero siempre dentro del marco imperativo fijado por la ley. Con todo, se consigue un modelo regulatorio tendente a una autorregulación guiada por el legislador[10].

[9] *Vid.* Deloitte, *El futuro de la regulación Principios para regular tecnologías emergentes*, 2019, p. 11.

[10] *Vid*. Gonzalo Domenech, J.J., y Bonmatí Sánchez, J., "La gestión de riesgos y su encaje legal en la regulación de la inteligencia artificial", en Fuentes Soriano, O., *Era digital, sociedad y derecho,* Tirant lo Blanch, Valencia, 2020, pp. 115-125.

Modelo tendente a la regulación basada en la gestión de riesgos

Fuente: elaboración propia.

Con la cuarta revolución industrial, han crecido exponencialmente tanto las ventajas y beneficios que ofrece la implementación y uso de las nuevas tecnologías, como los riesgos y la incertidumbre, que deben ser gestionados por las organizaciones para poder adoptar las estrategias y medidas necesarias con el objetivo de poder hacer frente a estos obstáculos. Es aquí donde se ponen en valor las metodologías y herramientas de gestión de riesgos y que, a lo largo del presente trabajo, se utilizarán para fijar un marco adecuado de gobernanza y gestión sobre la base de metodologías reconocidas internacionalmente, como los estándares ISO y la normativa estatal, europea e internacional, logrando así el reconocimiento de un idioma común entre organizaciones, la proporcionalidad y la adaptabilidad a cualquier contexto organizativo.

3. LAS NUEVAS TECNOLOGÍAS Y EL SECTOR ASEGURADOR: *INSURTECH*

3.1. LA CADENA DE VALOR EN EL *INSURTECH*

Como ya se ha expuesto en el anterior apartado, el impacto de la cuarta revolución industrial alcanza a todos los sectores y operadores del mercado y, entre ellos, al sector asegurador, que actualmente se encuentra inmerso en un complejo proceso de cambio derivado del uso de las herramientas y funcionalidades que ofrecen las nuevas tecnologías.

Es en este marco donde aparece el *insurtech*, término bajo el que se engloba el fenómeno por el cual las empresas que, operando dentro del sector asegurador, utilizan las nuevas tecnologías (p. ej., IA, Big Data, IoT, etc.) con el objetivo de innovar su actividad, optimizar sus procesos y, en definitiva, transformar su actuación en el mercado.

La digitalización del ámbito asegurador está suponiendo un enorme impacto para un sector que, con amplia tradición y fuertemente regulado, se está viendo forzado a renovar su modelo de negocio con la oferta de nuevos productos, nuevos canales de venta y el desarrollo de operadores complementarios, con la finalidad de mantener su nivel de competitividad frente al resto de operadores. Esto se traduce en la creación de nuevos modelos de negocio y productos centrados en la personalización de la oferta, como respuesta a un nuevo tipo de usuario caracterizado por la experiencia, amplia disponibilidad de información e interactivo.

Para ello, los operadores del sector asegurador, desde su alta dirección, están llevando a cabo planes estratégicos para materializar esta oportunidad en sus resultados económicos. Esto supone una transformación de la cadena de valor del negocio asegurador a través de la innovación, lo que permite a las entidades ser

competitivas en un panorama cada vez más cambiante, digitalizando sus procesos de negocio.

Para entender el impacto y el grado de digitalización y disrupción, necesitamos conocer la cadena de valor tradicional del sector asegurador y sus elementos clave[11]:

1. *Gestión de productos:* cuya función primordial consiste en la planificación, previsión y comercialización de un producto en todas sus etapas.

2. *Ventas y distribución:* que engloba los canales de comercialización y medios de promoción para llevar el producto al cliente.

3. *Suscripción de pólizas y la gestión de riesgos:* es el núcleo del sector asegurador, en que las entidades evalúan el riesgo de los potenciales clientes y garantizan el pago en caso de daños o pérdidas.

4. *Gestión de las reclamaciones:* ofrece el servicio consistente en asesorar al cliente, compensarle las pérdidas y cubrir los costes de los litigios.

5. *Servicio de atención al cliente:* es la provisión de un servicio antes, durante y después de la compra con el objetivo de mantener informado al cliente y resolver las cuestiones que pudieran surgirle. Esta fase supone un pilar fundamental en el cumplimiento de objetivos como la retención y/o captación de los clientes.

Con la evolución de las nuevas tecnologías, *estos elementos de la cadena de valor han ido transformándose y redimensionándose para adecuar la actividad aseguradora a la nueva realidad,* impulsada por la digitalización.

[11] *Vid.* PWC, *The Insurance Value Chain*, 2019, pp. 8-14.

Digitalización de la cadena de valor

Diseño y desarrollo de producto	› Seguros *on demand*/personalizables › IoT, telemáticos y robótica permiten las oportunidades del seguro basado en uso a partir del comportamiento del cliente › Aparición de nuevos riesgos (*cyber*) › Seguros colectivos para grupos de redes sociales
Tarificación/ suscripción	› Uso de Big Data/*analitycs* para identificar nuevos patrones de siniestros › Uso de *wearables* y sensores para capturar datos que pueden ser procesados a través de *machine learning* y analítica en tiempo real › Uso de técnicas predictivas para la suscripción basadas en datos de comportamiento › AI/computación cognitiva para valorar riesgos incrementando la automatización
Marketing	› Uso de Big Data/análisis para la segmentación del micromercado y aumentar la personalización del producto › Posicionar el seguro como más centrado en el cliente › Aumentar la frecuencia de interacción con el cliente
Distribución	› Las preferencias de los clientes para la interacción multicanal permiten una experiencia personalizada › Relación digital › Experiencia de compra automatizada y totalmente online › El ecosistema digital transforma el modelo de distribución de las compañias aseguradoras tradicionales › El alcance de la eficiencia para llegar a los clientes podría reducir la cantidad de agentes sustancialmente
Gestión de pólizas y siniestros	› Uso de Big Data/análisis para reducir el fraude y mejorar los procesos de siniestros › Aplicaciones de autoservicio para mejorar la experiencia de posventa del cliente y permitir la interacción del cliente durante el proceso de siniestros › Mejora de la costosa valoración de daños a través de modelos AI › *Text mining* y procesamiento de documentación para la automatización de flujos de trabajo
Cobros y pagos	› Pagos instantáneos y seguros a través de *blockchain*, API bancarias y plataformas de pago › Información rápida y flujo de dinero ágil con menores costos de transacción

Fuente: *NTT Global Report 2019*.

Para desarrollar una efectiva cadena de valor en el ecosistema *insurtech,* una organización debe considerar los siguientes hitos:

1. *Realizar una búsqueda de empresas insurtech.* Mediante este proceso, una organización investiga e identifica empresas emergentes en el panorama *insurtech*. En este punto, se debe listar las empresas *insurtech* que, en ese momento, se enfrenten a los retos existentes y que la operadora de seguros esté interesada en implementarlo en su modelo de negocio. Pueden incluir grandes nombres o nombres incipientes, sin embargo, deberían incluirse los que en un primer momento sean menos relevantes. A su vez, dicha lista debería completarse con aquellos fondos de riesgo centrados en el impulso de empresas tecnológicas.

2. *Organizar las empresas insurtech.* Tras la recopilación de las empresas emergentes, y debido a la gran proliferación de entidades tecnológicas focalizadas en ofrecer nuevas soluciones al sector del seguro, resulta conveniente establecer un método de clasificación que permita agruparlas por afinidades.

3. *Explorar soluciones adecuadas mediante la matriz QFD.* A través de este hito, se agrupan las empresas en grupos de afinidad sobre la base de características medibles e indicadores de desempeño. Por ejemplo, se pueden utilizar indicadores propios del sector del seguro como el tiempo promedio de resolución de reclamaciones o frecuencia de reclamaciones. El resultado se refleja en una matriz donde las necesidades de los clientes se colocan en las filas y los indicadores en las columnas.

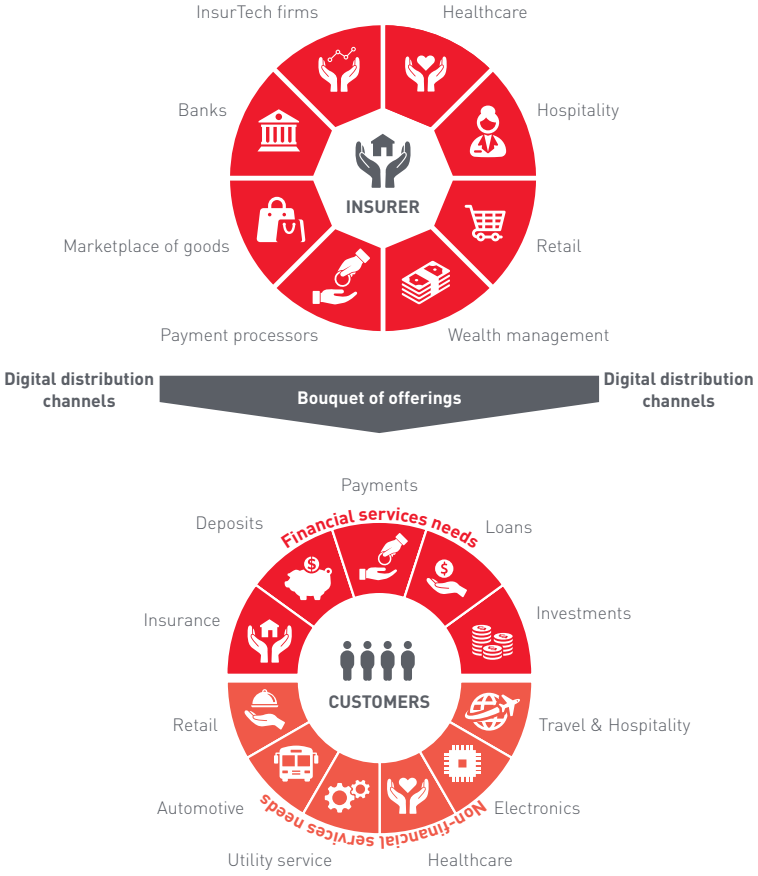
4. *Seleccionar la solución correcta usando la matriz de Pugh.* Finalmente, y tras cubrir los anteriores procesos, la entidad dispondrá de una solución que le proporcionará apoyo a la hora de escoger la solución empresarial más acorde a las necesidades y objetivos propuestos.

Además, y para hacer frente a este nuevo modelo de mercado, surgen, entre los operadores del mercado de los seguros, sinergias y colaboraciones que permiten agrupar productos que cubran tanto las necesidades financieras como no financieras, generando así una mejor percepción por parte de estos en comparación con la mera oferta individual de productos, debido a que la prestación conjunta de

dichos servicios puede personalizarse de tal forma que se adapte a las necesidades individuales de los clientes.

A su vez, la sinergia entre dichos actores, la aceleración de la comercialización de nuevas ofertas y el aumento de los canales de venta (que mejora la eficiencia en la identificación de las necesidades de los clientes), permite ir segmentando granularmente al consumidor, mejorando la creación de soluciones especializadas.

Mercado asegurador del futuro



Fuente: Capgemini Financial Services Analysis, 2019.

El consumidor al que actualmente se enfrentan los operadores del mercado ha cambiado radicalmente en los últimos años, convirtiéndose en un individuo cada vez más informado, con necesidades que varían con mayor frecuencia y donde la agilidad se ha convertido en un factor ampliamente valorado. Esto obliga a las entidades a adoptar las medidas necesarias e implementar las herramientas adecuadas tanto para mantener a los clientes como para captar a los potenciales.

Estos medios y herramientas pasan, en gran parte, por la implantación de soluciones tecnológicas que permitan ofrecer al cliente servicios cada vez más personalizados, agilizar la tramitación de sus peticiones y mejorar sus procedimientos internos. Entre las ventajas que ofrece la implementación de herramientas basadas en las nuevas tecnologías en la cadena de valor de las entidades aseguradoras, pueden destacarse[12]:

a. *Mayor eficiencia en los procesos mediante la automatización y optimización*

   El modelo de negocio de las entidades aseguradoras les brinda la oportunidad de disponer de grandes cantidades de datos e información que les permite agilizar y optimizar sus procesos.

   Mediante el análisis de datos se pueden construir modelos predictivos que permitan a las entidades aseguradoras automatizar procedimientos repetitivos y diarios, mejoran así el tiempo de respuesta (atendiendo así la agilidad que solicitan los nuevos consumidores) y permitiendo centrar la actividad humana en tareas que generen mayor valor y de carácter diferenciador.

b. *Cercanía en la relación con el cliente*

   La actual estructura de la oferta de los productos se caracteriza por la presencia de varios operadores: agentes de seguros, corredores y las propias aseguradoras, entre otros.

[12] *Vid*. AEFI. *Libro Blanco de insurtech*, Madrid, 2019, p. 15.

La digitalización mediante el *insurtech* proporciona una reducción de la longitud del canal de distribución, permitiendo una mayor cercanía con el consumidor y unos precios más competitivos al reducir el número de agentes intervinientes.

Por tanto, y mediante las nuevas tecnologías, el cliente dispone de la posibilidad de entablar una relación más directa respecto a las gestiones comunes que estos pueden realizar durante todo el ciclo de vida del seguro: contratación, modificación, renovación, extinción, etc.

c. *Prevención del fraude*

Debido a la actividad desempeñada por las empresas del sector asegurador, el riesgo de ser víctima de un fraude siempre es alto, por lo que uno de los objetivos de toda aseguradora es reducir este riesgo y las pérdidas asociadas.

Las nuevas tecnologías aplicadas al sector asegurador tienden a crear nuevos mecanismos y soluciones para atajar este problema. Por ejemplo, el uso de sensores de detección sobre vehículos conectados ya permite medir las características de la conducción del usuario.

d. *Análisis de suscripción de riesgo*

En la prestación de sus servicios, las aseguradoras también se enfrentan a la incertidumbre de los riesgos que aseguran, tanto desde una perspectiva de la probabilidad como de su cuantificación. Por tanto, las aseguradoras están interesadas en adquirir y utilizar datos que puedan ayudar a evaluar la probabilidad y, en consecuencia, mitigar su exposición a los riesgos.

Un ejemplo de ello es la obtención de datos sobre la actividad física de los clientes, lo que permite a la aseguradora disponer de una nueva fuente válida para la evaluación de riesgos del asegurado, en lugar de, sencillamente, la confianza en los datos declarados por el mismo.

e. *Procesos de pricing*

La disponibilidad y análisis de grandes cantidades de datos ayuda a las aseguradoras a disponer de una visión más concreta y acertada de la realidad de los clientes, su contexto y el resto de las entidades que participan en el mercado.

Este conocimiento permite la adaptación de decisiones más informadas, lo que, en el ámbito de los precios, permite a las entidades adecuarlos a las circunstancias concretas, reduciendo el riesgo asumido con los clientes y mejorando su posición frente al resto de operadores.

Llegados a este punto, cabe preguntarse las razones por las que las *insurtech* aportan el valor diferenciador a la cadena de valor del modelo asegurador tradicional. En este sentido, deben destacarse, al menos, las siguientes razones[13]: 1) lideran la digitalización; 2) establecen el foco en el consumidor y su experiencia, y 3) se construyen sobre una cultura ágil, de adaptación.

En primer lugar, son líderes en *aprovechar la tecnología más avanzada*. La innovación tecnológica es el núcleo de cualquier solución de las *insurtech*. Esto las convierte en pioneras en el uso de las nuevas tecnologías y su aplicación a soluciones empresariales, diseñando y transformando los productos, para posteriormente ofrecerlos a los líderes del mercado asegurador creando nuevas necesidades. Al tener un gran entendimiento de la tecnología y sus aplicaciones, no sorprende que las *insurtech* sean las primeras en encontrar sus aplicaciones en el sector asegurador, antes incluso que las grandes entidades aseguradoras.

Por otro lado, las mejoras que pretenden introducir están enfocadas *en mejorar la experiencia y prestación para el usuario.* Las *insurtech* se centran en mejorar la experiencia del usuario en todas las fases como, por ejemplo, durante la negociación y firma del contrato, brindan un apoyo durante la evaluación de riesgos o ajustan las pérdidas mediante una evaluación de pérdidas. De esta forma, se simplifica

[13] *Vid.* Vanderlinden, S. L. B *et al., The Insurtech Book: The Insurance Technology Handbook for Investors, Entrepreneurs and FinTech Visionaries,* Wiley, Sussex, 2018, p. 7.

la experiencia de los usuarios reduciendo los elementos formales de la contratación y mejorando la claridad de las condiciones y su accesibilidad.

Finalmente, y en consecuencia de lo expuesto previamente, las *insurtech se erigen sobre una cultura ágil e información, mediante el aprovechamiento avanzado de la analítica de datos para la toma decisiones.* La cultura de estas empresas emergentes se encuentra marcada por el uso de herramientas analíticas que les permitan la obtención de *insights* y así adoptar un modelo de gestión basado en la toma de decisiones informadas.

3.2. LOS INTERVINIENTES EN EL SECTOR *INSURTECH*

La materialización de estos objetivos, como se ha citado previamente, deriva de un cambio profundo en la cadena de valor, incorporándose nuevos intervinientes y creando nuevos servicios mediante la explotación de nuevas modalidades de negocio. Entre los nuevos actores, y por su importancia dentro de la digitalización del sector asegurador, pueden destacarse: distribuidores de los productos, proveedores de infraestructuras y servicios posventa.

3.2.1. Distribución

La *distribución* de los productos ha sido, dentro de la cadena de valor, uno de los procesos en el que más se ha avanzado respecto a su digitalización. Las acciones se han concentrado, mediante el uso de plataformas digitales, en el desarrollo y despliegue de aplicaciones móviles que permiten ofrecer el producto y los servicios directamente al cliente. Las empresas dedicadas a la distribución dentro del campo del *insurtech* se agrupan en las siguientes categorías:

- *Compradores y marketplaces:* como los clásicos comparadores de seguros, que consisten en portales *online* o aplicaciones móviles donde se permite a los consumidores comparar un mismo producto entre varias aseguradoras. Dentro de este propio servicio, se pueden subespecializar en la comparación de productos de un solo ramo o multirramos.

- *Recomendación y administración de seguros:* estos prestadores de servicios suponen una evolución en la oferta respecto de los comparadores expuestos en el apartado anterior. La novedad que introducen estos nuevos actores radica en el asesoramiento al consumidor durante todo el proceso de contratación. Un ejemplo son los corredores digitales; aquellos que prestan sus servicios de asesoramiento a través de plataformas digitales.

Estos últimos casos suponen reconversiones de integrantes clásicos del sector de la distribución de seguros, a través de la digitalización de una parte de la cadena de valor, que recientemente han tenido su inclusión en el nuevo régimen legal establecido en el artículo 134 del Real Decreto-ley 3/2020, de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la Unión Europea en el ámbito de la contratación pública en determinados sectores; de seguros privados; de planes y fondos de pensiones; del ámbito tributario y de litigios fiscales, al contemplar la posibilidad de que los mediadores utilicen páginas web donde se comparen productos de diferentes oferentes; y que cuya inclusión permite proteger al consumidor que obtiene un producto mediante esta vía[14].

Por otro lado, encontramos entidades que digitalizan completamente su cadena de valor, desde la oferta de información, hasta la gestión de reclamaciones, pasando por la contratación y gestión de cualquier proceso en el que interviene un cliente. A estas nuevas entidades se las denomina *entidades aseguradoras digitales* o "neoaseguradoras"[15].

3.2.2. Proveedores de infraestructura

De acuerdo con la digitalización de la cadena de valor y la evolución de los intervinientes en el mercado, deben destacarse una serie de intervinientes que, dentro de la rama vertical del mercado del seguro, prestan servicios de soporte a las *insurtech.*

[14] *Vid*. Almarcha Jaime, J., "¿Qué hay de nuevo para los consumidores en el ámbito de los seguros? Estado de la tramitación de la futura ley de distribución de seguros y reaseguros", *Centro de Estudios de Consumo,* S/N, 2017, p. 5.

[15] *Vid*. AEFI, *Libro Blanco de insurtech*, Madrid, 2019, p. 26.

Debido a la heterogeneidad de estos prestadores de soporte, se pueden clasificar en las siguientes categorías:

- *Entidades de credit scoring*

El uso del *credit scoring* es un sistema de calificación de créditos que, mediante el análisis de datos, permite automatizar la toma de decisiones en lo referente a la concesión, o no, de una determinada operación de riesgo.

Sus orígenes se remontan a los años sesenta en Estados Unidos, desarrollándose, principalmente, en diferentes ámbitos del sector financiero. Su consolidación se produjo en la década de los noventa, donde entidades del sector hipotecario empezaron a desarrollar sistemas de IA mentorizadas16.

En la actualidad, y mediante la extensión del concepto Big Data y la explotación de los datos libremente accesibles, las *insurtech* tienen los medios y la capacidad para obtener información valiosa de cara a poder implementar y mejorar soluciones *credit scoring*.

- *Proveedores de servicios de confianza en materia de identificación electrónica*

Esta categoría de prestadores de servicios deriva del Reglamento (UE) 910/2014 sobre identificación electrónica. Este reglamento tiene como objetivo armonizar los criterios que deben reunir los prestadores de servicios de identificación electrónica para asegurar un nivel mínimo de confianza.

La identificación digital tiene como base garantizar la confianza y la seguridad en las transacciones electrónicas. Por ejemplo, sobre la base de la Directiva (UE) 2018/843, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, se habilita el uso de medios de identificación digital para poder cumplir las obligaciones de identificación de las personas físicas y jurídicas, y

[16] *Vid*. Makuch, W., "Scoring Applications", en Mays. E. (ed.), *Handbook of Credit Scoring*, Glenlake, Chicago, 2001, p. 10.

en concreto, en la casuística específica para el sector del seguro (artículo 5 del Real Decreto 304/2014).

- *Proveedores de software*

Por último, existe otro componente central en la estructura de los nuevos actores del mercado del seguro: los proveedores que prestan la tecnología necesaria para implantar la digitalización en la estrategia de la aseguradora. Algunos de estos servicios son:

  – Gestión inteligente de contratos.

  – Promoción de la comercialización y las ventas cruzadas.

  – Servicios de consultoría específicos para el sector.

  – Servicios de contabilidad.

  – Servicios de automatización, estandarización, interconexión, comunicación y confidencialidad.

  – Valoración y gestión de siniestros.

  – Cálculo de riesgos.

3.2.3. Servicios de posventa

Por último, existen solo entidades que se dedican a potenciar los últimos elementos de la cadena de valor como es el servicio *posventa.* Este servicio incluye desde la tramitación de siniestros hasta la gestión de consultas e información a los consumidores. Se destacan las siguientes aplicaciones:

a. *Gestión de siniestros y reclamaciones:* el objetivo que se persigue es el de mejorar la eficiencia en la gestión de las reclamaciones recibidas y la prevención

del fraude. Como ejemplo se puede destacar el uso de *blockchain* para acreditar la relación fáctica de un siniestro.

b. *Botinsurance:* consiste en el uso de *chatbots,* basados en IA, para gestionar cualquier relación que el usuario final pretenda emprender ante la aseguradora, reduciendo así los costes de personal y el tiempo medio que se emplea para su resolución.

3.3. IMPLICACIONES REGULATORIAS EN EL *INSURTECH*

Como ya se ha mencionado al inicio de este apartado, las entidades aseguradoras se mueven en un entorno caracterizado por la existencia de una fuerte regulación tendente a la protección de los consumidores y un gran entorno normativo disperso, pero centralizado.

Sin embargo, existe una potente corriente internacional centrada en buscar un consenso global en una regulación adecuada para las *insurtech*[17]. Como primer ejemplo, por parte de la OCDE, requiere especial mención el informe *Technology and innovation in the insurance sector,* donde se abordan las dificultades que algunas *insurtech* deben afrontar tras obtener la autorización para operar en el sector como, por ejemplo, el aseguramiento de un porcentaje mínimo de capital social. Por ello, la OCDE plantea la existencia de plataformas experimentales que permitan a estas entidades desarrollarse en un entorno más controlado y abierto, conocido como *sandbox* regulatorio[18].

El fenómeno *sandbox* consiste en la creación de un espacio de desarrollo de nuevas soluciones tecnológicas en cualquier sector, en este caso el asegurador, para experimentar en un entorno regulatorio diferente al común. En este sentido, se aprobó la Ley 7/2020, de 13 de noviembre, para la transformación digital del sistema financiero, que regula un entorno controlado de pruebas que permita llevar

[17] *Vid*. Chatzara, V., "FinTech, InsurTech, and the Regulators", en Marano, P. y Noussia, K. (eds.), *InsurTech: A Legal and Regulatory View,* Springer, Cham, 2019, p. 7.

[18] *Vid*. OCDE, *Technology and innovation in the insurance sector,* 2017, p. 29.

a la práctica proyectos tecnológicos de innovación en el sistema financiero con pleno acomodo en el marco legal y supervisor.

Por otro lado, debemos destacar las nuevas obligaciones impuestas por la Directiva 2016/97, de 20 de enero de 2016, sobre la distribución de seguros, y traspuestas por el Real Decreto-ley 3/2020, que afectan directamente al desarrollo de nuevos productos y a la proliferación de nuevas *insurtech.* En concreto, destacamos el artículo 185 de esta última norma, que viene a trasponer la misma obligación contenida en el artículo 25 de la directiva.

Ambos artículos dictaminan la necesidad de que la entidad aseguradora debe establecer una evaluación previa a su distribución a los clientes, teniendo en cuenta las características de dicho producto y el mercado al que va dirigido. Esta evaluación, como se indica en el apartado uno del artículo, debe tener un enfoque al riesgo para el mercado al cual va dirigido. Puesto que este artículo refleja la idea principal del presente trabajo, como es la gestión del riesgo de las nuevas tecnologías, se analizará con mayor profundidad en el cuarto apartado.

Sin perjuicio de lo expuesto previamente, el impacto regulatorio en la actividad aseguradora no deriva únicamente del régimen jurídico específico del sector asegurador, ya que los operadores de este mercado se encuentran sometidos a normativa de carácter general que vinculan a cualquier actividad, incluida la llevada a cabo por el sector asegurador como, por ejemplo, la legislación sobre protección de datos y defensa de los consumidores.

En el proceso de digitalización del mercado hay un mínimo común denominador a todos los agentes que participan en él: los datos. Independientemente del tamaño de la empresa o el sector en el que desarrolle su actividad, los datos son la "gasolina" que permite implementar la mayor parte de las nuevas soluciones tecnológicas y, por tanto, la adaptación de los operadores a la cuarta revolución industrial. Los datos son una fuente valiosa de información cuyo uso debe ser apropiado y ajustado a lo establecido por la normativa vigente al momento de su uso.

Actualmente, y tras la entrada en vigor del Reglamento 2016/679 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 y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales, el acceso y la transmisión de datos personales se ha visto especialmente regulado por una normativa que se construye sobre la piedra angular de la privacidad, cuyo objetivo principal es garantizar el respeto de los derechos de los ciudadanos.

Del uso de los datos personales, se destaca la cuestión de los *datos abiertos.* El concepto de los datos abiertos deriva de la prestación de una licencia libre de uso, concepto utilizado en la Administración pública[19], pero este no podría utilizarse con los datos personales debido a la protección que genera la legislación; si bien se pueden buscar bases de legitimación como el interés legítimo y la manifestación pública de los datos realizada por el usuario para que pueda considerarse lícito su uso.

Introduciéndonos en el ámbito organizativo de las entidades aseguradoras, debemos destacar las restricciones en materia de externalización de servicios de seguro y reaseguro derivado del Reglamento (UE) 2015/35 de la Comisión, de 10 de octubre de 2014, por el que se completa la Directiva 2009/138/CE sobre el acceso a la actividad de seguro y de reaseguro y su ejercicio, el cual exige aplicar una política y requisitos de subcontratación centrados en la debida diligencia hacia dicho proveedor. En caso de que el servicio externalizado se considere crítico, los requisitos aumentan exponencialmente. El término crítico no deja de ser un concepto indeterminado y subjetivo, el cual requiere por parte de la entidad aseguradora determinar los criterios que permiten a un determinado servicio considerarse crítico. Un medio para ello consiste en la adopción de un análisis de impacto de negocio, consistente en analizar sobre la base de la indisponibilidad del servicio qué efectos tendría en la organización que un servicio dejara de prestarse durante un determinado tiempo, estableciendo el límite temporal máximo que la organización estuviera dispuesta a asumir.

En conclusión, el *insurtech*, concepto que se podría definir como la integración del uso de las nuevas tecnologías en el sector del seguro, con el objetivo principal de

[19] La definición no es única, dividiéndose las definiciones entre las realizadas por la legislación o las organizaciones defensoras de la información abierta. *Vid.* Almansa Morales, A., *Transparencia y datos abiertos en la Administración p*ública*,* INAP, Madrid, 2017, p. 43.

dotar de mayor eficiencia la prestación de los servicios, adaptándose a las necesidades de los consumidores y aumentando su capacidad competitiva, supone para las aseguradoras el problema de la moneda con dos caras: por un lado, son una fuente de innovación y oportunidades y, por otro lado, se erigen sobre la incertidumbre y riesgo del impacto que su integración en el modelo de negocio y uso puede generar.

3.4. TECNOLOGÍAS APLICABLES EN EL SECTOR ASEGURADOR

A la hora de hablar del uso de nuevas tecnologías y digitalización del sector del seguro, resulta conveniente acotar, en la medida de lo posible, el concepto y características de aquellas que, debido a su progresivo desarrollo e implementación, son las que mayor impacto generan en el sector asegurador debido a su relación directa con los datos y a la conexidad entre ellas: el Big Data, el IoT y la IA.

Debido a la multitud de referencias que se hará a las mismas y la importancia que tiene conocer sus características para poder comprender los beneficios que ofrecen y los riesgos que implican, a continuación, se expondrá un breve resumen de cada una de ellas.

3.4.1. Big Data

Bajo el término *Big Data* actualmente se engloban las prácticas encaminadas a la obtención, almacenamiento y tratamiento de un gran volumen de datos a gran velocidad. De esta definición se extraen las tres características principales del Big Data: la velocidad, el volumen y la variedad.

Con el avance de esta tecnología se han ido estableciendo nuevas características que complementan a las existentes, aportando singularidades al concepto[20]. El Big Data, a su vez, se basa en dos conceptos esenciales al margen de la calidad de los datos, como son la *fuente* y *el procesamiento de datos.*

[20] *Vid*. Buyya, R., *Big Data: Principles and Paradigms,* Morgan Kaufmann, 2016, p. 14.

Por un lado, es capital en el uso del Big Data observar el diferente origen de los datos que van a ser objeto de procesamiento. Cualquier resultado o decisión final mediante el uso del Big Data deriva de un contraste masivo de datos que son complementados entre sí para alcanzar un resultado lo más exacto posible a aquello que se pretende buscar. Existen varias fuentes de las cuales se pueden obtener los datos[21]:

1. *Web y social media.* Cualquier contenido almacenado en una página web, incluyéndose también los datos generados por las interacciones de los usuarios con las páginas web (p. ej., *likes,* recomendaciones, comentarios, etc.).

2. *Datos generados por máquinas.* Son aquellos datos generados directamente por la conexión entre diferentes dispositivos tecnológicos, sin que exista, *a priori,* intervención alguna de personas como, por ejemplo, los datos generados mediante sensores conectados entre sí por una red inalámbrica.

3. *Grandes transacciones de datos.* Este grupo recoge los datos generados sobre registros, cuyo significado puede variar enormemente.

4. *Biometría.* La información biométrica incluye huellas dactilares, reconocimiento de voz, escáneres de retina e iris, reconocimiento facial y genético. Los avances tecnológicos han aumentado enormemente la posibilidad de disponer de datos biométricos. Los datos biométricos están cada vez más disponibles en el ámbito comercial donde se puede mezclar con otros tipos de datos como los medios de comunicación social.

5. *Datos generados por humanos.* Los seres humanos generan grandes cantidades de datos a través de su interacción con el mundo físico y digital, tales como grabaciones de voz, correos electrónicos, documentos en papel, encuestas y registros médicos electrónicos, entre otros.

Por otro lado, todos estos datos deben procesarse para obtener los *outcomes* requeridos. En este sentido, para su procesamiento se requiere tanto elementos de

[21] *Vid.* Soares, S., *Big Data Governance. An Emerging Imperative*, MC Press, Boise (ID), 2012, pp. 7-8.

software como de hardware con alta capacidad de computación. Respecto al primer elemento, los datos son gestionados mediante sistemas implementados sobre hardware para almacenar, procesar y analizar grandes volúmenes de datos. Un ejemplo de ello sería Hadoop, sistema de código abierto que recopila las funciones referidas previamente.

Respecto al hardware, para el desarrollo de una estrategia empresarial basada en Big Data se debe tener en cuenta que, dado que serán objeto de procesamiento una gran cantidad de datos, las organizaciones deberán tener máquinas que puedan ser capaces de almacenar y soportar los procesos de cómputos ejecutados. Como solución, este servicio puede ser externalizado a proveedores de servicios de plataforma *cloud* (IaaS, PaaS y SaaS).

3.4.2. *Internet of Things* (IoT)

Internet of Things (IoT), o internet de las cosas, es el término bajo el cual se refiere al fenómeno digital de interconexión entre dispositivos y objetos a través de la red, que permite que nuestro mundo físico se convierta en un entorno cada vez más conectado y digitalizado.

El entorno IoT está permitiendo una generación masiva de datos a través de la interconexión entre personas (P2P), maquinas (M2M) y personas con máquinas (P2M). Pero, para comprender el alcance y contenido del IoT, es importante conocer previamente cuál ha sido la evolución de las redes e internet.

En el principio de todo y, al igual que muchas otras tecnologías, la creación de redes interconectadas nacen con un marcado carácter de uso gubernamental e investigador, concretamente, las primeras redes fueron creadas y desarrolladas con el objetivo de poder compartir información, es decir, como un medio en el cual almacenar contenido y poder compartirlo. De esta forma nace la que podríamos denominar la primera etapa de internet, conocida como el internet del contenido o *internet of content*.

Posteriormente, y con el incremento de las redes y su conectividad, entre otras cuestiones, internet comienza a ser el lugar donde los particulares, las empresas

y los profesionales intercambian la oferta y la demanda, naciendo así el denominado *e-commerce (internet of services),* y, finalmente, el lugar en el que las personas pudieran relacionarse con otras personas *(internet of people)* a través de aplicaciones para compartir contenido multimedia, como las redes sociales.

Es en este momento en el que aparece lo que hoy conocemos como IoT, es decir, el siguiente paso en la evolución de internet. Un ejemplo lo encontramos en algo tan cotidiano como la conducción, donde mantenemos interconectados nuestros dispositivos *smartphones* o tabletas con el propio vehículo y que, por ejemplo, mediante comandos de voz dirigidos al vehículo podemos interactuar con las aplicaciones y acceder al contenido de otros dispositivos.

Entre otros beneficios, como la mejora de la conectividad, el IoT permite la generación de cantidades ingentes de datos que, a través de procedimientos de analítica e interpretación de datos, permite extraer los tan valorados *insights*.

El sector asegurador, como muchos otros, también aprovecha los beneficios y ventajas que ofrece la interconectividad entre dispositivos, con el objetivo de modernizar y mejorar su intervención en el mercado, las relaciones con sus clientes y el diseño de sus productos. Esta afirmación adquiere aún mayor fuerza si se tiene en cuenta que para el año 2025 la población mundial contará con más de 50 mil millones de dispositivos conectados a la red[22] y que, en consecuencia, el consumidor medio evolucionará hacia un usuario con conectividad absoluta.

En el marco del seguro, el uso del IoT por parte de las aseguradoras se estima que puede repercutir una gran variedad de beneficios, como: 1) la reducción de los costes, al incrementar la optimización de sus recursos; 2) la mejora de la capacidad para reconocer los fraudes; 3) el incremento de los ingresos, al permitir una adecuada revisión de las primas, y 4) el desarrollo de nuevos servicios y modelos de negocio.

[22] *Vid.* McKinsey & Company, *Digital ecosystems for insurers: Opportunities through the Internet of Things.* Informe ejecutivo, 2019. Recuperado de: https://www.mckinsey.com/industries/financial-services/our-insights/digital-ecosystems-for-insurers-opportunities-through-the-internet-of-things (fecha de consulta: 21-09-2021).

Actualmente, pueden destacarse cuatro ecosistemas digitales en los que las aseguradoras pueden explotar las oportunidades que ofrece el IoT: los automóviles conectados, las viviendas inteligentes, la salud y las líneas comerciales.

- *Automóviles conectados.* Cada vez son más los vehículos que están equipados con sensores que les permiten captar el comportamiento del conductor durante la conducción y el entorno en el que se mueve. De esta forma, la aseguradora puede utilizar los datos obtenidos para adecuar cada póliza de seguro sobre datos reales, dejando en un segundo lugar criterios como la edad o la experiencia del conductor[23].

- *Salud de los asegurados.* Mediante el uso de aplicaciones instaladas en los dispositivos portátiles de los asegurados (p. ej., *smartphones, smartwatch,* etc.), se puede monitorizar la actividad física de los mismos, disponiendo así de información que permita a la aseguradora analizar los verdaderos riesgos de cada asegurador y, en consecuencia, adaptar las condiciones y coberturas.

- *Viviendas inteligentes.* Aunque la madurez de desarrollo y disponibilidad de una vivienda inteligente no sea tan alta como los dos anteriores ecosistemas, es cuestión de tiempo que cada vez sean más los inmuebles que dispongan de sistemas que automaticen ciertas funciones y permitan disponer de información actualizada sobre el mantenimiento de la vivienda (p. ej., consumo energético), su seguridad (p. ej., vigilancia mediante sensores) y las comodidades (p. ej., sistema de calefacción automatizado en función de la temperatura del inmueble mediante sensores instalados).

- *Líneas comerciales.* La creación y mantenimiento de ecosistemas comerciales con otros operadores del mercado que puedan aportar a la cadena de valor, colaborando con las aseguradoras en la gestión de redes de proveedores tecnológicos, innovación de productos o mejoras en los canales de distribución.

[23] *Vid.* Muñoz Paredes, M. L. *Algoritmos y seguro: la fijación de la prima atendiendo a factores ajenos al riesgo,* Almacén de Derecho, Madrid, 2020.

El desarrollo y uso de cada uno de los ecosistemas expuestos depende, en gran medida, de la madurez de la tecnología y del mercado que, a su vez, se encuentra influenciado por el entorno regulatorio, los actores que intervienen y la propia dinámica del mercado. Actualmente, aquellos ecosistemas que cuentan con un mayor desarrollo son los relacionados con los automóviles y la salud.

Independientemente del grado de desarrollo de cada una de estas aplicaciones, todas ellas reportan beneficios a las aseguradoras como, por ejemplo: 1) reducción del riesgo de cada operación de aseguramiento, ya que, al tener un mayor conocimiento sobre el asegurado y su entorno, la aseguradora puede adoptar las medidas que considere oportunas como respuesta y 2) ofrecer un trato más personalizado al asegurado/tomador, adaptando el precio de la prima o la cobertura durante la vigencia del contrato de seguro en función de las características de cada caso concreto.

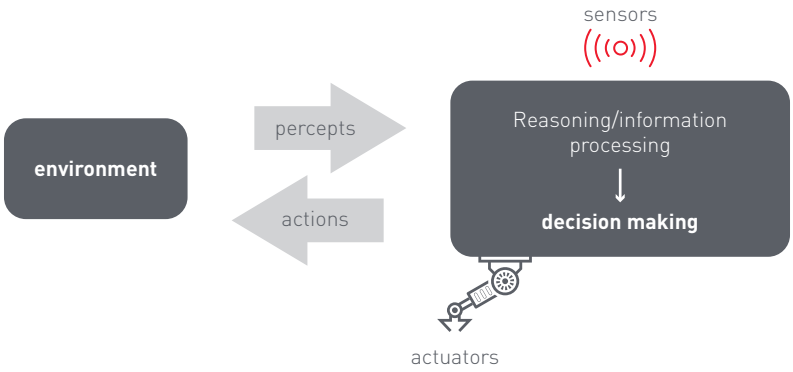
A pesar de no contar, a fecha de la presente investigación, con una regulación específica del IoT y la dificultad que entraña regular una tecnología de marcado carácter transversal, debido a la multitud de funcionalidades y situaciones en las que puede desplegarse, sí que puede destacarse, como punto de partida, el impacto que el uso de esta tiene para la privacidad y la seguridad de la información, además de la normativa sectorial que pudiera ser de aplicación en cada caso.

3.4.3. Inteligencia artificial (IA)

Aunque actualmente no existe un consenso único sobre una definición de la IA, debido a sus características, aplicaciones y su constante evolución, el Grupo de Expertos de Alto Nivel de la Comisión Europea sobre Financiamiento Sostenible (HLEG, por sus siglas en inglés) la ha definido como aquellos sistemas de software (y en algunos casos también de hardware) diseñados por seres humanos que, dado un objetivo complejo, actúan en la dimensión física o digital mediante la percepción de su entorno a través de la obtención de datos, la interpretación de los datos estructurados o no estructurados que recopilan, el razonamiento sobre el conocimiento o el procesamiento de la información derivados de esos datos, y

decidiendo la acción o acciones óptimas que deben llevar a cabo para lograr el objetivo establecido[24].

Descripción esquemática de un sistema de IA



Fuente: HLEG, *A definition of AI: Main Capabilities and Disciplines, 2019*.

La IA es una disciplina científica que incluye varios enfoques y técnicas, como el aprendizaje automático (del que el aprendizaje profundo y el aprendizaje por refuerzo constituyen algunos ejemplos), el razonamiento automático (que incluye la planificación, programación, representación y razonamiento de conocimientos, búsqueda y optimización) y la robótica (que incluye el control, la percepción, sensores y accionadores, así como la integración de todas las demás técnicas en sistemas ciberfísicos).

Para una aproximación menos técnica a la IA que permita concretar, aún más si cabe, el concepto que subyace detrás del citado término, se puede definir como la rama de la informática y las ciencias de la computación que estudia el desarrollo y creación de máquinas con capacidad para emular el comportamiento inteligente humano. La IA es, realmente, un conjunto de tecnologías y procesos:

- Por un lado, la IA refiere a un grupo de *tecnologías* que permiten a un sistema o agente relacionarse con el entorno. Mediante la obtención de datos, ya sea

[24] *Vid.* High-Level Expert Group on Artificial Intelligence, *A definition of AI: Main Capabilities and Disciplines.* Informe ejecutivo, 2019, p. 6.

introducidos de forma manual u obtenidos a través de sensores, y su procesamiento a través de algoritmos, le permite cumplir con las funciones encomendadas. A modo de ejemplo pueden destacarse el *machine learning, image recognition, natural lenguage processing* y *creative computation,* entre otros.

- Por otro lado, la IA también refiere al *procedimiento* seguido para el tratamiento de los datos obtenidos, es decir, la concatenación de actos que se llevan a cabo para alcanzar el objetivo fijado y entre las que destacan: la recopilación de datos, su análisis, valoración, uso para la toma de una decisión (intervenida o no por el ser humano) y, en algunos casos, aprendizaje.

A pesar de que el interés por la creación de seres con capacidad para simular la inteligencia humana tiene sus orígenes en la Grecia clásica, no es hasta 1956, en la Conferencia de Dartmouth, cuando se acuña el término "inteligencia artificial", sin perjuicio de que algunos años antes, personalidades como Alan Turing, Herbert Simon o Allen Newell ya hubieran dado los primeros grandes pasos en este campo.

Pero ha sido, sin duda, con la llegada del ML *(machine learning)* y el incremento de la capacidad de almacenamiento y análisis de datos, que el campo de la IA ha comenzado a explotar sus verdaderas capacidades, permitiendo abandonar el antiguo paradigma basado en la introducción de reglas y patrones, previamente descubiertos por los investigadores o programadores, y se abre la posibilidad a que sean los propios sistemas/programas, a través del uso de algoritmos y grandes cantidades de datos, los que puedan identificar patrones o relaciones que permitan cumplir el objetivo previamente fijado (p. ej., predicción, conceptualización, toma de decisiones, etc.) mediante el aprendizaje.

Por tanto, y mediante el uso de algoritmos, se pueden analizar grandes cantidades de información y extraer patrones o información que posteriormente puedan ser utilizados para la toma de decisiones, entre otras finalidades.

Aunque actualmente existen varios modelos de aprendizaje, son tres los modelos más destacados por su amplio uso en el campo de la IA: el aprendizaje supervisado *(supervised learning),* el aprendizaje no supervisado *(unsupervised learning)* y el aprendizaje reforzado *(reinforcement learning).*

- *Aprendizaje supervisado:* esta modalidad de aprendizaje se fundamenta sobre la base del uso de datos etiquetados *(labeled data),* es decir, datos que disponen de una serie de características prefijadas (p. ej., la foto de un perro se etiqueta como "perro"). El histórico de datos de los que se disponen se dividen en dos grupos: datos de entrenamientos *(training set)* y datos de comprobación *(test set).*

  Por un lado, y respecto de la fase de entrenamiento, se introducen los datos de entrenamiento y, dado que están etiquetados, se indica la respuesta correcta al sistema (p. ej., tras introducir la foto de un perro, se indica al sistema que es un "perro"). De esta forma, y tras el análisis de una gran cantidad de datos (en este caso, fotos de perros), el sistema obtendrá cuáles son los patrones que permiten identificar a un animal como un perro (p. ej., pelaje, cola, orejas, forma, patas, etc.).

  Por otro lado, y tras la finalización del entrenamiento, se procede a la validación del modelo, es decir, el uso del grupo de datos que se han reservado *(test set).* Esos datos se introducen en el sistema entrenado de tal forma que permite comprobar si efectivamente el sistema ha aprendido a identificar, en este caso, fotos de perros.

  En definitiva, y teniendo en cuenta el paradigma del aprendizaje supervisado, este tipo de aprendizaje es utilizado cuando: 1) se disponga de datos etiquetados suficientes para garantizar un aprendizaje óptimo y 2) la finalidad/objetivo perseguido sea la de clasificar o predecir.

- *Aprendizaje no supervisado:* a diferencia de lo referido para el aprendizaje supervisado, en este caso no se disponen de datos etiquetados, por lo que el aprendizaje consiste en la introducción de los datos de los que se disponga y, con un objetivo prefijado, descubrir la estructura de los datos, es decir, la existencia de categorías o patrones entre ellos.

  Siguiendo con el ejemplo anterior, supongamos que tenemos miles de fotos de animales, pero no están etiquetadas, es decir, no se les ha asignado una categoría (p. ej., perros, gatos, pájaros, serpientes, ranas, peces, etc.). Mediante

un modelo de aprendizaje no supervisado, el sistema podría identificar similitudes entre ellos y emitir, como *output,* un agrupamiento entre las fotos que disponen de patrones similares (p. ej., aves, reptiles, mamíferos, etc.).

Teniendo en cuenta el paradigma del aprendizaje no supervisado, este tipo de aprendizaje es utilizado cuando: 1) no se dispone de datos etiquetados o el volumen y variedad necesaria y 2) la finalidad/objetivo perseguido es el de establecer agrupaciones o correlaciones entre datos.

- *Aprendizaje reforzado:* este paradigma de aprendizaje se construye sobre la base de prueba-error, es decir, a través de un sistema de premios-penalizaciones se puede orientar el aprendizaje en la dirección que se prefiera.

  El aprendizaje reforzado no es idéntico al aprendizaje supervisado, pues no se basa estrictamente en un conjunto de datos etiquetados, sino en la monitorización de la respuesta a las acciones tomadas, pero tampoco es idéntico al sistema de aprendizaje no supervisado ya que, cuando se modela el sistema, sí se sabe cuál es el objetivo esperado.

  Dentro de este paradigma se pueden destacar las redes generativas adversarias (GAN, por sus siglas en inglés) que permiten el entrenamiento de sistemas de IA sobre la base del ensayo-error. Uno de los sistemas (red generativa) genera un *input* (p. ej., la foto de una persona) y otro sistema (red discriminadora) debe valorarlo y resolver la cuestión que le haya sido planteada (p. ej., la persona de la foto es real o no). De esta forma, y mediante un sistema basado en el ensayo-error, ambas redes perfeccionan las funciones encomendadas: generar retratos de personas cada vez más realísticos (red generativa) y detectar los retratos de personas falsas (red discriminadora).

Para escoger entre los distintos sistemas de aprendizaje, se deben tener en cuenta los siguientes factores: 1) los datos disponibles y 2) el objetivo perseguido. Respecto a este último criterio, cabe destacar que los sistemas de IA pueden proporcionar, como regla general, tres tipos de resultados[25]: predicciones (p. ej., probabilidad de

[25] *Vid.* ICO y Alan Turing Institute, *Project explAIn Interim report*, informe ejecutivo, 2019, p. 7.

impago de un préstamo por una persona concreta), recomendaciones (p. ej., ofrecer un producto sobre la base de los datos del cliente) y clasificaciones (p. ej., distribuir los correos electrónicos entre correo no deseado o *spam* y correo deseado).

A pesar de que lo expuesto previamente pueda generar una sensación de capacidades ilimitadas por parte de la IA, actualmente los sistemas de IA desarrollados son aquellos que disponen de capacidad para resolver tareas concretas y alcanzar los objetivos para los que han sido entrenados, es decir, lo que comúnmente es referido como IA de propósito especial. A modo de ejemplo, un sistema de IA entrenado para clasificar correos electrónicos como *spam* o no solo tiene capacidad para resolver este problema, por lo que no será capaz, salvo previo entrenamiento, de predecir, por ejemplo, el comportamiento del mercado bursátil. Es en este punto donde se debe diferenciar entre las dos categorías en las que se puede clasificar la IA en función de las tareas que pueda desempeñar:

- *IA débil (Weak AI).* A través de este concepto se engloba a los sistemas de IA orientados al cumplimiento de funciones u objetivos concretos: clasificación de fotos, conducción de vehículos, detección de enfermedad, etc. Cabe destacar que, como ya se adelantaba, es la IA que actualmente dispone de mayor desarrollo y uso.

- *IA fuerte (Strong AI):* mediante este término se refiere a los sistemas de IA con capacidad para desempeñar cualquier tarea o actividad, es decir, una IA de propósito general. Actualmente no existen ejemplos de IA fuerte, más allá de los que podemos encontrar en novelas, películas y series.

Desde una perspectiva práctica, y como ya se adelantaba al principio de este apartado, la IA se compone de diversas tecnologías y su marcado carácter transversal implica que, en la cadena de creación, diseño, desarrollo y despliegue de los sistemas de IA, intervengan una gran variedad de operadores, en función de las tareas asumidas por cada uno de ellos. Por tanto, resulta fundamental, para entender la IA y los sujetos que intervienen, conocer su ciclo de vida. Sin ánimo de ser estrictamente técnicos, en el ciclo de vida de un sistema de IA pueden destacarse las siguientes etapas: 1) diseño y desarrollo, 2) entrenamiento y validación, 3) despliegue, 4) explotación, 5) revisión y optimización, y 6) retirada.

Ciclo de desarrollo de un sistema de IA

Fuente: elaboración propia.

Independientemente del número de etapas que conforman el ciclo de vida de un sistema de IA, no existe una relación directa entre estas y el número de operadores que intervienen, lo que puede derivar en casos en los que, debido a la intervención de una gran cantidad de operadores, se incremente el grado de incertidumbre en el marco de la responsabilidad.

Sin perjuicio de lo anterior, no son pocas las ocasiones en las que el mismo operador asume gran parte o la totalidad de las etapas de desarrollo y validación, para posteriormente ofrecerlo como producto o servicio al usuario final.

Es en este punto donde adquiere protagonismo el *cloud computing,* término con el que se hace referencia a la prestación de servicios tecnológicos a través de la red. Debido al constante desarrollo de las nuevas tecnologías y, entre otras, el coste que supondría su desarrollo e implementación individual de estas por cada uno de los operadores del mercado, además del mantenimiento y la gran capacidad de computación necesaria, sería prácticamente inviable que las empresas pudieran implementar un sistema de IA, dado que tendrían que asumir todas las funciones de

desarrollo y explotación, con la consecuente necesidad de disponer de profesionales con los conocimientos necesarios y los costes para abordar todo el ciclo de vida previamente mencionado.

Si el objetivo de las empresas para adaptarse al mercado pasa por la transformación tecnológica, el *cloud computing* se erige como el "trampolín" que permite a las empresas poder implementar las soluciones tecnológicas que consideren necesarias, sin tener que asumir el enorme coste que supondría el desarrollo y mantenimiento técnico de estas.

Los servicios *cloud* se pueden clasificar atendiendo a una gran variedad de criterios, pero la que mayor reconocimiento ostenta es la que se establece en función de los servicios prestados al usuario y su posibilidad para poder modificarlo o adaptarlo a sus necesidades. En este sentido cabe diferenciar entre los siguientes servicios *cloud:* software como servicio o *Software as a Service* (SaaS), plataforma como servicio o *Platform as a Service* (PaaS) e infraestructura como servicio o *Infraestructure as a Service* (IaaS).

Por tanto, y en función de cuáles sean las necesidades y preferencias de cada operador, se optará por un servicio de *cloud computing* u otro, pues, aunque todos ellos son servicios en línea, cuyo funcionamiento se da a través de la nube, distan respecto del mantenimiento, funcionalidad y soporte ofrecidos por el proveedor. Por ejemplo, mientras que a través del SaaS los usuarios acceden exclusivamente a un servicio (p. ej., el correo electrónico), el PaaS permite al usuario gestionar la plataforma (p. ej., Google App Engine que permite ejecutar aplicaciones sobre la infraestructura de Google).

Respecto al campo de la IA, son muchos los proveedores de servicios que, a través de la nube *(cloud),* ofrecen herramientas de IA como producto o servicios. Por ejemplo, Microsoft Azure permite el desarrollo e implementación, a través de su plataforma, de una gran variedad de soluciones tecnológicas, que van desde el análisis de datos, hasta el *blockchain,* pasando por soluciones de IA e IoT.

Es en este punto donde las empresas que hayan implementado herramientas o soluciones basadas en IA podrán adaptarse a la nueva demanda y mejorar su

posición en el mercado. En este sentido, y sin ánimo de ser exhaustivos, la IA puede ofrecer a los operadores del mercado los siguientes beneficios:

- *Personalización de la experiencia.* La captación, almacenamiento y análisis de grandes cantidades de datos declarados por el propio usuario o generados en la propia red permite generar perfiles de los usuarios y, en consecuencia, el desarrollo y despliegue de soluciones de IA que permitan personalizar el trato de los usuarios, a través de sistemas de recomendaciones y avisos basados en sus preferencias e intereses. En este sentido, Neftlix dispone de soluciones de IA que permiten, a través de variables como el tiempo medio de conexión de los usuarios, franja horaria de conexión, películas y series vistas con anterioridad y edad, entre otras, habilitar un sistema de recomendaciones personalizado que avise al usuario sobre nuevo material audiovisual que podría ser de su interés.

- *Agilización en la atención y resolución de controversias*. Mediante el entrenamiento y uso de *chatbots,* las empresas pueden ofrecer a los usuarios una herramienta que permita resolver las dudas que los usuarios pueden plantear, algo que hasta el momento cumplían las ya tan conocidas FAQ pero que, a diferencias de los actuales *chatbots,* no se actualizan de forma automática con las cuestiones que puedan ir planteando los usuarios. De esta forma, los usuarios pueden resolver sus dudas en cualquier momento, sin importar si la cuestión la plantean un día festivo o si la hora de la consulta es antes o después del horario comercial, evitando así las, a veces, tan incompletas FAQ o los tiempos medios de respuesta que, en caso de tener que ser respondidas por personas, podrían demorarse en función del número de consultas y el momento en el que han sido planteadas.

- *Mejora en los procesos internos y logísticos.* El uso de soluciones basadas en IA permite a las empresas poder adoptar decisiones respecto de su actividad en el mercado, desde la cantidad de productos de los que disponen en oferta, hasta el desarrollo de nuevas áreas de negocio, pasando por el tipo de publicidad en función de las características de los usuarios que adquieren sus bienes y/o servicios. En este sentido, puede destacarse el sistema *Method and System for Anticipatory Package Shipping* de la empresa Amazon, que, a partir

del análisis de los datos de los usuarios (p. ej., historial de compras, hábitos de consumo, etc.), permite adoptar un modelo predictivo del comportamiento del consumidor. De esta forma, se podrá anticipar la demanda en una determinada área geográfica y abastecer los almacenes más cercanos con carácter previo al incremento previsto de la demanda.

4. USO DE LA IA EN EL SECTOR ASEGURADOR Y EL MARCO DE REGULACIÓN DE LA IA

4.1. LA GOBERNANZA DE LA IA EN LA UNIÓN EUROPEA

Las distintas jurisdicciones se están preparando para adaptarse al nuevo paradigma social y regulatorio que la IA va a generar en el mundo. Como hemos comentado previamente, la adopción de la IA lleva consigo una serie de riesgos y complejidades que los Estados deben atajar y solventar para generar una certidumbre jurídica suficiente como para generar el tan ansiado equilibrio entre seguridad jurídica e inversión. El reto de la regulación de la IA no puede afrontarse individualmente, puesto que cada jurisdicción sufre de los mismos riesgos respecto de la tecnología existente, por lo que surge la necesidad de delegar en los organismos supranacionales para construir un marco jurídico global y más heterogéneo.

En lo que corresponde a España y a la Unión Europea, sus enfoques desde las instituciones han consistido en una metodología "top-down", donde en las primeras etapas de comprensión tecnológica y jurídica han consistido en proyectos de investigación o comités de expertos que han pretendido abordar desde un enfoque técnico el aterrizaje de la tecnología emergente; posteriormente, los organismos gubernamentales han desarrollado la estrategia de implementación, y por último, han desarrollado y compartido los proyectos normativos con los principales *stakeholders.*

Etapas	Unión Europea
Investigación técnica	High-Level Expert Group on Artificial Intelligence: *Policy and investment recommendations for trustworthy Artificial Intelligence* (2019)
Planificación estratégica	Estrategia Digital Europea: *Libro Blanco sobre la inteligencia artificial* (2020)
Desarrollo legislativo	Propuesta de Reglamento por el que se establecen normas armonizadas sobre la inteligencia artificial (2021)

La gobernanza de la IA no solo es competencia de los operadores, sino también de los legisladores a la hora de determinar el proceso regulatorio de una manera idónea para que exista un equilibrio entre la seguridad jurídica y el desarrollo de la tecnología, tal y como se desarrolló en el apartado 2.2 respecto al proceso regulatorio que debe imperar en el desarrollo legislativo de la IA.

En este sentido, la UE ha avanzado en el modelo de gobernanza que pretende para el desarrollo de la IA en el ámbito europeo. Trasladando el modelo que impone el RGPD, la Comisión Europea aboga por la creación de un Comité Europeo de Inteligencia Artificial con un fin asistencial y coordinador para los Estados miembros. Este comité estará compuesto por la Comisión Europea como presidencia, el supervisor europeo de protección de datos y las autoridades nacionales competentes y designadas.

Las autoridades nacionales serán designadas por los Estados miembros, con la función principal de hacer cumplir las directrices del futuro reglamento. Cabe destacar que esta futura autoridad nacional no necesita las condiciones de autonomía e independencia en el desempeño de sus funciones, a diferencia de las autoridades de control en materia de protección de datos. Estas autoridades podrán ser órganos gubernamentales, al igual que también podrán ser autoridades independientes conforme al artículo 109 de la Ley de Régimen Jurídico del Sector Público (LRJSP). Actualmente, España cuenta con la Secretaría de Estado de Digitalización e Inteligencia Artificial, con la competencia para desarrollar dicha tecnología, y podría ser objeto para designación como autoridad nacional.

La propuesta de reglamento permitiría compartir dicha competencia entre varias autoridades nacionales, siempre que exista una motivación, por lo que sería posible que la competencia del control del cumplimiento en materia de protección de datos sea compartida con la Agencia Española de Protección de Datos; binomio similar al existente entre las competencias de cumplimiento que existe en la Ley de Servicios de la Sociedad de la Información, cuyas facultades de supervisión de control están compartidas entre la Agencia Española de Protección de Datos, en lo que respecta a las disposiciones relativas a la protección de datos personales, y el Ministerio de Asuntos Económicos y Transformación Digital.

4.2. IA E *INSURTECH*

Como ya se ha expuesto previamente, las entidades aseguradoras están transformando su estructura, su forma de intervenir en el mercado y los productos y servicios ofertados como consecuencia del uso de las nuevas tecnologías en sus procesos, aunque en este apartado se abordará desde la perspectiva del uso de la IA.

A medida que la IA se integra en la industria del seguro, los operadores deben responder a la transformación, debiendo comprender los factores que contribuirán al cambio y cómo la IA modificará los procedimientos tan recurrentes como, entre otras, las reclamaciones, la suscripción de las pólizas y la fijación de las primas. Solo con esta comprensión se pueden empezar a adoptar estas tecnologías emergentes para adquirir los beneficios que pueden ofrecer a la industria del seguro.

En relación con la explicación de la cadena de valor en el sector asegurador, la Autoridad Europea de Seguros y Pensiones de Jubilación (EIOPA, por sus siglas en inglés) destaca una serie de casos de uso a lo largo de la cadena de valor:

Producto	Precio y suscripción	Ventas y distribución	Servicio al cliente	Prevención del fraude	Gestión de reclamaciones
• Análisis de datos históricos de clientes y encuestas para informar nuevos productos. • Modelado predictivo de patrones de desarrollo de enfermedades. • Productos novedosos, p. ej., seguros paramétricos y basados en el uso.	• Evaluaciones de riesgos mejoradas que combinan fuentes de datos tradicionales y nuevas (incluidos datos de IoT).	• Técnicas de *marketing* digital basadas en el análisis dinámico del comportamiento de búsqueda *online.* • Asistente virtual y *chatbots* que utilizan procesamiento del lenguaje natural (NLP) y ontologías de seguros para respaldar la comunicación.	• Análisis de sentimiento del centro de llamadas, análisis de causa de ruta, *scripts* dinámicos y asignación de agentes. • Autoservicio del cliente a través de múltiples canales utilizando PNL, reconocimiento de voz, mapas de ontología de seguros y *chatbots.*	• Proporcionar asesoramiento y entrenamiento de diagnóstico basados en análisis de inteligencia artificial de Big Data automotriz y de salud, p. ej., sugerir cambios en el comportamiento de conducción y ejercicio.	• Análisis de fraude mejorado: puntuación de reclamaciones, detección de anomalías, análisis de redes sociales y modelado de comportamiento. • Reserva de pérdidas: uso de IA para estimar las pérdidas de valor, en particular para las reclamaciones de alta frecuencia.

Continúa

Producto	Precio y suscripción	Ventas y distribución	Servicio al cliente	Prevención del fraude	Gestión de reclamaciones
	• Optimización de precios: precios de microsegmento / personalizados basados en datos de comportamiento individual sin riesgo (por ejemplo, para estimar la elasticidad del precio, el valor de por vida y la propensión a la rotación) y análisis de la competencia del mercado.	• Comunicación proactiva con el cliente, promoción y venta cruzada de servicios relacionados ("siguiente mejor acción") basada en los datos del consumidor de los sistemas de gestión de relaciones con el cliente (CRM).	• Automatización robótica de procesos (RPA) que incluye reconocimiento óptico de caracteres (OCR) para extraer información de documentos (por ejemplo, FNOL, correo electrónico con preguntas, quejas, etc.) y enviarlos al departamento correcto.		• Reconocimiento de imágenes por IA para estimar los costos de reparación en seguros de propiedad del hogar, locales comerciales y automotriz. • Segmentación automatizada de reclamaciones por tipo y complejidad y proceso automatizado de verificación y pago de facturas.

Fuente: EIOPA, Consultative Expert Group on Digital Ethics in insurance.

La actividad de las aseguradoras se encuentra íntimamente ligada a los datos[26]. A consecuencia de lo anterior, y teniendo en cuenta la importancia que tiene para el sector asegurador la recolección y análisis de datos para cualquiera de las actividades que desarrolle, la implantación y uso del Big Data y la IA era un hecho que, inevitablemente, está sucediendo.

Las fuentes de las que las aseguradoras pueden obtener los datos con los que desarrollar su actividad se han ampliado considerablemente, disponiendo no solo de fuentes directas (p. ej., los obtenidos de los propios asegurados y tomadores), sino también de fuentes indirectas (p. ej., actividad del usuario a través de internet, información extraída de dispositivos IoT, datos bancarios, etc.)[27].

[26] *Vid*. Muñoz Paredes, M. L., "Big Data y contrato de seguro: los datos generados por los aseguradores y su utilización por los aseguradores", en Díaz González, G. M. (coord.), *La regulación de los algoritmos,* Thomson Reuters Aranzadi, Madrid, 2020, pp. 129-162.

[27] *Vid.* EIOPA, *Big Data Analythics in motor and health insurance: a themativ review,* Luxemburgo, 2019, p. 9. Recuperado de: https://register.eiopa.europa.eu/Publications/EIOPA_BigDataAnalytics_ThematicReview_April2019.pdf (fecha de consulta: 21-09-2021).

Fuentes de datos tradicionales	Fuentes de datos derivadas de la digitalización
Datos médicos (p. ej., historial médico y estado de salud).	*Datos IoT* (p. ej., tipo de conducción, actividad física y condición médica).
Datos demográficos (p. ej., edad, estado civil, profesión y dirección).	*Datos obtenidos de internet* (p. ej., búsquedas en la web, compras en línea, actividades en las redes sociales e información sobre el desarrollo profesional).
Datos sobre el riesgo (p. ej., tipo de coche y valor de los accesorios).	*Datos digitales propios de las compañías de seguros* (p. ej., interacción con las compañías de seguros: 1) datos del centro de llamadas, 2) información digital de las cuentas de los usuarios, 3) informes digitales de reclamaciones, 4) comportamiento en línea al acceder a los sitios web de las compañías de seguros o al utilizar la aplicación de las compañías de seguros).
Datos de comportamiento del asegurado (p. ej., fumar, consumo de alcohol, distancia recorrida en un año).	
Datos sobre siniestros (p. ej., informes de reclamaciones por accidentes de tráfico y casos de responsabilidad).	*Datos de geolocalización* (p. ej., coordenadas de latitud y longitud de una dirección física).
Datos sobre la población (p. ej., ratios de mortalidad, tasas de morbilidad, accidentes de tráfico).	*Datos genéticos* (p. ej., resultados de análisis predictivos de los genes y cromosomas de una persona).
Datos sobre el peligro (p. ej., frecuencia y gravedad de los peligros naturales).	*Datos de cuentas bancarias / tarjetas de crédito* (p. ej., hábitos de compra del consumidor, datos de ingresos y patrimonio).
Otros datos tradicionales (p. ej., puntuación de crédito, informes de ajuste de reclamaciones, información de los talleres de reparación de automóviles).	*Otros datos digitales* (p. ej., selfi para estimar la edad del consumidor).

Fuente: elaboración propia.

Como consecuencia directa de la ampliación de las fuentes de las que las entidades aseguradoras pueden obtener datos de los asegurados y, en consecuencia, el volumen y variedad de estos, se produce un incremento en el desarrollo y uso de las nuevas tecnologías emergentes que necesitan de grandes volúmenes de datos para poder explotar sus funcionalidades, como el caso de los sistemas de IA.

4.3. MARCO NORMATIVO EMERGENTE: PROPUESTAS NACIONALES Y COMUNITARIAS

En el marco de una realidad donde existe un incremento exponencial en el número de entidades e instituciones, públicas y privadas, que hacen uso de herramientas basadas en IA para el desarrollo de su actividad, cada vez son más los aspectos de la realidad en los que, de forma directa o indirecta, existe un impacto derivado del uso de esta tecnología.

Si bien la IA tiene un gran poder para resolver problemas complejos y ofrecer nuevas posibilidades, que hasta hace una década formaban parte de la ciencia ficción, no debe olvidarse que la IA también se erige, a su vez, como una herramienta con capacidad para generar un potencial impacto negativo en la sociedad. Adicionalmente, existen problemas presentes referidos a la responsabilidad jurídica que los operadores afrontan con incertidumbre debido a la inadecuación del marco jurídico existente[28].

En este sentido, y desde el año 2017, las instituciones de la Unión Europea han elaborado una gran cantidad de propuestas, proyectos y dictámenes con el objetivo de fomentar el desarrollo seguro de la IA a través de un equilibro entre: 1) el fomento del desarrollo y uso de herramientas basadas en IA y 2) la protección de la sociedad frente a los posibles impactos negativos derivados de la implementación de soluciones basadas en IA.

La agenda digital publicada por la Comisión Europea el 19 de febrero de 2020[29] tiene como objetivo establecer los pilares para impulsar la economía europea aprovechando las ventajas económicas y sociales sostenibles del mercado único digital.

---

[28] *Vid*. Bonmatí, J. y Gonzalo, J. J., "La gestión de riesgos y su encaje legal en la regulación de la inteligencia artificial", en Fuentes, O. (dir.), *Era digital, sociedad y derecho*, Tirant lo Blanch, Valencia, 2020, p. 34.

[29] *Vid*. Comisión Europea, *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Configurar el futuro digital de Europa*, COM(2020) 67 final, 2020, pp. 2-3. Disponible en: https://ec.europa.eu/transparency/regdoc/rep/1/2020/ES/COM-2020-67-F1-ES-MAIN-PART-1.PDF (fecha de consulta: 21-09-2021).

En los próximos cinco años, la Comisión se centrará en tres objetivos clave para garantizar que las soluciones digitales incrementen la importancia de la UE en el mercado digital:

- Garantizar el uso de la tecnología al servicio de las personas, garantizando así una economía fuerte y competitiva que domine y dé forma a la tecnología respetando los valores europeos.

- Alcanzar una economía justa y competitiva, en la que las empresas de todos los tamaños y de cualquier sector puedan competir en igualdad de condiciones y puedan desarrollar, comercializar y utilizar tecnologías, productos y servicios digitales a una escala que impulse su productividad y competitividad global.

- Asegurar una sociedad abierta, democrática y sostenible, basándose en un entorno de confianza en el que los ciudadanos tengan poder sobre su forma de actuar e interactuar y sobre los datos que proporcionan tanto en línea como fuera de ella.

Para el desarrollo de esta agenda digital, basada en la sociedad, la economía y las personas, son múltiples los proyectos legislativos que actualmente se encuentran en fases de desarrollo, aprobación y aplicación: regulaciones de las plataformas digitales, desarrollo de una estrategia relativa al tratamiento de los datos personales, actualización de la normativa de defensa y protección de consumidores, el establecimiento de una regulación relativa a la ciberseguridad y la IA, entre otros.

La revolución digital se erige como una de las cuestiones fundamentales sobre las que la UE ha decidido centrar la futura regulación, con la finalidad de procurar seguridad jurídica y, con ella, el desarrollo efectivo de las nuevas tecnologías.

En este sentido, y respecto a la IA, la UE pretende construir la futura regulación en un enfoque basado en el riesgo mediante la aplicación de criterios flexibles[30] que permitan evitar la rápida obsolescencia de la regulación desarrollada[31].

En el marco de la IA, la UE ha desarrollado durante los últimos años, y más concretamente desde el año 2017, una gran variedad de informes, recomendaciones, directrices y propuestas legislativas que, si bien cada vez otorgan una mayor seguridad jurídica arrojando luz sobre la regulación del desarrollo y uso de sistemas de IA, la dispersión y volumen de documentos hace necesario que en las próximas páginas se exponga de forma cronológica los principales hitos, ideas y propuestas.

4.3.1. Recomendaciones destinadas a la Comisión sobre Normas de Derecho Civil sobre Robótica (Parlamento Europeo)

Los primeros pasos, desde una perspectiva legislativa, comienzan con la resolución del Parlamento Europeo de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre Normas de Derecho Civil sobre Robótica. En esta resolución, y sin perjuicio de otro contenido, se destaca que el desarrollo de la robótica y la IA genera nuevas preocupaciones relativas a la responsabilidad y que deben analizarse desde una perspectiva común, con el fin de garantizar el mismo grado de eficiencia, transparencia y coherencia en la garantía de la seguridad jurídica en toda la UE en beneficio de los ciudadanos, el mercado y las empresas.

En este sentido, y respecto a la resolución de las preocupaciones en materia de responsabilidad, el Parlamento propone tres ideas que, *a posteriori*, han sido desarrolladas y forman la base de las principales propuestas normativas en materia de responsabilidad y ética en el campo de la IA:

- Enfoque dual de la responsabilidad civil: 1) responsabilidad objetiva y 2) responsabilidad subjetiva, basada esta última en atribuir la responsabilidad a la

[30] *Vid*. Bonmatí, J. y Gonzalo, J. J., "La gestión de riesgos y su encaje legal en la regulación de la inteligencia artificial", en Fuentes, O. (dir.), *Era digital, sociedad y derecho*, Tirant lo Blanch, Valencia, 2020, p. 118.

[31] *Vid*. CE, *Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza*, COM (2020) 65 final, 2020, p. 31.

persona que es capaz, en determinadas circunstancias, de minimizar los riesgos y gestionar el impacto negativo del sistema de IA.

- Proponer el establecimiento de un régimen de seguro obligatorio, como ya se aplica, por ejemplo, en el caso de los automóviles.

- Sometimiento del desarrollo y uso de sistemas de IA al cumplimiento de los valores europeos. Este apartado ha sido ampliamente desarrollado por el HLEG.

4.3.2. Directrices éticas para una IA fiable (HLEG) y su adaptación según la EIOPA

Posteriormente, y ya en el año 2019, el HLEG emitió uno de los informes con mayor repercusión en el campo jurídico de la IA dentro de la UE: *Ethics guidelines for trustworthy AI*. A lo largo del informe, que se erige como una suerte de directrices, se promueve un marco de cumplimiento que garantice que los sistemas de IA sean fiables, es decir, pasar de la IA a la IAF. Para alcanzar la IAF, el HLEG recoge los tres requisitos que deben satisfacerse a lo largo de todo el ciclo de vida del sistema de IA:

- *Licitud:* se garantiza el cumplimiento de la normativa aplicable.

- *Ética:* se asegura el cumplimiento de los principios y valores éticos de la UE.

- *Robustez:* se garantiza un funcionamiento seguro, tanto desde el punto de vista técnico como social.

Sin perjuicio de las características de licitud y robustez, el informe se centra, principalmente, en la vertiente ética. La ética de la IA es un subcampo de la ética que estudia los problemas éticos que plantea el desarrollo, despliegue y utilización de la IA.

El informe recoge, en forma de cascada: 1) la exposición de los cuatro principios éticos esenciales que debe de cumplir todo sistema de IA; 2) el desarrollo de los requisitos clave que deben cumplirse para poder asegurar la vigencia de los principios éticos, y 3) las medidas con las que abordar y evaluar el cumplimiento de los requisitos.

En primer lugar, el informe reconoce cuatro imperativos éticos que, extraídos de los derechos fundamentales, deben cumplirse para garantizar que los sistemas de IA se desarrollen, desplieguen y utilicen de manera fiable:

- *Respeto de la autonomía humana.* Los sistemas de IA deberán ser desarrollados para incentivar las aptitudes cognitivas, sociales y culturales de las personas (p. ej., garantizar una plena información del usuario) y no con la finalidad, directa o indirecta, de subordinar, coaccionar, engañar, manipular, condicionar o dirigir a los seres humanos de manera injustificada.

- *Prevención del daño.* Los sistemas de IA deberán desarrollarse y desplegarse garantizando su seguridad, es decir, adoptando todas las medidas técnicas (p. ej., obtención de certificados) y sociales necesarias para asegurar su inocuidad.

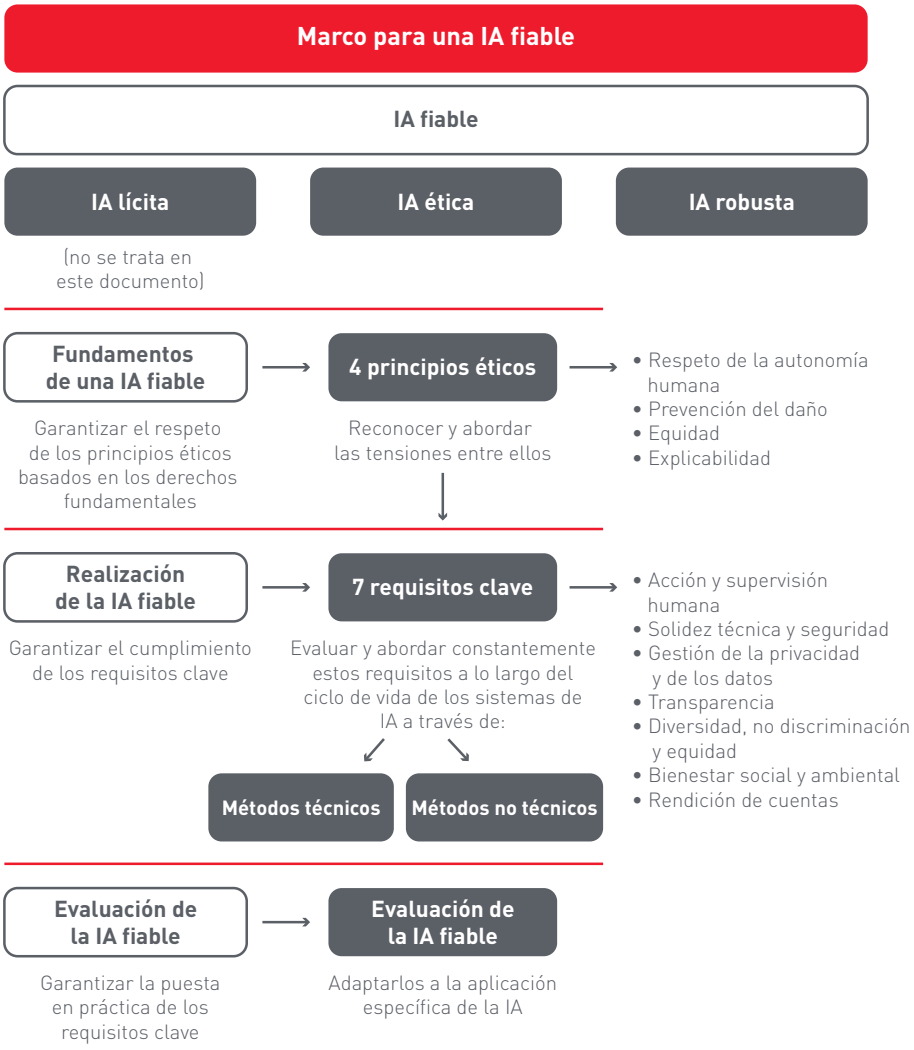
  - *Equidad.* Especialmente orientado a repeler los dos principales problemas de los sistemas de IA: los sesgos y la discriminación. La equidad se debe enfocar desde una doble perspectiva:

  - *Sustantiva:* asegurar que las personas y grupos no sufran sesgos injustos, discriminación y/o estigmatización, así como garantizar la proporcionalidad en el uso de sistemas de IA atendiendo a los medios y el fin propuesto.

- *Procedimental:* garantizar la interactuación de las personas en la toma de decisiones mediante el uso, total o parcial, de sistemas de IA, así como la posibilidad de oponerse.

- *Explicabilidad.* Fundamental para construir la confianza en la IA, estableciendo mecanismos que permitan que los procesos sean transparentes, dotados de trazabilidad y con posibilidad de emitir las correspondientes explicaciones, proporcionalmente a una amplia variedad de criterios.

Marco para una IA fiable



Fuente: HLEG.

En segundo lugar, y con el objetivo de poder llevar a la práctica los principios éticos referidos en el apartado anterior, el HLEG expone los siete requisitos que, bajo su consideración, debe cumplir cualquier sistema de IA:

1. *Acción y supervisión humana.* Con la finalidad de garantizar que los sistemas de IA son diseñados y desplegados como medios para mejorar la capacidad de las personas (p. ej., mejorar el conocimiento sobre las necesidades del tipo de seguro que necesita el usuario conforme a sus necesidades). En este sentido, los sistemas de IA siempre deben garantizar la intervención humana en cualquier de sus fases. La supervisión humana puede implementarse a través de tres modelos:

   - *Human in the loop* (HITL): las personas intervienen en la toma de decisiones del sistema de IA.

   - *Human on the loop* (HOTL): las personas supervisan el funcionamiento del sistema de IA y pueden revisar las decisiones adoptadas.

   - *Human in control* (HIC): las personas supervisan, a rasgos generales, el sistema de IA, pudiendo decidir cuándo y cómo utilizarlo.

   Según el modelo utilizado y, por tanto, en función del nivel de supervisión que se ejerza sobre un sistema de IA, podrá variar la exigencia respecto de la implementación de otros medios que aseguren una adecuada gobernanza de la IA.

2. *Solidez y seguridad técnica.* Desde una perspectiva técnica y funcional, los sistemas de IA deben desarrollarse y desplegarse bajo el cumplimiento de una serie de garantías que permitan asegurar el sólido funcionamiento de este, con unos niveles óptimos de precisión y fiabilidad de sus resultados.

   Adicionalmente, debe asegurarse que, desde una perspectiva de seguridad, los sistemas de IA sean resistentes a los posibles ataques que, física o digitalmente, pudieran ir dirigidos contra: 1) los datos, 2) el propio modelo y/o 3) la infraestructura informática subyacente (tanto el software como el hardware).

3. *Gestión de privacidad de los datos.* Dado que los sistemas de IA se entrenan y usan sobre la base del uso de los datos, adquiere especial importancia: la protección de estos cuando son catalogados como datos de carácter personal y garantizar que los datos utilizados disponen de la calidad suficiente para la finalidad del sistema de IA.

   - Por un lado, cabe destacar que la privacidad es un derecho fundamental que se ve especialmente afectado en el campo de la IA, por lo que debe garantizarse, en todo momento, la protección de la intimidad y la privacidad de los datos a lo largo de todo el ciclo de vida del sistema de IA.

   - Por otro lado, los datos también deben ser objeto de control desde una perspectiva de la calidad e integridad de estos, es decir, que los datos deben ser recopilados y revisados con la finalidad de eliminar los posibles sesgos sociales, imprecisiones y errores, así como evitar sus posibles modificaciones malintencionadas una vez introducidos.

4. *Transparencia.* Debido a la complejidad en el diseño, entrenamiento y funcionamiento de los sistemas de IA, pero la cada vez mayor relevancia que está adquiriendo en el desarrollo de las personas y la sociedad, adquiere especial importancia que la empresa u organización que haga uso de los sistemas de IA garantice a los usuarios:

   - La trazabilidad de los datos y los procesos que hayan dado lugar a la decisión del sistema de IA, facilitando la posibilidad de identificar los motivos principales que han llevado a la toma de una decisión, así como los posibles sesgos y errores.

   - La explicabilidad del sistema de IA, con la finalidad de poder ofrecer a la parte interesada una explicación, oportuna y acorde a su nivel de especialización, respecto de las decisiones adoptadas total o parcialmente por el sistema de IA.

   - La comunicación de que se está relacionando con un sistema de IA, así como la posibilidad de decidir si prefiere interactuar con un sistema de IA

o con otra persona, con el fin de garantizar el cumplimiento de sus derechos fundamentales.

5. *Diversidad, no discriminación y equidad.* Sobre la base de la protección de los derechos fundamentales de los usuarios que puedan verse afectados directamente por un sistema de IA, deben examinarse con precisión los datos utilizados, los modelos aplicados y/o la estructura sobre la que se desarrolla el sistema de IA, para reducir/eliminar los prejuicios y la discriminación que podrían instaurar o perpetuar.

   Asimismo, y con el fin de desarrollar sistemas de IA fiables, es recomendable consultar a las partes interesadas que se puedan ver afectadas de manera directa o indirecta por el sistema a lo largo de todo su ciclo de vida.

6. *Bienestar social y ambiental.* El desarrollo y despliegue de sistemas de IA requiere de la inversión de una gran cantidad de medios técnicos y humanos, por lo que adquiere especial importancia fomentar la sostenibilidad y la responsabilidad ecológica de los sistemas de IA, impulsando la investigación de soluciones de IA para hacer frente a los temas que suscitan mayor preocupación a escala mundial, aprovechando los recursos ya desarrollados en otros sistemas de IA.

7. *Rendición de cuentas.* Se deben establecer mecanismos que permitan garantizar la responsabilidad y rendición de cuentas sobre los sistemas de IA y sus resultados, tanto *a priori* (antes de su implantación) como *a posterior* (tras su despliegue).

   Uno de los medios más destacados para la rendición de cuentas se sustenta en la auditabilidad, es decir, la evaluación de los algoritmos, los datos y los procesos de diseño, así como en el establecimiento de mecanismos accesibles que aseguren una compensación adecuada cuando se produzcan efectos adversos injustos.

La aplicación de todos los requisitos y el cumplimiento de todos los principios no están exentos de conflictos pues, en ocasiones, la garantía de unos puede traducirse

en el incumplimiento de otros. En este sentido, cabe destacar el conflicto existente entre la precisión y la explicabilidad de los sistemas de IA.

Los sistemas de IA evolucionan hacia una mayor complejidad técnica, en aras de garantizar una mejor precisión de estos, es decir, la capacidad del sistema para realizar juicios correctos o tomar decisiones correctas basándose en datos o modelos. Esta complejidad dificulta la posibilidad de exponer de forma sencilla la lógica de su funcionamiento, es decir, la explicabilidad y la transparencia.

Tanto la transparencia como la precisión son características esenciales para asegurar la fiabilidad de los sistemas de IA, pero existe un evidente conflicto entre el incremento de la complejidad de algunos sistemas de IA con el objetivo de aumentar su precisión y la obligación de explicar la lógica de funcionamiento de un sistema de IA para dar cumplimiento al principio de transparencia.

Principios en el desarrollo de un sistema de IA

Fuente: Comisión Europea.

Todos los requisitos expuestos previamente se encuentran relacionados, de una forma u otra, con los principios éticos referidos previamente. A continuación, se expone la relación existente entre los requisitos y los principios éticos cuyo cumplimiento protegen.

Requisitos	Principio ético
Acción y supervisión humana	Autonomía humana
Solidez técnica y seguridad	Prevención del daño
Gestión de la privacidad y los datos	Prevención del daño
Transparencia	Explicabilidad
Diversidad, no discriminación y equidad	Equidad
Bienestar social y ambiental	Prevención del daño y equidad
Rendición de cuentas	Equidad

Fuente: elaboración propia.

En tercer lugar, y para el cumplimiento de los requisitos referidos previamente, los operadores deberán desplegar los métodos técnicos y no técnicos necesarios. Los métodos son complementarios y alternativos entre sí, dado que los diferentes contextos pueden plantear la necesidad de utilizar distintos métodos.

Métodos técnicos	Métodos no técnicos
Desarrollo de una correcta arquitectura para una IA fiable	Cumplimiento de la normativa
Evaluación de la ética y Estado de derecho desde el diseño	Elaboración de códigos de conducta
Análisis de los distintos métodos de explicación	Normalización
Realización de ensayos y validación	Obtención de certificaciones
Indicadores de calidad del servicio	Rendición de cuentas a través de marcos de gobernanza
	Educación y concienciación para fomentar una mentalidad ética
	Participación de las partes interesadas y diálogo social
	Diversidad y equipos de diseño inclusivos

Fuente: elaboración propia.

En el marco de la consecución de una IAF, y sobre la base de las directrices referidas previamente, la EIOPA elaboró el informe *Artificial Intelligence Governance Principles: Towards Ethical and Trustworthy Artificial Intelligence In The European Insurance Sector*[32], publicado en junio del año 2021, en el que desarrollan los principios de gobernanza de la IA desde la perspectiva de las especialidades del sector del seguro.

Tal y como se refiere en el informe, y sin perjuicio de que actualmente existe un amplio marco legislativo que sustenta la actividad de las empresas del sector asegurador, cabe destacar que las empresas de seguros deben disponer de un sistema eficaz de gobernanza que permita una gestión sana y prudente de su actividad, lo que requiere de un análisis más profundo para ayudar a las organizaciones a comprender su significado en el contexto de la IA, garantizando así un uso ético de los datos y las tecnologías digitales.

Como ya se ha indicado previamente, la EIOPA parte de las directrices fijadas por el HLEG, realizando una serie de modificaciones, tal y como se recoge en la siguiente tabla[33], donde se comparan los informes AI HLEG y GDE.

Commission's AI HLEG ethical guidelines for trustworthy AI	EIOPA's GDE AI governance principles
Human agency and Oversight	Human oversight
Technical robustness and safety	Robustness and performance
Privacy and Data Governance	Data governance and record keeping
Transparency	Transparency and explainability
Diversity, non discrimination and fairness	Fairness and non-discrimination
Societal and environmental well-being	(Fairness and non-discrimination)
Accountability	(Transparency and Explainability / Data Governance and record keeping)
	Principle of proportionality

Fuente: EIOPA.

[32] *Vid*. EIOPA, *Artificial Intelligence Governance Principles: Towards Ethical and Trustworthy Artificial Intelligence in the European Insurance Sector*, 2021.

[33] *Vid*. *Op. Supra,* p. 15.

Partiendo de las directrices elaboradas por la HLEG respecto de la IAF, la EIOPA las ha adaptado a las especificidades del sector de los seguros, centrándose en aquellos requisitos que se han considerado más relevantes para este sector. Como resultado, seis son los principios de gobernanza de la IA que el sector asegurador debe tener en cuenta al implementar o considerar la implementación de sistemas de IA.

Con carácter previo a la implementación de sistemas de IA, la entidad interesada deberá realizar la pertinente evaluación de impacto, con la finalidad de determinar las medidas de gobernanza necesarias para cada uso específico de la IA, garantizando siempre la proporcionalidad de los beneficios derivados de su uso y el impacto potencial en los consumidores y/o en las propias empresas de seguros.

En función del resultado de la evaluación de impacto, que deberá arrojar la existencia de un riesgo alto, medio o bajo (sin perjuicio de la posibilidad de modificar o añadir más niveles), sobre la base de la probabilidad y gravedad de los daños potenciales sobre los consumidores y la propia empresa, esta deberá resolver la implementación o no del sistema de IA que ha sido objeto de evaluación.

Si finalmente se procede a la implementación y uso de la IA, la EIOPA recomienda que esta cumpla, durante todo su ciclo de vida, con los siguientes principios:

1. *Equidad y no discriminación*

   Dado que las empresas aseguradoras deben actuar siempre con honestidad, equidad y profesionalidad, de acuerdo con los mejores intereses de los clientes, estas deben evitar el refuerzo de las desigualdades existentes (p. ej., mediante las puntuaciones de crédito o la aplicación de políticas de maximizar la "disposición a pagar" o la "disposición a aceptar" de los consumidores), así como controlar y mitigar los sesgos.

   La equidad debe ser valorada desde una doble dimensión: 1) procedimental, que se centra en la gobernanza, y 2) sustantiva, que se centra en los resultados.

   La equidad procedimental, tal como se referirá en los siguientes puntos, se consigue promoviendo la transparencia y la explicabilidad suficientes para

garantizar la responsabilidad de la empresa y el conocimiento de los consumidores, así como la correcta gobernanza de los datos, eliminando o mitigando así los sesgos de los datos utilizados.

Por otro lado, y respecto a la equidad sustantiva, las empresas aseguradoras deben valorar la distribución justa de los beneficios y los costes derivados del uso de la IA, debiendo tener en cuenta el impacto que el uso de los sistemas de IA puede tener en los grupos de consumidores vulnerables, así como en la accesibilidad de ciertas líneas de negocio que son importantes para la inclusión financiera.

Esta última cuestión adquiere importancia, pues determinados productos de seguros son especialmente relevantes para la inclusión financiera y social, lo que implica que su acceso por parte de la población no debería quedar limitado u obstaculizado como consecuencia del uso de sistemas de IA.

Entre los productos que deben ser objeto de una mayor supervisión humana, debido a su importancia social, se destacan los siguientes: seguro del vehículo, seguro médico, seguro del hogar, seguro de responsabilidad civil, seguro de vida y seguro de indemnización de los trabajadores.

Si bien no se pretende prohibir el uso de sistemas de IA en el marco de los citados productos, estos deben disponer de medidas complementarias, como la supervisión humana y una correcta gobernanza de datos, que garanticen una correcta accesibilidad por todos los sectores de la población.

En cuanto a la no discriminación, resulta necesario que las empresas aseguradoras atiendan especialmente a los datos y modelos de IA utilizados. Independientemente de si el sistema de IA implementado ha sido desarrollado internamente por la empresa o ha sido contratado a un tercero, la empresa aseguradora debe garantizar que:

- Se han detectado y eliminado los sesgos, errores, imprecisiones o equivocaciones en los datos utilizados para entrenar el sistema de IA.

– Se han detectado y mitigado las correlaciones no deseadas, dado que los sistemas de IA utilizados funcionan, en su mayoría, mediante la identificación de patrones en los datos, utilizando posteriormente estos patrones para hacer predicciones para nuevos datos.

En este sentido, se propone la restricción en el uso de ciertos tipos de indicadores para la toma de decisiones, a menos que su uso esté objetivamente justificado por una finalidad legítima y sea adecuado y necesario. Entre estos indicadores destacan: el género de las personas, la orientación sexual, las creencias religiosas, la nacionalidad y/o la edad, entre otros.

En la práctica, el uso de sistemas de IA para resolver sobre la contratación de ciertos productos del mercado de los seguros obliga a las empresas aseguradoras a evaluar y desarrollar medidas para mitigar el impacto que pueden tener variables como la calificación crediticia, la ubicación, los ingresos, la ocupación o el nivel de educación.

2. *Transparencia y explicabilidad*

Aunque son términos interrelacionados, que abordan el tipo de información sobre un sistema de IA que debe proporcionarse a las distintas partes interesadas, debe distinguirse ambos conceptos:

– La transparencia supone el suministro de información sobre el uso, la naturaleza o el diseño de un sistema de IA, así como las variables y parámetros de datos utilizados.

– La explicabilidad implica la capacidad de explicar a un tercero el resultado arrojado por el sistema de IA, especialmente en lo referente al peso, la influencia y la relación causal de una o varias variables en el resultado final.

Dado que la normativa impone a las empresas del sector asegurador la obligación de proporcionar al cliente información objetiva sobre el producto de seguro de forma comprensible para que pueda tomar una decisión informada, así como informar a los consumidores de forma oportuna, adecuada

y transparente sobre el tratamiento de sus datos personales, adquiere especial importancia el cumplimiento de las obligaciones en materia de transparencia y explicabilidad.

Respecto a la explicabilidad, el informe hace especial hincapié en la necesidad de adaptar el contenido y detalle de esta en función del destinatario, diferenciando entre consumidores, auditores, supervisores y los propios órganos de gobierno internos.

Mientras que en la información proporcionada a los consumidores debe primar la facilidad de la comprensión y la claridad, la proporcionada a los supervisores y auditores debe caracterizarse por su exhaustividad y detalle.

Por otro lado, la transparencia debe orientarse a garantizar un correcto conocimiento del sistema de IA utilizado, proporcionando información sobre el uso o no de sistemas de IA y, en caso afirmativo, sobre los datos utilizados.

Uno de los supuestos prácticos en los que más relevancia adquiere la transparencia y la explicabilidad en el uso del sistema de IA es el cálculo de la prima que deberá abonarse, siendo necesario poder establecer varios niveles de explicación sobre los principios en los que se basa el modelo y los principales factores de calificación que influyen en el cálculo de la prima.

3. *Supervisión humana*

Debido a las distintas partes que conforma el ciclo de vida de los sistemas de IA, así como su implementación y uso, resulta vital asignar y documentar las personas/departamentos internos y/o terceros que participan, así como sus funciones y responsabilidades.

En este sentido, adquieren especial importancia los roles relativos a la revisión de la propia actuación del sistema de IA, siendo deseable un equilibrio adecuado de la colaboración entre el personal humano y el sistema de IA para determinadas tareas, teniendo en cuenta la existencia de diferentes niveles de supervisión humana.

Uno de los supuestos prácticos en los que más relevancia adquiere la supervisión humana es la relativa al uso de sistemas de IA para resolver las reclamaciones presentadas por los consumidores, debiendo distinguir entre aquellas reclamaciones que tiene un menor impacto (requerirán menor supervisión humana) de las de mayor impacto (requerirán mayor supervisión humana). A la hora de evaluar si un siniestro tiene un impacto significativo en los consumidores, las aseguradoras deben considerar tanto los factores financieros como los no financieros.

4. *Gobernanza de los datos y mantenimiento de registros*

Debido a la importancia de los datos durante todo el ciclo de vida de los sistemas de IA, así como a la existencia de una regulación proteccionista en el tratamiento de los datos de carácter personal, debe implementarse una gobernanza de datos sólida.

Las empresas de seguros deben garantizar que los datos utilizados en los sistemas de IA sean precisos, completos y adecuados, garantizando que se almacenan en un entorno seguro y protegido, así como mantener registros apropiados de los procesos de tratamiento y gestión de estos.

La gobernanza de los datos debe articularse en tres fases, en función del ciclo de vida de los datos utilizados en los sistemas de IA:

- *Recogida.* Durante la fase de recopilación de datos, las empresas de seguros deben seleccionar cuidadosamente los tipos y las fuentes de datos que son adecuados para la tarea específica que desarrollará el sistema de IA.

- *Preparación.* Durante la fase de procesamiento de los datos, que tiene como finalidad garantizar que los datos sean precisos, completos y adecuados, las empresas de seguros deben eliminar los posibles sesgos de los datos de entrenamiento.

- *Posprocesamiento.* Durante el uso del sistema de IA, las empresas de seguros deben prestar especial atención a los nuevos tipos de datos que

puedan utilizarse, siendo importante que los mismos sean verificados y, en caso de ser necesario, corregidos.

Sin perjuicio de lo anterior, y en caso de externalizarse alguna o todas las fases referidas previamente (p. ej., mediante la contratación de un sistema de IA como servicio ofertado por un tercero), la empresa aseguradora es responsable de comprobar que el tercero cumple con una correcta gobernanza de los datos y mantenimiento de registros.

Adicionalmente, y especialmente relacionado con la transparencia y la explicabilidad, las empresas aseguradoras deben conservar los registros pertinentes de los datos utilizados, así como las metodologías de modelización, lo que permitirá: 1) rastrear las decisiones y verificarlas en caso de que pudieran ser eventualmente impugnadas y 2) evitar el mal uso de los modelos por falta de atención.

En el caso de usos de sistemas de IA para el cálculo de las primas que deberán abonarse, adquiere especial importancia la necesidad de garantizar la calidad, imparcialidad y actualización de los datos, evitando así posibles cálculos no adecuados a la verdadera realidad del consumidor.

5. *Robustez y rendimiento*

Desde una perspectiva esencialmente técnica, los sistemas de IA utilizados por las empresas del sector asegurador deben garantizar que los mismos son seguros (robustez) y ofrecen resultados precisos (rendimiento).

Independientemente de si el sistema de IA ha sido desarrollado y desplegado en su totalidad por la propia entidad aseguradora o si el mismo ha sido desarrollado por un tercero, debe garantizarse el rendimiento y seguridad de este, pues las empresas de seguros son las responsables últimas de las aplicaciones de IA que utilizan.

Debido al contexto principalmente digital en el que se desarrolla la IA, las empresas aseguradoras deben garantizar que los sistemas de IA utilizados son seguros, tanto desde una perspectiva de ser objeto de ataques, que podrían

implicar fallos en su uso o modificaciones en su funcionamiento (debiendo introducir así los conocidos como *fall-back plans* o planes de emergencia), como desde una perspectiva de sus efectos para con terceros.

Respecto al rendimiento de los sistemas de IA, es decir, la capacidad de hacer predicciones correctas y precisas, y aunque siempre existe el riesgo de que existan errores, son muchas las variables que deben valorarse antes del desarrollo o contratación de un sistema de IA, con la finalidad de reducir el riesgo de error lo máximo posible:

- La correcta definición de la tarea y finalidades previstas para el uso de la IA.

- La evaluación de las métricas de rendimiento (p. ej., exactitud, recuperación, precisión, etc.), que dependerán de la naturaleza de los datos utilizados y de la aplicación prevista del concreto sistema de IA.

- La adecuada gobernanza de los datos, que permitirán el correcto rendimiento del sistema de IA, debiendo atender a la integridad y precisión de los datos, así como su adecuación al objetivo marcado.

- Las medidas internas dispuestas para que los sistemas de IA sean reentrenados, recalibrados y revalidados periódicamente.

En la práctica, concretamente en el uso de sistemas de IA para el acceso a productos de seguro y el cálculo de las primas, el correcto rendimiento del modelo dependerá de los datos disponibles, debiendo evitarse su uso en el marco de riesgos sujetos a una gran incertidumbre, pues generalmente darán lugar a modelos menos precisos. En este sentido, y respecto a los productos que cubran riesgos con mayor incertidumbre, se recomienda identificar las principales fuentes de incertidumbre, con el fin de evaluar las medidas que pueden adoptarse para reducir dicha incertidumbre, si es posible, y la posible mejora del rendimiento del modelo.

En definitiva, y debido al importante papel que se espera que desempeñe la IA en la configuración del futuro digital de las sociedades y economías europeas,

incluido el sector del seguro, las empresas que desarrollan su actividad en este sector deben aplicar medidas de gobernanza adecuadas a lo largo de todo el ciclo de vida del sistema de IA, habiendo evaluado previamente y de forma proporcional el impacto derivado del uso de la IA, para cada supuesto concreto, con el fin de aplicar posteriormente una combinación de las medidas necesarias (técnicas y no técnicas) para garantizar que cada sistema de IA utilizado es fiable.

4.3.3. Artificial intelligence: from ethics to policy (Parlamento Europeo) y The Assessment List for Trustworthy Artificial Intelligence (HLEG)

Durante la primera mitad del año 2020 se emitieron varios informes, entre los que destacan dos relativos a la puesta en práctica de los principios éticos y requisitos referidos en el informe publicado en el año 2019.

En primer lugar, el Parlamento Europeo publicó, en junio de 2020, el informe "Artificial intelligence: from ethics to policy"[34], en el que se proponen una serie de instrumentos que permiten dar respuesta a las dudas sobre la puesta en práctica de la ética de la IA. Concretamente, se propone la imposición de alguna de las siguientes alternativas:

- *Certificado de limpieza de datos o DHC (Data Hygiene Certificate)*. Dado que la calidad de los datos desempeña un papel fundamental en la eficacia y la precisión de un algoritmo, se plantea la posibilidad de exigir a todos los desarrolladores de sistemas de IA que pretendan vender sus soluciones a las instituciones públicas que dispongan de un certificado de higiene de datos.

- *Evaluación ética de la tecnología o eTA (Ethical Technology Assessment)*. Con el objetivo de garantizar el principio de transparencia y seguridad, se propone la redacción de un documento en el que se registren los posibles riesgos éticos que podrían derivarse de la aplicación de la IA en cuestión.

- *Informe de responsabilidad o AR (Accountability Report)*. Tras la elaboración de la eTA, y con el objetivo de dar respuesta a su resultado, se propone que la

[34] PE 641.507.

institución o empresa que pretenda desplegar sistemas de IA elabore un informe de responsabilidad en el que deje constancia las medidas que se han adoptado para mitigar o corregir las preocupaciones planteadas en la eTA.

Además, y como herramienta adicional, se propone que, previamente al uso de la IA por parte de una institución o empresa, esta deberá haber concretado los objetivos de forma clara y determinada, evitando así el uso de herramientas de IA con una finalidad "exploradora".

En definitiva, los instrumentos planteados previamente se centran en el análisis de las consideraciones éticas relevantes para la IA, permitiendo crear procedimientos sistemáticos para documentar las evaluaciones éticas, trazando un camino hacia la rendición de cuentas y, en consecuencia, al cumplimiento de los principios y directrices de la UE.

En segundo lugar, el HLEG publicó, en julio de 2020, el informe "The Assessment List for Trustworthy Artificial Intelligence (ALTAI)", en el que se recoge la lista de evaluación de la IAF, con la finalidad de ofrecer a las organizaciones un medio para poder autoevaluar el cumplimiento de las directrices y requisitos recogidos en el informe *Ethics guidelines for trustworthy AI,* publicado en el año 2019 por el citado grupo de expertos.

Para cada requisito se ofrece una orientación introductoria y las definiciones pertinentes a través de un glosario, así como las preguntas que deben plantearse para poder analizar y resolver si se cumplen los citados requisitos y, en consecuencia, con los principios éticos.

Mediante el ALTAI se facilita que los operadores puedan autoevaluar si cumplen con uno de los tres requisitos exigibles para un sistema de IAF: el marco ético.

4.3.4. Libro Blanco sobre la inteligencia artificial (Comisión Europea)

Saltando de la vertiente ética a la vertiente regulatoria, en febrero del año 2020 se publicó el tan esperado *Libro Blanco sobre la inteligencia artificial* (*White Paper on AI),* en el que se establecían las principales líneas de actuación de la UE en materia

de IA, así como, entre otros, los elementos clave para la elaboración de un futuro marco regulatorio específico sobre la IA.

En el *Libro Blanco sobre la inteligencia artificial* se destaca que la UE cuenta con un marco jurídico estricto para garantizar, entre otros, la protección de los consumidores, la lucha contra las prácticas comerciales desleales y la protección de los datos personales y la privacidad, pero puede que se requieran algunas actualizaciones mediante: 1) la reforma de las normas actualmente vigentes en la UE, a fin de reflejar la transformación digital y el uso de la IA, y 2) el desarrollo y aprobación de un nuevo marco regulador específico en materia de IA.

Respecto a la responsabilidad en el ámbito de la IA, principal elemento de interés, el *Libro Blanco sobre la inteligencia artificial* distingue dos tipos de responsabilidad, en función de la calificación del sistema de IA sobre la base del riesgo que genera:

- Sistemas de IA de alto riesgo *(high-risk).*

- Resto de sistemas de IA *(all other systems).*

En el *Libro Blanco sobre la inteligencia artificial* se establece que, en general, un sistema IA debe considerarse de alto riesgo cuando, en función de un doble criterio (sector y uso), supone un riesgo significativo, en especial desde la perspectiva de la protección de la seguridad, los derechos de los consumidores y los derechos fundamentales.

- *Sector:* debe valorarse si, por las características o actividades que se llevan a cabo normalmente, es previsible que existan riesgos significativos. Este criterio vela por que la intervención reguladora se centre en aquellas áreas en las que, de manera general, se considere que hay más probabilidad de que surjan riesgos.

- *Uso:* debe valorarse, adicionalmente, si el uso del sistema de IA puede generar riesgos significativos.

Ambos requisitos deben concurrir de forma cumulativa, es decir, el sistema de IA debe desplegarse en un sector que, por sus características, sea considerado de alto riesgo y, adicionalmente, su uso del sistema de IA también sea considerado de alto riesgo. En consecuencia, no por el hecho de desplegarse en un sector de alto riesgo debe ser considerado un sistema de IA como de alto riesgo, pues el uso desplegado puede no implicar un riesgo significativo.

Sin perjuicio de lo referido previamente, el *Libro Blanco sobre la inteligencia artificial* también establece que existen ciertos usos que, si bien no se encuentran en sectores de alto riesgo, el uso es suficiente para la clasificación del sistema de IA como de alto riesgo. En este sentido, destaca el uso del sistema de IA para la identificación biométrica y otros usos de vigilancia intrusiva.

Cabe destacar que en el mismo se indica que la consideración de un sistema de IA como de alto riesgo no quedará supeditado a la valoración de la entidad que haga uso de este, siendo competencia de las instituciones de la UE establecer qué sectores y usos serán considerados de alto riesgo.

Catalogar un sistema de IA como de alto riesgo o no tiene –como se verá en el desarrollo que se hará de las recomendaciones y propuestas– un alto impacto para la empresa que haga uso del sistema, especialmente en lo referente a las obligaciones que deberá cumplir, así como en la responsabilidad que deberá asumir.

4.3.5. Propuesta de Reglamento por el que se establecen normas armonizadas sobre la inteligencia artificial (Comisión Europea)

De entre todas las propuestas[35], la propuesta de reglamento[36] publicada el pasado 21 de abril de 2021 y que, a fecha de redacción del presente análisis, se erige como una de las iniciativas normativas más destacadas a nivel europeo en materia de IA

[35] El 20 de octubre de 2020, el Parlamento Europeo emitió varias resoluciones con recomendaciones destinadas a la Comisión Europea, relativas a tres ámbitos de la IA: marco de los aspectos éticos de la IA, la robótica y las tecnologías conexas; régimen de responsabilidad civil en materia de IA; y derechos de propiedad intelectual para el desarrollo de las tecnologías relativas a la IA.

[36] COM (2021) 206 final.

es la Propuesta de Reglamento por el que se establecen normas armonizadas sobre la inteligencia artificial *(Artificial Intelligence Act)*.

A través de la propuesta referida previamente se pretende armonizar y mejorar el funcionamiento del mercado interior en el marco de la IA, mediante el establecimiento de un marco jurídico uniforme, en particular para el desarrollo, la comercialización y la utilización de la IA de conformidad con los valores de la UE.

Para el cumplimiento de esta finalidad, la propuesta aborda una gran variedad de cuestiones relacionadas con la IA, pudiendo resumirlas, conforme al contenido de los distintos títulos y capítulos que componen la propuesta, en las siguientes principales materias:

1. Exponer la clasificación de los distintos sistemas de IA en función de sus características y usos: a) sistemas de IA prohibidos; b) sistemas de IA de alto riesgo; c) sistemas de IA de riesgo limitado, y d) sistemas de IA de riesgo mínimo o nulo.

2. Establecer los requisitos que deben cumplir los sistemas de IA de alto riesgo, así como los procedimientos de evaluación, certificación y registro que deben seguirse para su válida comercialización.

3. Regular las autoridades europeas y nacionales de supervisión en materia de IA.

4. Fijar las obligaciones que deberán cumplir los distintos operadores de sistemas de IA de alto riesgo.

5. Favorecer la creación de un marco jurídico favorable a la innovación en el marco de la IA.

Con carácter previo cabe destacar el amplio ámbito de aplicación del futuro reglamento pues, en caso de no sufrir modificación, será de aplicación a todo aquel sujeto que comercialice o ponga en servicio sistemas de IA en la UE, con independencia de que esté establecido en un tercer país, así como a todos los sistemas de IA que se utilicen en la UE, independientemente de su origen.

Respecto a la primera de las materias, del contenido del articulado se extrae la existencia de cinco tipos de sistemas de IA, en función del mayor o menor riesgo que sus características y uso implican para los valores de la UE y la sociedad:

- *Sistemas de IA prohibidos.* El artículo 5 de la propuesta recoge aquellos sistemas de IA que, debido a sus características y usos, se prohíbe su desarrollo, despliegue y comercialización, dado que contravienen los valores de la UE e implican un grave riesgo para los ciudadanos.

  En esta categoría se encuentran, entre otros, aquellos sistemas de IA que manipulen el comportamiento humano para condicionar la voluntad de los usuarios y los sistemas que permitan llevar cabo una puntuación social del ciudadano.

  Cabe destacar que la prohibición referida previamente no es absoluta, pues el uso de sistemas de identificación biométrica remota en tiempo real y en espacios de acceso público sí que se permite, siempre que sea estrictamente necesario para alcanzar uno o varios de los objetivos referidos en el propio artículo como, por ejemplo, la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de un atentado terrorista.

  Adicionalmente, el uso de sistemas de IA con el fin de evaluar o clasificar la fiabilidad de personas físicas atendiendo a su conducta social o a características personales solo estará prohibido si implica, entre otras consecuencias, un trato perjudicial o desfavorable en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente.

- *Sistemas de IA de alto riesgo.* Los artículos 6 y 7, así como el anexo III de la propuesta, recogen aquellos sistemas de IA considerados de alto riesgo y, en consecuencia, sujetos al cumplimiento de todos los requisitos y procedimientos de evaluación destinados a garantizar el cumplimiento de los mismos.

  En esta categoría se encuentran, entre otros, aquellos sistemas de IA destinados a evaluar el acceso y disfrute de los servicios privados esenciales y de

los servicios y prestaciones públicas, así como la gestión de infraestructuras críticas y la administración de justicia.

En este sentido cabe destacar que los sistemas de IA referidos expresamente como sistemas de IA de alto riesgo en el anexo III de la propuesta pueden ser objeto de modificación por parte de las instituciones de la UE, es decir, la Comisión Europea estaría facultada para adoptar actos delegados y actualizar la lista de sistemas de IA de alto riesgo referidos en el anexo III, cuando se cumplan las dos condiciones siguientes:

- el sistema de IA esté destinado a utilizarse en cualquiera de los ámbitos enumerados en los puntos 1 a 8 del anexo III; y

- el sistema de IA implique un riesgo de daño para la salud y la seguridad o un riesgo de impacto adverso en los derechos fundamentales, que, conforme a su gravedad y probabilidad de materializarse, sea equivalente o mayor al riesgo de daño o de impacto adverso planteado por los sistemas de IA de alto riesgo ya mencionados en el anexo III.

- *Sistemas de IA de riesgo limitado.* El artículo 52 de la propuesta recoge aquellos sistemas de IA que, independientemente de si tienen la consideración o no de sistemas de IA de alto riesgo, deben cumplir una serie de obligaciones mínimas en materia de transparencia. En esta categoría se encuentran aquellos sistemas de IA destinados a la interacción con las personas, la manipulación de imágenes, audios o vídeos *(Deepfake)* o el reconocimiento emocional, entre otros.

- *Sistemas de IA de riesgo mínimo o nulo.* En esta categoría se encuentran todos los sistemas de IA que, por sus características o usos, no se puedan incluir en las categorías referidas previamente.

En segundo lugar, y erigiéndose como una de las principales cuestiones abordadas por la propuesta, cabe destacar que la mayor parte de esta se centra en la regulación de los sistemas de IA de alto riesgo, estableciendo: a) los requisitos que deben cumplirse para la correcta comercialización y uso de los sistemas de IA

de alto riesgo; b) los procedimientos de evaluación de conformidad, certificación y registro de los sistemas de IA de alto riesgo, y c) las obligaciones que asumen los operadores de los citados sistemas de IA.

A. Requisitos que deben cumplir los sistemas de IA de alto riesgo

Todos los sistemas de IA de alto riesgo deberán cumplir, antes de su distribución y comercialización en el mercado de la UE, todos los requisitos referidos en el capítulo 2 del título III. Sin perjuicio del contenido de estos, los requisitos que deberán cumplir los sistemas de IA de alto riesgo son:

Requisito	Contenido
Sistema de gestión de riesgos *(Risk Management System)*	Se establecerá, aplicará, documentará y mantendrá un sistema de gestión de riesgos con la finalidad de determinar los riesgos asociados al sistema de IA y, en consecuencia, las medidas que se adoptarán para eliminarlos o reducirlos, en la medida de lo posible, así como la aplicación de las medidas adecuadas para mitigarlos e informar a los usuarios.
Gobernanza de los datos *(Data Governance)*	El entrenamiento de modelos con datos se desarrollará sobre la base de conjuntos de datos de entrenamiento, validación y prueba que cumplan con una serie de criterios de calidad.
Registro de eventos *(Record Keeping)*	Los sistemas de IA de alto riesgo se diseñarán y desarrollarán con capacidades que permitan el registro automático de eventos durante su funcionamiento, consiguiendo así disponer de datos para garantizar un nivel mínimo de trazabilidad del funcionamiento del sistema de IA a lo largo de su ciclo de vida.
Transparencia y suministro de información a los usuarios	Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de forma que: 1) se garantice que los usuarios puedan interpretar los resultados del sistema y utilizarlos adecuadamente y 2) vayan acompañados de instrucciones de uso que incluyan información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para los usuarios.
Supervisión humana *(Human Oversight)*	Los sistemas de IA de alto riesgo se diseñarán y desarrollarán con herramientas adecuadas de interfaz hombre-máquina que permitan la supervisión por personas físicas durante el funcionamiento del sistema de IA para prevenir o reducir al mínimo los riesgos que puedan surgir.

Continúa

Requisito	Contenido
Precisión, solidez y ciberseguridad	Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de manera que alcancen, a la luz de su finalidad prevista, un nivel adecuado de: 1) precisión, 2) solidez (resistentes en lo que respecta a los errores, fallos y/o incoherencias) y 3) ciberseguridad (resistentes a los intentos de terceros no autorizados de alterar su uso o rendimiento aprovechando las vulnerabilidades del sistema).
Documentación técnica	La documentación técnica se elaborará de forma que demuestre que el sistema de IA de alto riesgo cumple con los requisitos establecidos previamente, de tal forma que proporcione a las autoridades nacionales y a los organismos europeos toda la información necesaria para evaluar la conformidad del sistema de IA.

Cabe destacar que la propuesta recoge una serie de presunciones respecto al cumplimiento de los citados requisitos, concretamente, se presume el cumplimiento total o parcial de los requisitos referidos previamente cuando se acredite que los sistemas de IA de alto riesgo son conformes a determinadas normas como, por ejemplo: el Reglamento (UE) 2019/881 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación o la Directiva 2009/48/CE sobre la seguridad de los juguetes, entre otras.

B. Procedimiento de evaluación, certificación y registro de los sistemas de IA de alto riesgo

Los requisitos referidos previamente no solo deben ser objeto de cumplimiento, sino también de acreditación ante las autoridades competentes. En este sentido, y aunque la propuesta establece un procedimiento de desarrollo y despliegue homogéneo y armonizado de los sistemas de IA de alto riesgo, divide estos en dos tipos, en función de: si los requisitos referidos previamente deben ser objeto de acreditación ante la autoridad competente antes de la distribución y comercialización del sistema de IA o, por el contrario, si deben ser objeto de acreditación solo cuando sea requerido por las autoridades de control competentes.

- *Sistemas de IA enumerados en el punto 1 del anexo III:* el proveedor deberá seguir uno de los dos siguientes procedimientos:

  – Procedimiento de evaluación interno de conformidad con el anexo VI, que no prevé la intervención previa de un organismo control.

  – Procedimiento de evaluación externo de conformidad con el anexo VII, que prevé la participación de un organismo de control. En estos casos, la superación de la evaluación supondrá la obtención del pertinente certificado.

- *Sistemas de IA enumerados en los puntos 2 a 8 del anexo III.* El proveedor seguirá el procedimiento de evaluación de la conformidad basado en el control interno al que se refiere el anexo VI, que no prevé la participación de un organismo de control.

Sin perjuicio de las especialidades recogidas en la propuesta respecto a la evaluación de conformidad de los distintos sistemas de IA de alto riesgo, cabe destacar que la Comisión Europea se encuentra facultada para adoptar actos delegados destinados a: 1) introducir nuevos elementos en los procedimientos de evaluación de conformidad que resulten necesarios a la luz del progreso técnico y 2) modificar los sistemas de IA de alto riesgo que quedan sometidos a los procedimientos de evaluación de la conformidad recogidos en los anexos VI y VII.

Una vez cumplidos internamente los requisitos referidos previamente en el apartado A (sistemas de IA sometidos al procedimiento del anexo VI) o una vez obtenida la certificación que acredite el cumplimiento de los citados requisitos (sistemas de IA sometidos al procedimiento del anexo VII), y con carácter previo a la comercialización, el proveedor deberá: 1) elaborar una declaración de conformidad de la UE; 2) colocar la marca de conformidad CE en el sistema de IA, y 3) registrar el sistema de IA en la base de datos de la UE.

Por otro lado, y respecto de aquellos sistemas de IA no considerados de alto riesgo, la propuesta pretende promover y facilitar la elaboración de códigos de conducta destinados a fomentar la aplicación de los requisitos establecidos para los sistemas de IA de alto riesgo sobre la base de especificaciones técnicas y soluciones

que sean medios adecuados para garantizar el cumplimiento de dichos requisitos a la luz de la finalidad prevista de los sistemas de IA concretos.

C. Obligaciones asumidas por los operadores de los sistemas de IA de alto riesgo y régimen sancionador

Lo que sin duda adquiere una especial importancia en la propuesta es la profundidad con la que regula los sujetos intervinientes durante el ciclo de vida de los sistemas de IA, así como las obligaciones que asume cada uno de ellos.

Este análisis no se expone desde una perspectiva meramente teórica, pues la propia propuesta recoge un régimen sancionador aplicable a aquellos sujetos que incumplan las obligaciones impuestas en el futuro reglamento y cuyos importes oscilan entre los 10.000.000 euros o un 2 % del volumen de negocios anual a nivel mundial del ejercicio anterior y los 30.000.000 euros o un 6 % del volumen de negocios anual a nivel mundial del ejercicio anterior.

Como consecuencia directa del impacto económico que podría tener el incumplimiento de las obligaciones que se impongan en la futura regulación, adquiere especial importancia analizar los distintos sujetos que asumen obligaciones respecto de los sistemas de IA, así como las obligaciones que asumen. En este sentido, la propuesta identifica a los siguientes sujetos:

a. *Proveedor:* bajo este término se engloba a toda persona física o jurídica, de carácter público o privado, que desarrolle un sistema de IA o que haga desarrollar un sistema de IA con el fin de comercializarlo o ponerlo en servicio bajo su propio nombre o marca, ya sea a cambio de una remuneración o de forma gratuita. Adicionalmente, la propuesta distingue una subcategoría de proveedores, en función de su tamaño: los proveedores de pequeña escala *(small scale provider).*

b. *Representante autorizado:* toda persona física o jurídica establecida en la UE que haya recibido un mandato escrito de un proveedor de un sistema de IA para, respectivamente, cumplir y ejecutar en su nombre las obligaciones y procedimientos establecidas en el futuro reglamento.

c. *Importador:* toda persona física o jurídica que, establecida en la UE, comercialice o ponga en servicio un sistema de IA que lleve el nombre o la marca de una persona física o jurídica establecida fuera de la UE.

d. *Distribuidor:* toda persona física o jurídica de la cadena de suministro, distinta del proveedor o del importador, que comercialice un sistema de IA en el mercado de la UE sin afectar a sus propiedades.

e. *Usuario:* toda persona física o jurídica, de carácter público o privado, que utilice un sistema de IA bajo su autoridad, excepto cuando el sistema de IA se utilice en el curso de una actividad personal no profesional.

f. *Operador:* término común para referirse al proveedor, el usuario, el representante autorizado, el importador y/o el distribuidor.

Cada uno de los operadores referidos previamente asume una serie de obligaciones respecto del sistema de IA objeto de desarrollo, distribución, comercialización y uso, siendo que las obligaciones de los sujetos situados en las posiciones finales de la cadena se encuentran orientadas, fundamentalmente, a asegurar que los anteriores operadores han cumplido con sus obligaciones.

En primer lugar, el operador que más obligaciones asume es el *proveedor,* pues es el encargado de garantizar que el sistema de IA cumple con todos los requisitos y que ha obtenido todos los permisos y autorizaciones necesarias; además, el proveedor confecciona toda la documentación exigida por la normativa y adopta las medidas correctoras necesarias si el sistema de IA de alto riesgo no se ajustara a los requisitos de forma sobrevenida, entre otros.

En segundo lugar, para aquellos casos en los que el proveedor no se encuentre en la UE, pero distribuya o comercialice sistemas de IA en el mercado de la UE, emergen dos operadores adicionales:

- *Representantes autorizados:* sus principales obligaciones están relacionadas con la colaboración y comunicación con las autoridades europeas y nacionales

competentes, así como disponer de copias de la documentación e información exigida por la normativa de la UE respecto de los sistemas de IA.

- *Importadores:* con carácter previo a la importación del sistema de IA deberán asegurar que el proveedor de dicho sistema de IA ha llevado a cabo el procedimiento de evaluación de la conformidad adecuado, dispone de la documentación técnica exigida, el sistema lleva el marcado de conformidad exigido y dispone de las instrucciones de uso requeridas.

En tercer lugar, los *distribuidores* deberán verificar, antes de la comercialización de los sistemas de IA, que el sistema dispone del marcado de conformidad CE requerido, de la documentación y las instrucciones de uso necesarias y que el proveedor y/o el importador del sistema, según proceda, han cumplido sus obligaciones formales y materiales.

En cuarto lugar, los *usuarios* deberán garantizar que el uso de los sistemas de IA se realiza de acuerdo con las instrucciones de uso, sin perjuicio de otras obligaciones impuestas por legislación de la UE o nacional, así como de la discrecionalidad del usuario a la hora de organizar sus propios recursos y actividades para aplicar las medidas de supervisión humana indicadas por el proveedor.

Cabe destacar en este punto que, si bien los operadores se encuentran correctamente delimitados en la propuesta, cualquier operador podrá ser considerado proveedor y, en consecuencia, estará sujeto a las obligaciones de los proveedores si concurren alguna de las siguientes circunstancias: 1) que comercialice o ponga en servicio un sistema de IA de alto riesgo con su nombre o marca comercial; 2) que modifique la finalidad prevista de un sistema de IA de alto riesgo ya comercializado o puesto en servicio, y/o 3) que realice una modificación sustancial del sistema de IA de alto riesgo.

En conclusión, y teniendo en cuenta los distintos roles analizados previamente, cabe destacar que adquiere especial importante la determinación del papel que la aseguradora asume frente al sistema de IA objeto de análisis, adquiriendo obligaciones de muy diversa categoría y, en consecuencia, quedando sometida a un

régimen de obligaciones distinto que desembocaría, en caso de incumplimiento, en la posible aplicación del régimen sancionador.

4.4. LOS RIESGOS DE CUMPLIMIENTO EN PROTECCIÓN DE DATOS PERSONALES

4.4.1. Tratamientos como responsable o encargado en el ciclo de vida de un sistema de IA

Tras exponer las distintas fases del ciclo de vida, cada una de ellas consiste en un proceso ejecutado en un macroproceso que los engloba, siendo el macroproceso el servicio prestado por el sistema de IA. En el caso de que, durante la ejecución del proceso, se tratasen datos personales, en cualquiera de sus formas, estaríamos ante una actividad de tratamiento de datos personales.

Las actividades de tratamiento son atribuidas siempre al responsable de este, que será quien determine la finalidad y los medios con los que se efectúa el tratamiento; sin embargo, si el responsable decide contratar a terceras partes para el desarrollo del sistema, estas pueden convertirse en encargados del tratamiento, cuyo rol se adquiere cuando el responsable subcontrata parte del proceso de tratamiento a un tercero. Es decir, si un responsable encarga a un tercero la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción[37], este se convertirá en encargado del tratamiento.

Pero esta condición depende, a su vez, de la prestación del servicio pactado. Si el servicio está totalmente externalizado, es posible que la organización cliente y usuaria de la solución solo sea responsable de la finalidad para la cual ha sido contratada, siendo el responsable de todos los tratamientos de las fases del ciclo de vida la entidad prestadora del servicio.

[37] *Vid*. Artículo 4. 2) del RGPD.

Una vez determinado el responsable del tratamiento, este tiene la obligación de ser diligente en la elección de las soluciones más adecuadas y del proveedor de la solución, de acuerdo con el artículo 28 del RGPD respecto a las obligaciones de contratación con el encargado del tratamiento y con el principio de responsabilidad activa del artículo 5.2 del RGPD.

Además, la AEPD ha emitido una serie de responsabilidades asociadas a los roles existentes en cada fase del ciclo de vida[38]:

Etapa	Responsable	Encargado
Desarrollo/ entrenamiento	La entidad que defina los fines del componente IA y decida qué datos se van a emplear para entrenar el sistema. En caso de que se contrate el desarrollo a un tercero, pero este tercero tome las decisiones sobre los datos personales utilizados para entrenar al componente IA para sus propios fines, será considerado responsable la entidad contratada. En el caso de que aquel que defina los fines adquiera un conjunto de datos personales será responsable de tratamiento.	La entidad contratada para entrenamiento o desarrollo, siempre y cuando el contratante fije los términos que definen los fines del tratamiento y las características sustanciales de los datos, tanto si el contratante es quien cede dichos datos como si los obtiene por sí mismo el contratado, y el encargado los utilice solo para cumplir con los fines del responsable.
Validación	Igual que en el caso anterior.	Igual que en el caso anterior.

Continúa

[38] *Vid*. AEPD, *Adecuación al RGPD de tratamientos que incorporan inteligencia artificial. Una introducción,* p. 19.

Etapa	Responsable	Encargado
Despliegue	En el caso de que la solución IA es un componente que se vende a otra entidad (podría ser formando parte de tratamiento), y ese componente incluye datos de carácter personal, ambas entidades realizan una comunicación de datos personales y ambas son responsables. Si la comercialización tiene como objeto la venta de un producto que incluya un componente de IA a una persona física para su uso particular, aunque el modelo incluya datos de carácter personal, aplicará la excepción doméstica, salvo que realice un tratamiento para sus propios fines de los datos personales incluidos, en cuyo caso también será considerado responsable.	La entidad que pone un modelo al servicio de un responsable para que lo explote en un marco de prestación de servicios sin intervenir en esa explotación o que, en caso de hacerlo porque sea necesario para la adecuada ejecución de ese servicio, no utiliza los datos personales para fines propios.
Inferencia/ perfilado	La entidad que decide tratar los datos de los interesados con el sistema IA para sus propios fines. Si el tratamiento lo realiza una persona física sobre sus propios datos personales o de aquellas personas en su entorno para una actividad exclusivamente personal o doméstica, se aplicará la excepción doméstica. Esta excepción no aplica a aquellos que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas para sus propios fines.	Igual que en el caso anterior.
Decisión	La entidad que tome decisiones automatizadas sobre los interesados para sus propios fines.	Igual que en el caso anterior.

Continúa

Etapa	Responsable	Encargado
Evolución	La entidad que decide tratar los datos de los interesados con el sistema IA, si comunica a una tercera entidad los datos de los usuarios, será responsable de la comunicación de datos si no existe una relación de responsable-encargado. La entidad que determina la evolución del componente IA en base a los datos de los usuarios, tanto si los datos son cedidos directamente por los interesados como por la entidad que les proporciona servicio, es responsable de dicho tratamiento de evolución o reentrenamiento.	En el caso de que la entidad que decide tratar los datos de los interesados contrate el tratamiento IA a un tercero, dicho tercero actuará como encargado de tratamiento, siempre que no los trate para sus propios fines.

Fuente: elaboración propia.

4.4.2. Principio de licitud

Siempre que se vaya a emprender una actividad de tratamiento, debe configurarse una base legal de legitimación estipulada en el artículo 6 del RGPD. Este requisito consistirá en el primer riesgo de cumplimiento que la solución de IA genera en materia de protección de datos.

Podemos destacar la existencia de las siguientes actividades de tratamiento que suceden en el desarrollo de un sistema de IA, para los cuales se necesita una base jurídica individual:

- El entrenamiento y/o validación del modelo.
- El uso de datos de terceros en la inferencia.
- La comunicación de datos implícitos en el modelo.
- El tratamiento de los datos del interesado en el marco del servicio prestado por la IA.
- El tratamiento de datos del interesado para la evolución del modelo.

Según las anteriores finalidades, podemos destacar tres bases legales adecuadas para los tratamientos:

- El tratamiento es necesario para la *ejecución de un contrato* en el que el interesado es parte, o para la aplicación de medidas precontractuales a petición de este.

- El *interés legítimo,* siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

- El *consentimiento* de los interesados, que, como establece el artículo 4.11 del RGPD, es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

El alcance de la base legal llega hasta el origen de los datos personales. El responsable debe asegurarse de que los datos recibidos por terceras partes, ya sea mediante una comunicación o encargo de tratamiento, deben transmitirse sobre una base legal adecuada. Aunque la finalidad del tratamiento sea lícita y tenga sustento legal, si la obtención de los datos no tiene base legal, la actividad de tratamiento sería ilícita.

En el caso de que el sistema de IA utilizase categorías especiales de datos personales, a tenor del artículo 9 del RGPD, se necesitará una base jurídica reforzada para legitimar el tratamiento de esa categoría especial de datos personales.

4.4.3. Principio de transparencia

El principio de *transparencia* resulta ser crítico en los tratamientos basados en sistemas de IA, puesto que el interesado tiene el derecho a conocer las condiciones en las que se realiza el tratamiento. Pero la transparencia se concreta también en

obligaciones a los operadores para prestar de una manera adecuada la información en un formato que permita ser entendible al interesado.

La transparencia no se reduce a un instante puntual, sino que debe ser entendida como un principio en torno al que orbita de forma dinámica el tratamiento realizado y que afecta a todos y cada uno de los elementos y participantes que intervienen en la solución.

El RGPD contiene en su articulado medidas concretas respecto a la obligatoriedad del deber de transparencia a los responsables, y de forma adecuada para cubrir los conflictos legales existentes. En concreto, el artículo 13.2.f) del RGPD obliga a ofrecer al interesado una información significativa sobre la lógica aplicada, así como respecto a la importancia y las consecuencias previstas de un tratamiento cuando implica la adopción de decisiones automatizadas de las que deriven efectos jurídicos o le afecten significativamente de modo similar, obligación que va dirigida a tratar los problemas de explicabilidad del algoritmo[39]. Sobre la base de este principio descansa la licitud de la toma de decisiones basadas en tratamientos automatizados. La AEPD aporta los elementos que deben proporcionarse al interesado de cara a garantizar el derecho de información:

- El detalle de los datos empleados para la toma de decisión, más allá de la categoría, y en particular, la información sobre los plazos de uso de los datos (su antigüedad).

- La importancia relativa que cada uno de ellos tiene en la toma de decisión.

- La calidad de los datos de entrenamiento y el tipo de patrones utilizados.

- Los perfilados realizados y sus implicaciones.

- Valores de precisión o error según la métrica adecuada para medir la bondad de la inferencia.

[39] *Vid*. Martínez, R., "Inteligencia artificial, derecho y derechos fundamentales", en De la Quadra Salcedo, T., y Piñar Mañas, J. L. (dirs.), *Sociedad digital y derecho*, Boletín Oficial del Estado, Madrid, 2018, p. 275.

- La existencia o no de supervisión humana cualificada.

- La referencia a auditorías, especialmente sobre las posibles desviaciones de los resultados de las inferencias, así como la certificación o certificaciones realizadas sobre el sistema de IA. En el caso de sistemas adaptativos o evolutivos, la última auditoría realizada.

- En el caso de que el sistema de IA contenga información de terceros identificables, la prohibición de tratar esa información sin legitimación y de las consecuencias de realizarlo.

Es tal la incidencia del impacto jurídico de las decisiones automatizadas, que existe el derecho a no ser objeto de una decisión basada únicamente en un tratamiento automatizado en las diferentes normas sobre protección de datos europeas. El nuevo RGPD materializa este derecho en el artículo 22 estableciendo que el afectado tendrá derecho a no ser objeto de tales conductas cuando le afecten jurídicamente o tengan un efecto similar. Este derecho es diferente a otros que podemos encontrar en el RGPD, puesto que este derecho no se ejerce por parte del afectado. No está claro cómo se caracteriza esta figura, dado que el apartado 1 lo configura como un "derecho", mientras que el apartado 4 establece que las decisiones automatizadas "no se basarán en categorías especiales de datos". Es decir, lo configura como una "prohibición". Podría argumentarse que los legisladores habrían formulado el artículo 22.1 más como el artículo 22.4 si el derecho no fuese ejercido por el interesado[40]. Dependiendo de cómo se considere, las consecuencias pueden ser varias[41]:

1. *Tratándolo como un derecho*[42] de oposición hace depender su efecto de la acción de la persona afectada, al menos para los procesos de decisión que no entran dentro de las tres categorías de excepciones del párrafo segundo. Este es claramente un resultado más débil de una perspectiva de privacidad y protección de datos que si el artículo 22.1 es tratado como una prohibición.

[40] *Vid*. Mendoza, I. y Bygrave, L., "The Right not to be Subject to Automated Decisions based on Profiling", *University of Oslo Faculty of Law Research Paper No. 2017-20*, Oslo, 2017, p. 9.

[41] *Vid. Op. Supra*, p. 10.

[42] A favor de esta consideración, *Vid*. Savirimuthu, J., "Do algorithms dream of 'data'...", *op. cit.*, p. 259.

2. *Considerándolo una prohibición,* se prohíben aquellos procesos de decisión que no estén comprendidos en las excepciones previstas en el apartado 2, independientemente de la acción o inacción de la persona afectada, permitiendo únicamente los procesos decisorios especificados en el apartado 2 (con las calificaciones indicadas en los párrafos tercero y cuarto). Tal resultado más idóneo respecto al objetivo general del artículo 22 y, de hecho, del RGPD en general: proteger la privacidad y la protección de datos como derechos humanos fundamentales frente a la evolución tecnológica y de cualquier otro tipo.

Además, si el derecho del artículo 22.1 es ejercitado por el afectado, funcionaría efectivamente como un derecho a garantizar la participación humana en la toma de decisiones en cuestión. Esto haría superflua la salvaguardia de la "implicación humana" que se establece en el artículo 22.3 como requisito previo para la aplicación de las excepciones a) y b) al artículo 22.1. Según lo visto, tanto desde un punto de vista lógico como desde una perspectiva más teleológica, basada en la preocupación por la privacidad y la protección de datos como derechos fundamentales, tiene más sentido concluir que el derecho aparente proporcionado por el artículo 22.1 no tiene que ser ejercida por el interesado. Lo más probable es que el "derecho" funcione, en otras palabras, como una prohibición con la que el tomador de la decisión debe cumplir con independencia de si el "titular del derecho" lo invoca o no[43].

4.4.4. Principio de exactitud

El principio de *exactitud* incide principalmente sobre la existencia de sesgos en los modelos de inferencia. En concreto, en el considerando 71 del RGPD, los datos asociados a los interesados, ya sean los datos directamente recogidos o los inferidos, han de ser exactos. En particular, se hace explícito que el responsable del tratamiento ha de utilizar "procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles" que garanticen que los datos vinculados con el interesado son exactos. Es obligatorio demostrar y documentar que los procedimientos

[43] *Vid*. Mendoza, I. y Bygrave, L., "The Right not to be Subject to Automated Decisions based on Profiling", *University of Oslo Faculty of Law Research Paper No. 2017-20*, 2017, p. 11.

empleados para la inferencia de información sobre un interesado son precisos y, por tanto, estables y predecibles de acuerdo con el artículo 24 del RGPD.

Respecto a los datos inferidos, datos derivados de la interpretación realizada por el sistema de IA, y su exactitud, se destacan tres factores influyentes (AEPD, 2020, p. 56):

- La propia implementación del sistema IA. Las reglas implementadas que permiten a los sistemas de IA introducir inferencias erróneas, o los errores de programación que afectan a la implementación práctica, creando un sesgo que no puede ser alterado por un cambio de código *(hardwired).*

- El conjunto de datos utilizado para la validación y entrenamiento está viciado de manera intencionada, lo que se conoce como inyección de "bad data".

- La evolución sesgada del modelo de IA.

4.4.5. Principio de minimización

El principio de *minimización* choca directamente con el principio rector del Big Data, tecnología que alimenta al sistema de IA, que es la maximización de tratamiento de los datos personales[44]. Esa limitación se puede conseguir mediante:

- Limitar la extensión de las categorías de datos que se utilizan en cada fase del tratamiento a aquellas que son estrictamente necesarias y relevantes.

- Limitar el grado de detalle o precisión de la información, la granularidad de la recogida en tiempo y frecuencia y la antigüedad de la información utilizada.

- Limitar la extensión en el número de interesados de los que se tratan los datos.

- Limitar la accesibilidad de las distintas categorías de datos al personal del responsable/encargado o incluso al usuario final (si hay datos de terceros en los modelos de IA) en todas las fases del tratamiento.

[44] *Vid*. Gil González, E., *Big Data, privacidad y protección de datos*, AEPD, Madrid, 2015, p. 52.

4.5. SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información podemos entenderla como una dimensión relacionada con la protección de datos. No en vano, el artículo 32 del RGPD contempla la obligación de implementar las medidas de seguridad adecuadas para asegurar la integridad, disponibilidad, confidencialidad y resiliencia de la información sobre la base del artículo 5 del mismo respecto al principio de confidencialidad. Cualquier vulneración de las anteriores cualidades sobre los datos personales supone una violación de la seguridad de los datos personales, pudiendo generar, si así es demostrado, la exigencia de una indemnización por responsabilidad civil sobre la base del artículo 89 del RGPD.

Pero no todo el marco de la seguridad de la información se limita únicamente a la legislación de protección de datos personales. El Real Decreto-ley 12/2018 de seguridad de las redes y sistemas de información regula la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establece un sistema de notificación de incidentes[45]. Esto supone el marco jurídico de la seguridad de la información en los sistemas de IA, sin entrar en la legislación sectorial, como telecomunicaciones, sector público, etc.

La seguridad de la información puede definirse como el proceso tendente a prevenir, responder y corregir los incidentes de seguridad, protegiendo así la confidencialidad, integridad y disponibilidad de la información. Dentro de este concepto, se encuentra la ciberseguridad, una dimensión incluida en la seguridad de la información que persigue los anteriores objetivos en los ordenadores, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas y comunicación por cable[46].

La existencia de riesgos de seguridad de la información está asociada a la pérdida de dichas cualidades, por ejemplo, los ciberatacantes podrían hacer mal

[45] A efectos de esta norma, el sector asegurador no se encontraría entre su campo de aplicación al no considerarse como tal un operador esencial.

[46] *Vid*. NIST Special Publication 800-37, Risk *Management Framework for Information Systems and Organizations. A System Life Cycle Approach for Security and Privacy*. Rev. 2, 2018, p. 96.

uso de los datos recabados o generados por los dispositivos al comprometer la disponibilidad de los datos o cambiarlos, causando problemas de integridad de estos, y el uso de conocimientos de Big Data para reforzar o crear resultados discriminatorios. Cuando no hay datos disponibles, lo que puede provocar un fallo en el sistema, podrían producirse daños. La integridad de los datos puede causar problemas más sustanciales. Cuando los atacantes cambian datos, como la codificación, el cambio de valores o el reemplazo de datos con los suyos, la información proporcionada a los usuarios puede ser engañosa, o los límites establecidos previamente o los algoritmos que dirigen la funcionalidad del dispositivo pueden cambiar[47].

Como se ha explicado, la IA deriva de la aplicación de diversas tecnologías como el IoT, Big Data o *Machine Learning,* y la dependencia tecnológica hace que las amenazas inherentes de una repercutan al resto.

La conectividad, derivada de la aplicación del IoT, genera una serie de amenazas y vectores de ataque que pueden ser explotados[48]:

a. *Ataque sobre el dispositivo.* Este tipo de ataque es capaz de comprometer los dispositivos IoT. Su objetivo principal es comprometer las funciones arquitectónicas críticas del sistema (dependiendo de los dispositivos involucrados). En un sistema de control de inventario impulsado por RFID, un atacante exitoso podría derribar toda la red (especialmente cuando el dispositivo base, por ejemplo, el servidor, es el objetivo). En una red de área vecina (NAN) de una red eléctrica, un ataque de dispositivo podría afectar la resistencia de la red que, en el caso extremo, puede conducir a ataques distribuidos de denegación de servicio en toda la red. Los ataques al dispositivo pueden ser causados por una configuración incorrecta de IP, corrupción de memoria y código ejecutado incorrectamente en el sistema operativo del dispositivo en la capa de *middleware*.

[47] *Vid*. Tschider, C., "Regulating the Internet of Things: discrimination, Privacy, and Cybersecurity in the Artificial Intelligence age", *Denver Law Review*, vol. 96, n. 1, p. 97.

[48] *Vid*. Tweneboah-Koduah, S., "Cyber Security Threats to IoT Applications and Service Domains", *Wireless Personal Communications*, 2017, pp. 7-9.

b. *Ataque sobre el servicio.* Este es un tipo de ataque que compromete las aplicaciones del sistema (web, móvil, sistema, etc.) que se ejecutan en varios componentes del sistema. Una aplicación de IoT típica ejecuta varias sesiones tanto a nivel local como a nivel de servidor. En la mayoría de los casos, las aplicaciones pueden ser propiedad de proveedores de servicios de aplicaciones (ASP) o proveedores externos. Como se indicó anteriormente, los ataques cibernéticos a estas aplicaciones seguramente podrían comprometer otros sistemas interdependientes. Las vulnerabilidades comunes en este tipo de ataque incluyen inyección SQL, ejecución de código y denegación del servicio.

c. *Ataque de red.* Este es un ataque que tiene como objetivo comprometer la intercomunicación entre dispositivos al retrasar el reenvío de mensajes o la pérdida de mensajes. Los ataques a la red pueden destruir procesos computacionales dentro de los sistemas de configuración del IoT. En las redes de área doméstica (HAN), este tipo de ataque tiene como objetivo destruir las funcionalidades de los dispositivos de monitoreo o interconectados. De manera similar, en una red de área de vecindario (NAN), este tipo de ataque podría aislar o negar que los dispositivos conectados accedan a información vital de los dispositivos vecinos o atiendan la solicitud de mensajes del dispositivo vecino. Las causas de tales ataques incluyen inyección SQL, denegación del servicio y ejecución de código.

d. *Ataque a la interfaz web.* Este tipo de ataque se presenta como resultado de la enumeración de la cuenta, la falta de bloqueo de la cuenta o las credenciales débiles de la cuenta. En este caso, un atacante utiliza protocolos de autenticación débiles (ya sea capturando credenciales de texto sin formato o enumerando cuentas) para acceder a la interfaz web. Los ataques a la interfaz web pueden ser causados por secuencias de comandos entre sitios (XSS), falsificación de referencias entre sitios (CSRF), configuración incorrecta de IP e inyección SQL. Otras fuentes incluyen diseño de interfaz web inseguro y credenciales de cuenta débiles. El ataque compromete la integridad del dispositivo y podría conducir a la denegación de servicios.

e. *Ataque a la integridad de los datos.* Este es un ataque por el cual un agente de amenaza intenta comprometer los datos del sistema insertando, alterando o

eliminando completamente los datos (ya sea almacenados o en transmisión) para engañar al dispositivo inteligente y tomar decisiones incorrectas o comprometer su integridad. Los ataques de datos pueden ser causados por inyección SQL y ejecución de código que puede ser ejecutada por un atacante remoto.

Existe una serie de tipologías de amenaza que deben ser tenidas en cuenta dependiendo de las fases de desarrollo del sistema mediante *Machine Learning* según la AEPD[49]:

a. Fase de entrenamiento:

   - Acceso y manipulación del conjunto de datos de entrenamiento, previo a la configuración del modelo, por ejemplo, mediante técnicas de envenenamiento con patrones adversos.

   - Inclusión de troyanos y puertas traseras durante el proceso de desarrollo de la IA, bien en el propio código o en las herramientas de desarrollo.

   - Manipulación de la API de usuario para realizar accesos al modelo, tanto a nivel de caja negra como de caja blanca, para la manipulación de parámetros del modelo, filtrado del modelo a terceros, ataques a la integridad o disponibilidad de las inferencias.

b. Fase de pruebas:

   - Ataques por "adversarial machine learning"[50], por lo que sería necesario un análisis de la robustez y control de la alimentación con datos al modelo.

[49] *Vid*. AEPD, *Adecuación al RGPD de tratamientos que incorporan inteligencia artificial. Una introducción*, p. 41.

[50] Técnica de ataque que consiste en alimentar la IA con datos de ejemplo, que desde el punto de vista de la percepción humana pueden resultar indistinguibles de datos normales, pero que incluyen pequeñas perturbaciones que fuerzan a la IA a realizar inferencias erróneas.

- Ataques por imitación de patrones que se conoce que serán admitidos por el sistema.

- Reidentificación de los datos personales incluidos en el modelo (inferencia de pertenencia o inversión del modelo) por parte de usuarios internos y externos.

- Fraude o engaño a la IA por parte de los interesados, especialmente en casos que puedan suponer un perjuicio para otros interesados, lo que implica la necesidad de realizar un análisis de la robustez ante dichas actuaciones y la realización de auditorías.

- Filtrado a terceros de resultados de perfilado o decisiones inferidas por la IA (también relacionado con las API de usuario).

- Filtrado o acceso a los *logs* resultado de las inferencias generadas en la interacción con los interesados.

Ante estas amenazas, se propone una tipología de medidas defensivas para prevenir las amenazas presentadas[51]:

a. *Data sanitization*. Es una técnica de defensa práctica para garantizar la pureza de los datos de entrenamiento al separar las muestras adversas de las normales y luego eliminar estas muestras maliciosas.

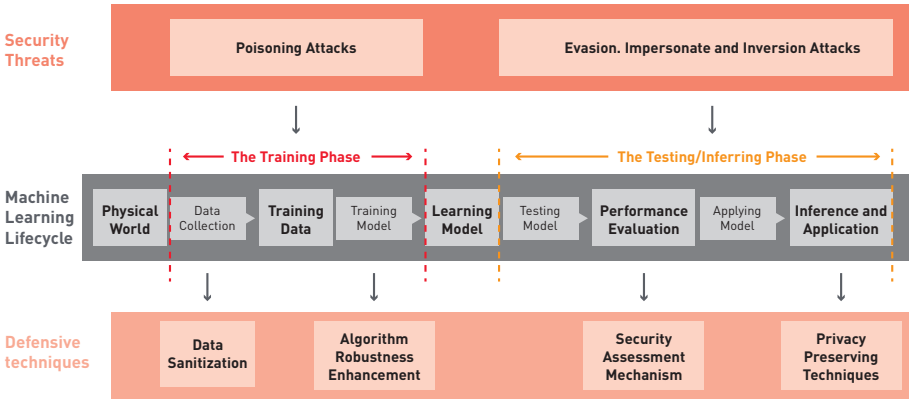
b. Mejora de la robustez de los algoritmos. Aplicación de metodologías de desarrollo seguro en el desarrollo del código.

c. Mecanismos de apreciación de la seguridad.

d. Técnicas de preservación de la privacidad.

[51] *Vid*. Qiang, L. *et al.*, "A Survey on Security Threats and Defensive Techniques of Machine", *IEEE Access*, 2018.

Amenazas y controles de seguridad de la información en un sistema de IA



Fuente: IEEE.

El deber de responsabilidad proactiva debe demostrarse también respecto a los riesgos en materia de seguridad de la información, y esto se consigue mediante una adecuada gestión del riesgo, tal y como recoge el artículo 32.1[52] del RGPD. Como veremos más adelante[53], la gestión de riesgos supone un proceso que abarca la identificación, análisis, evaluación y tratamiento de los riesgos, con el fin de adoptar una decisión estratégica respecto a estos. Si bien podemos encontrar diversas metodologías que establecen recomendaciones para la gestión de riesgos de seguridad de la información, existen mecanismos de certificación que permiten acreditar ante terceros la seguridad de un servicio, producto o sistemas[54], como son:

- ISO/IEC 27001:2013.

[52] Teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

[53] *Vid*. apartado 5.

[54] En cualquier caso, estos certificados decaerían en su utilidad cuando entre en vigor el proceso de evaluación de la conformidad del artículo 43 de la propuesta de reglamento sobre inteligencia artificial.

- Certificación LINCE.

- Esquema Nacional de Seguridad.

- Common Criteria.

En cualquier caso, debe asegurarse de que el sistema de IA pueda auditarse correctamente para poder demostrar una responsabilidad proactiva; para ello, se deberán mantener los ficheros de *logs* con el fin de proporcionar evidencias para[55]:

- Determinar quién y bajo qué circunstancias accede a los datos personales que pudieran estar incluidos en el modelo.

- Proporcionar trazabilidad en cuanto a la actualización de los modelos de inferencia, las comunicaciones del API del usuario con el modelo y la detección de intentos de abuso o intrusión.

- Proporcionar trazabilidad para permitir la gobernanza en la comunicación de datos entre todos los intervinientes en la solución IA en cuanto a las obligaciones que se derivan del considerando 66 del RGPD.

- Proporcionar seguimiento de los parámetros de calidad de la inferencia cuando la IA se utilice para la toma de decisiones o procesos de ayuda a la toma de decisión.

[55] *Vid. AEPD, Adecuación al RGPD de tratamientos que incorporan inteligencia artificial. Una introducción*, p. 43.

5. GESTIÓN DE RIESGOS COMO HERRAMIENTA PARA ABORDAR LA INCERTIDUMBRE: IA Y CUMPLIMIENTO NORMATIVO

5.1. LA GOBERNANZA CORPORATIVA DEL SECTOR ASEGURADOR

5.1.1. Concepto y componentes de un sistema de gobernanza corporativa

Tras los numerosos escándalos financieros del siglo XX que llevaron a la desaparición de varias entidades, se vio la necesidad de implantar nuevos principios éticos en la dirección de la organización, con el fin de crear una nueva forma de gobierno de las organizaciones al modular sus objetivos estratégicos mediante un conjunto de principios de comportamiento.

Fue en Estados Unidos, mediante la aprobación de la ley Sarbanes-Oxley, donde se introdujeron obligaciones en la estructura de gobierno de una organización. Este método fue trasladado a otras jurisdicciones, tanto como obligaciones generales a cualquier organización, como a obligaciones específicas según el sector donde se opere.

La gobernanza corporativa surge como una forma en la que las organizaciones son dirigidas y controladas, promoviendo la justicia corporativa, la transparencia y la rendición de cuentas[56]. El fin de la gobernanza corporativa se dirige a mitigar los conflictos de interés entre sus partes interesadas que surgen de discrepancias entre accionistas y la alta dirección[57]. Busca definir la existencia de deberes y responsabilidades entre los diferentes participantes en la organización, y especificar las reglas y procedimientos de compromiso en los asuntos corporativos[58].

---

[56] *Vid*. Wolfensohn, J., "The critical study of corporate governance provisions in India", *Financial Times*, 25, 4, 1999.

[57] *Vid*. Goergen, M., *International Corporate Governance*, Prentice Hall, 2012.

[58] *Vid*. Osei, E., "A winning governance structure: basic components of a corporate governance structure that supports a winning corporate strategy and enterprise value enhancement", *International Journal of Advancements in Research & Technology*, vol. 3, n. 8, p. 100.

Se basa en una serie de principios estipulados por distintas organizaciones nacionales o internacionales[59]. Pero es el trabajo de la OCDE donde traslada en el ámbito internacional unos principios internacionalmente aceptados y dirigidos a sus Estados miembros sobre los que se vertebra el fin que persigue la gobernanza corporativa:

1. *Consolidación de la base para un marco eficaz de gobierno corporativo.* El marco de gobierno corporativo promoverá la transparencia y la equidad de los mercados, así como la asignación eficiente de los recursos. Será coherente con el Estado de derecho y respaldará una supervisión y una ejecución eficaces.

2. *Derechos y tratamiento equitativo de los accionistas y funciones de propiedad clave.* El marco del gobierno corporativo protegerá y facilitará el ejercicio de los derechos de los accionistas y garantizará el trato equitativo a todos ellos, incluidos los minoritarios y los extranjeros. Todos tendrán la posibilidad de que se reparen de forma eficaz las violaciones de sus derechos.

3. *Inversores institucionales, mercados de valores y otros intermediarios.* El marco del gobierno corporativo debe proporcionar incentivos sólidos a lo largo de toda la cadena de inversión y facilitar que los mercados de valores funcionen de forma que contribuya al buen gobierno corporativo.

4. *El papel de los actores interesados en el ámbito del gobierno corporativo.* El marco de gobierno corporativo reconocerá los derechos de los actores interesados que disponga el ordenamiento jurídico o se estipulen de mutuo acuerdo y fomentará la cooperación activa entre estos y las sociedades con vistas a la creación de riqueza y empleo, y a la sostenibilidad de empresas sólidas desde el punto de vista financiero.

5. *Divulgación de información y transparencia.* El marco del gobierno corporativo garantizará la comunicación oportuna y precisa de todas las cuestiones relevantes relativas a la empresa, incluida la situación financiera, los resultados, la propiedad y sus órganos de gobierno.

[59] Cadbury Report (1992), Principles of Corporate Governance (OECD, 1999, 2004 y 2015) y Sarbanes-Oxley Act of 2002 (EE. UU., 2002).

6. *Las responsabilidades del consejo de administración.* El marco para el gobierno corporativo debe garantizar la orientación estratégica de la empresa, el control efectivo de la dirección por parte del consejo y la rendición de cuentas ante la empresa y los accionistas.

Sobre la base de estos principios, los Estados impulsaron marcos normativos de gobernanza que cubren, en mayor o menor profundidad, el desarrollo de estos principios, como pueden ser los marcos para:

- Una entidad financiera (MiFid II).
- Una entidad aseguradora (Solvencia II).
- Una entidad cotizada (Ley de Sociedades de Capital).

Sin embargo, son otros organismos internacionales, como ISACA (Information Systems Audit and Control Association), quienes definen la estructura que debe guardar un marco de gobernanza en todas las organizaciones[60]:

a. Los *procesos* describen una serie de prácticas y actividades organizadas para lograr determinados objetivos y producir una serie de salidas que contribuyan a la consecución de la totalidad de los objetivos de la organización.

b. Las *estructuras* organizativas son las entidades clave de toma de decisiones en una empresa.

c. Los *principios, políticas* y *marcos de referencia* convierten el comportamiento deseado en una aplicación práctica para la gestión diaria.

d. La *información* es generalizada a través de cualquier organización e incluye toda la información producida y utilizada por la empresa.

[60] Marco definido en la metodología de IT Government COBIT 2019 de ISACA.

e. La *cultura, ética* y *comportamiento* de individuos y de la empresa son, a menudo, subestimados como un factor de éxito en las actividades de gobierno y gestión.

f. Las *personas, habilidades* y *competencias* son necesarias para tomar buenas decisiones, ejecutar medidas correctivas y completar satisfactoriamente todas las actividades.

g. Los *servicios* y *aplicaciones* incluyen la infraestructura, la tecnología y las aplicaciones que brindan a la empresa un sistema de gobierno.

Las estructuras de gobernanza deben servir como un medio para monitorizar la conducta, estrategias y decisiones de una organización y asegurar que estas cumplen con los requisitos de las partes interesadas[61]; nacen sobre la base de este objetivo la necesidad de crear estructuras de control interno, ya sean funciones de auditoría interna, cumplimiento normativo y estándares que permiten reglar la correcta adecuación del proceso de gobernanza, como es el marco COSO para control interno integral.

La gobernanza corporativa ha evolucionado de un modelo únicamente resultadista, derivado de las obligaciones legales que los reguladores venían imponiendo a finales de siglo XX, en métodos para generar valor en los servicios ofertados, alejándolo de una visión burocrática de la dirección de las organizaciones.

5.1.2. El sistema de gobernanza del sector asegurador

Para el sector asegurador, no es desconocida las funciones de control interno debido a la gran regulación existente en el sector, en el sentido de que actúa no solo como integrante del sector financiero, sino también, en el sector económico, como uno de los miembros que sostiene el riesgo de cualquier tercero.

Debido al impacto estructural y multilocalizado del sector asegurador, la Unión Europea ha asumido competencias en materia regulatoria. Así, destaca la Directiva

[61] *Vid*. Zabihollah, R., *Financial Statement Fraud*, John Wiley & Sons, 2002, p. 67.

2009/138/CE sobre el seguro de vida, el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II), que se basa en los siguientes pilares:

a. *Pilar I:* se centra en el cálculo de los requerimientos de capital y de los fondos propios para cubrirlos. Se basa en el principio general de que la entidad debe tener fondos propios suficientes y valorados conforme al mercado para cubrir sus riesgos.

b. *Pilar II:* se centra en la supervisión, es decir, regula, por un lado, las labores del supervisor de seguros, los mecanismos con que contará para hacer su trabajo, y por otro, respecto de las aseguradoras, establece igualmente una serie de herramientas y políticas de medición y gestión de sus riesgos.

c. *Pilar III:* se centra en la disciplina de mercado y en la transparencia financiera de las entidades aseguradoras. La herramienta fundamental que deberán elaborar las aseguradoras en este ámbito es un informe sobre la situación financiera y de solvencia.

Centrándonos en el pilar II, este capítulo propone un sistema de gobernanza en la sección 2 del capítulo IV de la directiva formado por las funciones de: gestión de riesgos, verificación del cumplimiento, auditoría interna y actuarial, y seguridad de la información[62], siendo estas funciones clasificadas como *fundamentales* y sometidas a un férreo control, y dos sistemas paralelos de gestión de riesgos y control interno, constituidos mediante sus procesos, procedimientos y políticas. La justificación de este sistema deriva del considerando 29 de la directiva Solvencia II: "Algunos riesgos solo pueden tenerse debidamente en cuenta a través de exigencias en materia de gobernanza y no a través de los requisitos cuantitativos que se reflejan en el capital de solvencia obligatorio. Resulta, pues, esencial un sistema de gobernanza eficaz para la correcta gestión de la empresa de seguros y para el sistema de control".

[62] Esta función no se recoge en el marco normativo de Solvencia II, sino que es una imposición de las Guidelines on Information and Communication Technology (ICT) security and governance (EIOPA-BoS-19-526).

Sistema de gobernanza de Solvencia II

Fuente: elaboración propia.

Estos elementos son desarrollados en el Reglamento Delegado (UE) 2015/35, por el que se completa la Directiva 2009/138/CE del Parlamento Europeo y del Consejo sobre el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II) y que, posteriormente, quedarían transpuestas en la Ley 20/2015, de ordenación, supervisión y solvencia de las entidades de seguro y reaseguro, y desarrollado esta por el Reglamento 1080/2015 por el que se desarrolla la Ley 20/2015, con el apoyo de las Directrices sobre el Sistema de Gobernanza de la EIOPA[63].

En concreto, el artículo 268 del reglamento delegado especifica el estatuto funcional de las personas que desempeñen una función establecida por la norma. En especial, obliga a las organizaciones a implementar las funciones obligatorias y las líneas de rendición de cuentas para que ninguna influencia pueda comprometer el desarrollo objetivo de su trabajo, cuyas personas rendirán cuentas en última

[63] EIOPA-BoS-14/253 ES.

instancia ante el órgano de administración, cooperando con el resto de las funciones de la organización. A su vez, permite a estas personas comunicarse por iniciativa propia con el resto del personal de la organización y dispondrán de la autoridad y recursos necesarios, así como ninguna restricción en la obtención de la información.

Observamos que el legislador ha implementado los principios de autonomía e independencia[64] para la labor desarrollada por cualquier persona que desempeñe las funciones correspondientes, cuya vulneración de estos principios haría incurrir tanto al superior jerárquico como al titular de la función en conflicto de intereses[65].

Claramente, la Unión Europea ha optado por un modelo de gestión basado en la teoría de las tres líneas de defensa, ahora llamado "modelo de las Tres Líneas" tras la actualización de 2020, estándar propuesto por el Instituto de Auditores Internos para proporcionar un marco de gestión integrado de los riesgos de una organización[66] y siendo este un modelo adecuado para establecer una función integral de GRC (gobierno, riesgo y cumplimiento). El presente modelo está basado en los siguientes principios[67]:

- *Principio 1. Gobierno.* El gobierno de una organización requiere de estructuras y procesos apropiados que permitan: 1) la rendición de cuentas por parte de un órgano de gobierno a las partes interesadas; 2) acciones por parte de la dirección para lograr los objetivos de la dirección, y 3) aseguramiento y asesoramiento por parte de un rol de auditoría interna.

---

[64] *Vid*. Casanova, A., *Autonomía e independencia en compliance*, ASCOM, Madrid, 2019. Estos conceptos no son sinónimos. La autonomía se obtiene cuando la organización da acceso a las personas y documentos de esta, publicitando las facultades de la función y trabajando en los comités internos. Por otro lado, la independencia se logra cuando se aleja a la función de condicionantes que pueden alterar la ética en el trabajo, como es la presión sobre los objetivos de negocio.

[65] *Vid*. Muelas, P., "La ubicación de la función de verificación del cumplimiento normativo en las entidades aseguradoras", *Análisis GAP*, julio, 2016, p. 2.

[66] *Vid*. IIA, *Las tres líneas de defensa para una efectiva gestión de riesgos y control*, 2013. Actualmente, este modelo se encuentra en revisión, complementándose hasta que salga la nueva versión, por el Documento de consulta del IIA. tres líneas de defensa, junio, 2019.

[67] *El modelo de las Tres Líneas del IIA 2020. Una actualización de las tres líneas de defensa.*

- *Principio 2. Roles del órgano de gobierno.* El órgano de gobierno debe asegurar la implantación de estructuras y procesos para un gobierno eficaz. Delega la responsabilidad y aporta recursos a la dirección para alcanzar los objetivos.

- *Principio 3. Dirección y roles de primera y segunda línea.* La responsabilidad de la dirección de alcanzar los objetivos organizativos comprende tanto los roles de primera como los de segunda línea. Los roles de primera y segunda línea pueden mezclarse o separarse. Algunos roles de segunda línea pueden ser asignados a especialistas para proporcionar experiencia adicional, apoyo, monitoreo y cuestionar a aquellos con roles de primera línea. Los roles de segunda línea pueden centrarse en objetivos específicos de la gestión de riesgos, tales como: el cumplimiento de las leyes, las regulaciones y el comportamiento ético aceptable; el control interno; la seguridad de la información y la tecnología; la sostenibilidad; y el aseguramiento de la calidad.

- *Principio 4. Roles de tercera línea.* La auditoría interna proporciona aseguramiento y asesoramiento independientes y objetivos sobre la adecuación y eficacia del gobierno y la gestión de riesgos.

- *Principio 5. Independencia de tercera línea.* La independencia de la auditoría interna de las responsabilidades de la gerencia es fundamental para su objetividad, autoridad y credibilidad.

- *Principio 6. Creación y protección del valor.* Todos los roles que trabajan juntos contribuyen colectivamente a la creación y protección del valor cuando están alineados entre sí y con los intereses prioritarios de las partes interesadas.

Sobre la base de los principios anteriores, se establece una serie de roles relativos a las funciones de primera, segunda y tercera línea:

1. *La dirección,* donde podemos diferenciar:

    a. Roles de *primera línea,* que se encargan del cumplimiento de los objetivos operativos, comunican el seguimiento de los objetivos y los riesgos,

crean estructuras organizativas para la gestión de la operativa y garantizan el cumplimiento normativo.

b. Roles de *segunda línea,* que proporcionan conocimientos especializados complementarios, apoyo, vigilancia y cuestionamientos relacionados con la gestión del riesgo. Estas funciones son desarrolladas por personas que deben gozar de auditoría e independencia. Adaptándolo al modelo de Solvencia II, se han estipulado las funciones obligatorias:

   - Una *función de gestión de riesgos,* integrada en el sistema de gestión de riesgos de la entidad aseguradora. El sistema de gestión de riesgos deberá ser eficaz y sustentado por las políticas y procedimientos al uso, por lo que se deberán medir el desempeño de dicho sistema, integrado en el organigrama y en el proceso de toma de decisiones. El sistema de gestión de riesgos deberá cubrir la gestión de un catálogo de riesgos[68], en concreto, cubrirá el riesgo operativo, que se incluye el riesgo legal. La función de gestión de riesgos deberá asistir y asesorar al órgano de administración sobre todo lo relativo a la gestión de riesgos de una organización.

   - Una *función de verificación del cumplimiento,* integrada en el sistema de control interno. El fin de este sistema es garantizar el cumplimiento legal y la eficiencia y eficacia de las operaciones según sus objetivos. La función de verificación del cumplimiento comprenderá el asesoramiento al órgano de administración, dirección o supervisión acerca del cumplimiento de las disposiciones legales, reglamentarias y administrativas, y la evaluación de las posibles repercusiones de cualquier modificación del entorno legal en las operaciones de la empresa y la determinación y evaluación del riesgo de cumplimiento.

[68] Artículo 44 de la directiva Solvencia II: a) la suscripción y la constitución de reservas; b) la gestión de activos y pasivos; c) la inversión, en particular, en instrumentos derivados y compromisos similares; d) la gestión del riesgo de liquidez y de concentración; e) la gestión del riesgo operacional; f) el reaseguro y otras técnicas de reducción del riesgo.

- Una *función actuarial,* con la misión principal de calcular las provisiones técnicas.

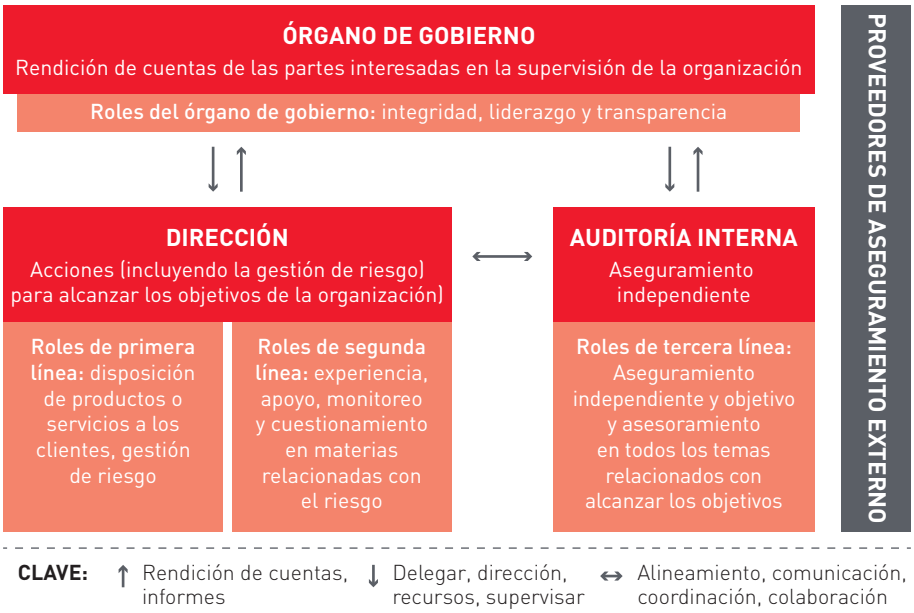
- Una *función de seguridad de la información,* impuesta por la Guidelines on Information and Communication Technology (ICT) security and governance, con el fin de gestionar la seguridad de la información de la entidad.

2. *Auditoría interna,* que supone la *tercera línea.* Tiene la labor de rendir cuentas ante el órgano de dirección, primando la independencia y autonomía en sus funciones, y evaluar el sistema de gobernanza y gestión de riesgos, evaluando también la eficacia de los controles implantados. La definición de la segunda y tercera línea está claramente establecida por el artículo 47 de la directiva Solvencia II, cuando estipula que la función "abarcará la comprobación de la adecuación y eficacia del sistema de control interno y de otros elementos del sistema de gobernanza", perfilándose como "último" bastión de la gestión de los riesgos. Esta función reportará directamente al órgano de administración, vinculando su existencia al mantenimiento de un buen gobierno corporativo.

3. *Proveedores de aseguramiento externo,* que se apoyan en la satisfacción de las expectativas legales y normativas, y prestan asesoramiento al órgano de gobierno.

Por último, existen otros elementos externos al organigrama de la empresa aseguradora y al propio modelo de gestión, como son los *reguladores,* que serían en este caso la EIOPA, en el ámbito europeo, y la Dirección General del Seguro y Fondos de Pensiones. Si bien en la versión de 2020 del modelo de las Tres Líneas se ha eliminado como rol interviniente al regulador, no se puede obviar su influencia en la entidad. Es relevante destacar la labor de estos organismos respecto a las recomendaciones de los sistemas de gobernanza de las entidades aseguradoras, como son las directrices en materia de gobernanza y, sobre todo, la facultad que tiene la Dirección General del Seguro y Fondos de Pensiones de verificar el sistema de gobierno, pudiendo exigir las medidas necesarias para mejorar y consolidar su sistema de gobierno (art. 65.5 LOSSEAR).

Modelo de las Tres Líneas



Fuente: IIA.

Este sistema descansa sobre un marco de gobernanza regido por los artículos 41 y 43 de la directiva Solvencia II basado en el principio de transparencia y regido por las políticas internas de la entidad aseguradora dictadas al uso. Los modelos y sistemas de gobernanza no deben verse como elementos burocráticos, sino como una forma de crear valor en la organización mediante una gestión coordinada de varios elementos organizativos que interactúan entre sí.

Las entidades aseguradoras cuentan con un marco complejo pero adecuado para la gestión de los riesgos legales derivados de la IA al estar vinculados los riesgos legales con los riesgos operativos, objetos de gestión bajo la directiva Solvencia II.

La empresa aseguradora debe aprovechar el marco jurídico de control impuesto para gestionar aquellos riesgos derivados del uso de esta tecnología; si bien serán necesarias algunas matizaciones que describiremos en puntos posteriores, ofrece un punto de partida ideal, puesto que permite, mediante este modelo, integrar los

elementos de gestión fundamentales en una organización, como son las funciones de gobernanza y la implicación de la alta dirección, elementos obligatorios en cualquier metodología de gestión de riesgos reconocidos internacionalmente.

5.1.3. La gobernanza de los servicios de tecnologías de la información mediante sistemas de cumplimiento gestionados

Hemos observado que los sistemas de gobernanza que son implantados en las organizaciones no obedecen a meras obligaciones legales, sino a una oportunidad de generar valor y eficiencia en su gestión, pero la gobernanza corporativa puede afrontarse desde varios puntos de gestión, centrando su estrategia en ámbitos concretos que soportan una organización; en concreto, una organización puede adoptar un sistema de gobernanza basado en las tecnologías de la información, o gobernanza de TI.

Esta dimensión de la gobernanza no debe separarse del propio sistema de gobernanza de Solvencia II, puesto que las tecnologías de la información tienen una importancia capital a la hora de poder cumplir no solo con los objetivos de negocio, sino con las propias obligaciones del pilar II de la directiva.

5.1.3.1. Modelos y estándares actuales sobre la gobernanza de las tecnologías de la información

La gobernanza de TI es un marco para el liderazgo, estructuras organizacionales y procesos de negocio, estándares y cumplimiento, que asegura que las tecnologías de la información que apoyan a la organización permiten el cumplimiento de sus estrategias y objetivos. Este concepto no discrepa de los postulados de gobernanza que estipula Solvencia II, al recoger como elementos fundamentales la gestión de riesgos, el cumplimiento normativo, el control interno y la revisión del sistema, solo que se debe partir de las tecnologías de la información como base para desplegar el sistema de gobernanza. No se debe confundir con la gestión de los servicios de TI. La gobernanza de TI consiste en definir el "qué hacer" por parte de la organización, en cambio, la gestión de los servicios de TI se centra en "cómo hacerlo", asegurando que la tecnología de la información de una organización opera de manera efectiva, eficaz y conforme.

Desde el comienzo del nuevo milenio, la gobernanza de TI ha sido un concepto que ha crecido en importancia, creándose numerosos estándares para proporcionar unas guías para establecer un modelo de gobernanza eficaz y entendible ante terceros.

En esta materia, los estándares internacionales ISO/IEC 38500:2015 gobernanza de TI para la organización[69] y el Control Objectives for Information and related Technology (COBIT), actualmente en su versión 2020, y perteneciente a Information Systems Audit and Control Association (ISACA), son los más importantes en materia de gobernanza de TI, siendo en muchos de sus elementos coherentes entre sí debido a su retroalimentación a lo largo de sus respectivas actualizaciones.

Estos estándares definen la gobernanza de TI como un sistema, integrado en la gobernanza corporativa, por el cual el uso actual y futuro de TI, consistente en la planificación, diseño, desarrollo, despliegue, operación, gestión y aplicación de TI para cumplir con los objetivos de negocio y crear valor para la organización, es dirigido y controlado.

La buena gobernanza de TI apoya a los órganos de gobierno para asegurar que el uso de TI contribuye positivamente al desempeño de la organización, a través de[70]:

- la innovación en los servicios, mercados y negocios;
- el alineamiento de TI con las necesidades de negocio;
- la implementación y operación adecuadas de los activos de TI;
- la aclaración de la responsabilidad y la rendición de cuentas, el suministro y la demanda de TI en el logro de los objetivos de la organización;
- la continuidad del negocio y su sostenibilidad;
- la asignación eficiente de los recursos;

[69] Esta norma supone el primer estándar internacional que propone un modelo sobre el uso efectivo, eficiente y aceptable de tecnologías de la información (TI) dentro de sus organizaciones.

[70] ISO/IEC 38500:2015.

- las buenas prácticas en las relaciones con los interesados, y

- la realización actual de los beneficios esperados de cada inversión en TI.

Ambos estándares otorgan al cumplimiento normativo un papel crucial respecto al sistema de gobernanza de IT, puesto que uno de los objetivos es buscar la conformidad con las obligaciones legales o voluntarias debido a que el mal uso de las infraestructuras de TI de una organización conlleva el riesgo de no cumplir con la legislación; en concreto, imponen una gestión adecuada de los riesgos en los procesos relacionados con TI respecto a las legislaciones de privacidad, seguridad de la información y la propiedad intelectual.

La organización debe ser determinada por esta, dependiendo del tamaño, misión y las decisiones del órgano de gobierno en cuanto a límites de responsabilidad, pero cualquier marco de gobernanza de TI definido debe pivotar sobre la base de los siguientes elementos[71]:

1. *Principios para una buena gobernanza de TI.* El marco de gobernanza debería estar basado en un conjunto de principios estandarizados, como pueden ser los principios establecidos en la ISO/IEC 38500 o COBIT 2019.

2. *Estrategias y normas sobre el uso de TI.* Las estrategias y normas para el uso de TI dirigidas por la alta dirección comunicadas a los gestores deberían proporcionar las bases para la aplicación de la gobernanza a los sistemas de gestión de una organización. Ya sea que estén basadas en parte por requisitos legales o por recomendaciones emanadas del sector público, las estrategias y normas de la organización deben dirigirse a los requisitos organizacionales específicos establecidos por la dirección, teniendo en cuenta los principios de buena gobernanza.

3. *Planificación estratégica de TI.* Los procesos de planificación empresarial deberían tener en cuenta las capacidades actuales y futuras de TI para asegurarse de que los planes estratégicos de TI satisfacen las actuales y continuas necesidades de la planificación estratégica de la organización.

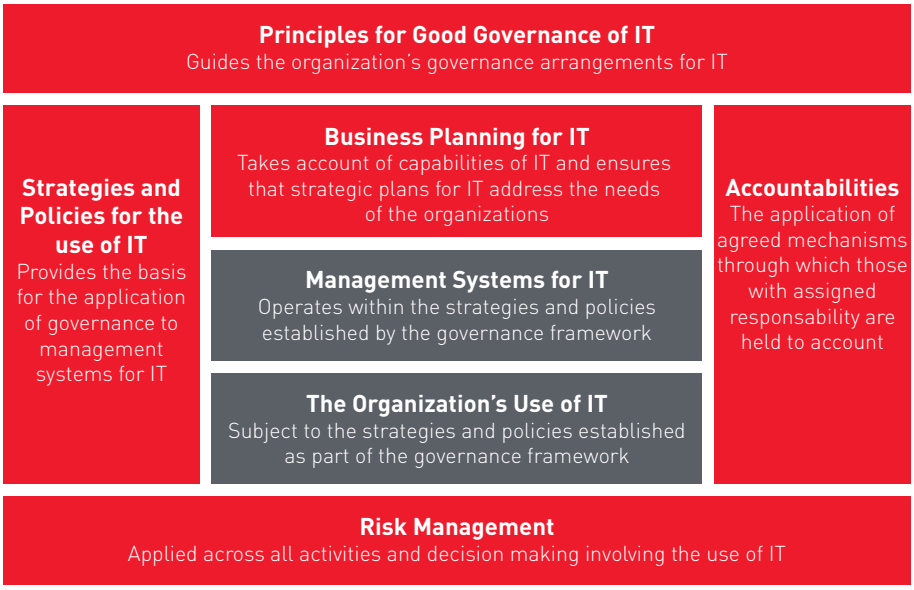
[71] ISO/IEC 38502:2017.

4. *Gestión de riesgos.* El marco de gobernanza de TI debería involucrar unas prácticas robustas de gestión de riesgos en todas las actividades de TI y toma de decisiones. La gestión del riesgo por el uso de TI debería basarse sobre la aplicación de los procesos de gestión de riesgos de la organización.

5. *Sistemas de gestión de TI.* Los sistemas de gestión de TI deberían operar dentro de las estrategias y normas establecidas por la alta dirección para lograr los objetivos estratégicos y operacionales de la organización. Esta responsabilidad debería recaer sobre los gestores de la organización.

6. *El uso de TI por parte de la organización.* El centro de un marco de gobernanza para TI es el propio uso TI. Para cumplir con las necesidades de negocio, el uso de TI debería estar sujeto a las estrategias y normas establecidas por las organizaciones definidas como parte del marco de gobernanza, y también para los sistemas de gestión de TI de la organización.

Principios para un buen gobierno de las TI



Fuente: ISO/IEC 20000-1.

Los estándares proponen una serie de principios diferentes para inspirar a los modelos de gobernanza de TI que pueden adoptarse como elementos del marco de gobernanza de la organización.

ISO 38500	COBIT 2019
Los individuos y grupos dentro de la organización entienden y *aceptan sus responsabilidades* con respecto del suministro y la demanda de TI. Los que tienen la responsabilidad por las acciones también tienen la autoridad para realizarlas.	Cada empresa necesita un sistema de gobierno para *satisfacer las necesidades de las partes interesadas y generar valor* a partir del uso de TI. El valor refleja un equilibrio entre beneficios, riesgos y recursos, y las empresas necesitan una estrategia accionable y un sistema de gobierno para realizar este valor.
La *estrategia de negocio* de la organización toma en cuenta las capacidades actuales y futuras de TI; los planes para el uso de TI satisfacen las necesidades actuales y en curso de la estrategia de negocio de la organización.	Un sistema de gobernanza para TI empresarial se construye a partir de una serie de componentes que pueden ser de diferentes tipos y que funcionan juntos de manera *holística.*
Las *adquisiciones* de TI son hechas por razones válidas, sobre la base del análisis apropiado y en curso, con la toma de decisiones clara y transparente. Existe un balance apropiado entre los beneficios, oportunidades, costos y riesgos, tanto a corto como a largo plazo.	Un *sistema de gobernanza debe ser dinámico*. Esto significa que cada vez que se modifican uno o más de los factores de diseño, se debe considerar el impacto de estos cambios en el sistema. Una visión dinámica conducirá a un sistema viable y a prueba de futuro.
La TI es adecuada para el propósito de *apoyar a la organización,* proporcionando los servicios, niveles de servicio y calidad del servicio requerido para satisfacer los requisitos del negocio actual y futuro.	Un sistema de gobernanza debe *distinguir claramente entre las actividades y estructuras de gobernanza y gestión.*
El uso de TI *cumple con toda la legislación y regulaciones obligatorias.* Las políticas y prácticas son claramente definidas, implementadas y cumplidas.	Un sistema de gobierno debe *adaptarse a las necesidades de la empresa,* utilizando un conjunto de factores de diseño como parámetros para personalizar y priorizar los componentes del sistema de gobierno.

Continúa

ISO 38500	COBIT 2019
Las políticas, prácticas y decisiones de TI demuestran respeto por el *comportamiento humano,* incluyendo las necesidades actuales y cambiantes de todas las "personas en el proceso".	Un sistema de gobierno debe abarcar a la empresa de principio a fin, centrándose no solo en la función de TI, sino también en toda la tecnología y el procesamiento de la información que la empresa implementa para lograr sus objetivos, independientemente de dónde se encuentre el procesamiento en la empresa.

Fuente: elaboración propia.

El modelo de gobernanza de TI se basa en tres tareas principales[72]:

1. *Evaluar* el uso actual y futuro de TI, incluyendo planes, propuestas y acuerdos de suministro, ya sean internos, externos o ambos. Deberán tener en cuenta los elementos externos e internos a la organización, tales como el cambio tecnológico, las tendencias económicas y sociales, las obligaciones regulatorias, las expectativas legítimas de los interesados y las influencias políticas, teniendo en cuenta las necesidades de negocio tanto actuales como futuras, los objetivos organizacionales actuales y futuros que se tienen que alcanzar, tales como el mantenimiento de la ventaja competitiva, así como los objetivos específicos de los planes y propuestas que están evaluando.

2. *Dirigir* la preparación e implementación de estrategias y políticas para asegurar que el uso de TI cumpla con los objetivos del negocio. Para ello, se deben asignar las responsabilidades correspondientes, fomentar una cultura de buena gobernanza de TI en su organización requiriendo que los gerentes proporcionen información oportuna.

3. *Monitorizar* la conformidad con las políticas y su desempeño en relación con las estrategias, y asegurarse de que TI está en conformidad con las obligaciones externas (regulatorias, legislación, contractual) y prácticas internas de trabajo.

[72] Estas tareas han sido adoptadas por otros estándares internacionales. *Vid*. Control Objectives for Information and related Technology (COBIT), actualmente en su versión COBIT 2020, y perteneciente a Information Systems Audit and Control Association (ISACA), si bien se basan en principios diferentes a los recogidos por la ISO/IEC 38500:2015.

Estas tareas deben aplicarse sobre los principios propuestos, interactuando entre sí, tal y como se muestra en la siguiente ilustración sobre el modelo de gobernanza.

Estructura de gobierno de TI

Fuente: ISO/IEC 38500.

5.1.3.2. La relación entre la gobernanza y la gestión, y los sistemas de gestión de servicios

Como hemos incidido anteriormente –y se muestra en la anterior ilustración–, el proceso de gobernanza debe mantenerse separado de los procesos de gestión. Sin embargo, esto no debe entenderse como la existencia de compartimentos estancos entre la gestión y la gobernanza, pero tampoco como elementos al mismo nivel, puesto que la gobernanza consiste en la "gestión de los servicios".

Los marcos de gobernanza deberían habilitar a los gestores para llevar una gestión del día a día con la máxima autonomía posible. La gobernanza requiere el desarrollo de valores compartidos y finalidades, estableciendo una dirección, proporcionando recursos y delegando la autoridad para habilitar a los gestores a actuar con autonomía y sensibilidad en un entorno cambiante.

La relación entre el proceso de gobernanza y los procesos de gestión son los siguientes[73]:

a. *Responsabilidades del órgano de gobierno.* Los miembros del órgano de gobierno son responsables de la gobernanza de TI y deben rendir cuentas por la efectividad, eficiencia y uso aceptable dentro de la organización.

b. *Formulación de la estrategia y supervisión.* La gobernanza proporciona los medios por los cuales la alta dirección establece la dirección de la organización respecto al uso de las TI y monitoriza el estado de la organización y el desempeño de sus gestores en la consecución de los resultados requeridos.

c. *Delegación.* Los aspectos de la gobernanza de TI pueden ser emprendidos por los gestores si tienen asignadas las responsabilidades apropiadas por la alta dirección junto con la delegación de autoridad.

d. *Responsabilidades de los gestores.* Los gestores son responsables de lograr los objetivos estratégicos de la organización dentro de las estrategias y políticas por el uso de las TI dirigidas por la alta dirección.

e. *Gobernanza y control interno.* La gobernanza de TI requiere del establecimiento de un sistema efectivo de control interno como parte de los sistemas de gestión de la organización.

Los sistemas de gestión de servicios de TI se centran en la implementación adecuada de unos procesos o prácticas de gestión del propio servicio y en la evaluación del desempeño de estos elementos, interactuando directamente con el proceso

[73] ISO/IEC 38502:2017.

de gobernanza. La organización, por lo tanto, debe evaluar, dirigir y monitorizar el proceso de la gestión del servicio que se presta sobre sistemas de IA y permitir la creación de la cadena de valor del servicio[74].

En este sentido, existen guías de buenas prácticas internacionales que proporcionan un marco de gestión de los servicios de TI, como son la Information Technology Infrastructure Library (ITIL), propiedad de AXELOS, y la serie de normas internacionales ISO/IEC 20000. Estos estándares proporcionan los requisitos para la adopción de un sistema de gestión de servicios sobre la base de la implicación de la alta dirección, la gestión de determinados procesos y la mejora continua.

Las obligaciones del sistema de gobernanza derivada de Solvencia II deben alcanzar a la dirección de TI de la entidad aseguradora y la gestión de sus servicios, e implementar las políticas y procedimientos correspondientes.

[74] ITIL v4 Foundations.

Sistema de gestión de servicio TI

Fuente: ISO/IEC 20000-1.

5.1.3.3. La gobernanza de TI en el marco de Solvencia II

Como hemos explicado, la gobernanza de TI es un subelemento incluido en la gobernanza corporativa de la organización. El modelo de gobernanza de Solvencia II aplicable a las entidades aseguradoras no es ajeno a la implicación de las TI en las obligaciones del sistema de gobernanza del pilar II. Según la EIOPA, se pueden desprender ciertos requisitos de gobernanza de las tecnologías de la información que el Reglamento delegado (UE) 2015/35 se encargó de ampliar.

Estas obligaciones deben ser entendidas y enmarcadas dentro de la dimensión global del sistema de gobernanza del artículo 41 de la directiva[75]. Las obligaciones de asignación de recursos para la existencia de un sistema de gobernanza eficaz pueden cumplirse mediante la puesta a disposición de los medios tecnológicos para sostener el modelo de gobernanza de la entidad aseguradora y el aseguramiento de la continuidad y recuperación de las operaciones.

El Reglamento delegado (UE) 2015/35, en su artículo 258, añade requisitos específicos donde las TI juegan un papel nuclear en el sistema de gobernanza de la entidad aseguradora:

- establecerán sistemas de información que ofrezcan información completa, fiable, clara, coherente, oportuna y pertinente sobre las actividades de la empresa, los compromisos asumidos y los riesgos a los que esté expuesta;

- mantendrán registros adecuados y ordenados de la actividad y la organización interna de la empresa;

- salvaguardarán la seguridad, integridad y confidencialidad de la información, teniendo en cuenta la naturaleza de la información de que se trate;

- establecerán, aplicarán e implementarán una política de continuidad para garantizar la continuidad de las operaciones en el caso de sufrir incidentes disruptivos.

[75] *Vid*. Baena Álvarez de Quevedo, F. J., "Solvencia II y gestión del riesgo tecnológico en las compañías de seguros", *CSTIC 2012*, 18 de septiembre de 2012.

Esta concepción ha sido expandida mediante las Guidelines on Information and Communication Technology (ICT) security and governance de la EIOPA[76]. En esta guía se imponen una serie de obligaciones respecto a la implicación de las TI en el sistema de gobernanza respecto a la alta dirección de la entidad aseguradora, estableciendo a su vez unos controles en materia de seguridad de la información y continuidad de las operaciones que serán aplicables a partir del 1 de julio de 2021.

Tal y como dicta la directriz 1, las directrices deben implementarse de acuerdo con el *principio de proporcionalidad* según la naturaleza, escala y complejidad de los riesgos inherentes a la actividad. Como elemento inexorablemente ligado al sistema de gobernanza, la alta dirección (directriz 2):

a. Debe garantizar que el sistema de gobernanza de las empresas, en particular el sistema de gestión de riesgos y control interno, gestione adecuadamente los riesgos de seguridad y TI de las empresas.

b. Debe asegurarse de que la cantidad y las habilidades del personal de las empresas sean adecuadas para apoyar sus necesidades operativas de TI, los procesos de gestión de riesgos de TI y seguridad de forma continua y para garantizar la implementación de su estrategia de TI.

c. Debe asegurarse de que el presupuesto asignado para cumplir con lo anterior sea continuamente apropiado. Además, el personal debe recibir una formación adecuada sobre las TI y los riesgos de seguridad, incluida la seguridad de la información, de forma regular.

Las directrices especifican que la alta dirección tiene la responsabilidad general de establecer y aprobar la estrategia de TI de las empresas, alineada con su estrategia comercial general, así como supervisar su comunicación e implementación, siguiendo la estructura de la gobernanza de TI como elemento incluido en la gobernanza corporativa. La estrategia debe definir al menos:

- cómo deberían evolucionar las TI de las empresas para apoyar e implementar eficazmente su estrategia comercial, incluida la evolución de la estructura

[76] EIOPA-BoS-20/600.

organizativa, los modelos comerciales, el sistema TI y las dependencias clave con los proveedores de servicios;

- la evolución de la arquitectura de las TI, incluidas las dependencias de los proveedores de servicios; y

- los objetivos claros de seguridad de la información, centrándose en los sistemas y servicios de TI, el personal y los procesos.

Las empresas deben garantizar que la estrategia de TI se implemente, adopte y comunique a todo el personal relevante y a los proveedores de servicios cuando corresponda y sea pertinente, de manera oportuna, y establecer un proceso para monitorear y medir la efectividad de la implementación de la estrategia de TI.

Teniendo en cuenta estos requisitos, y la directriz 4 de la guía comentada, la alta dirección tiene la responsabilidad general de establecer un sistema efectivo para administrar los riesgos de seguridad y TI *como parte del sistema general de gestión de riesgos de la entidad aseguradora.* Esto incluye la determinación de la tolerancia al riesgo para esos riesgos, de acuerdo con la estrategia de riesgo de la empresa y un informe periódico por escrito sobre el resultado del proceso de gestión de riesgos dirigido a la alta dirección.

También la gestión del riesgo tiene una dimensión de TI que debe ser tenida en cuenta, puesto que los riesgos en materia de seguridad de la información y continuidad de negocio forman parte del riesgo operativo[77] y estos, como parte de su sistema general de gestión de riesgos. Las empresas deberían, en relación con los riesgos de TI y seguridad (al definir los requisitos de protección de las TI como se describe a continuación), considerar al menos lo siguiente:

a. Las empresas deben establecer y actualizar periódicamente un mapeo de sus procesos y actividades comerciales, funciones comerciales, roles y activos

[77] *Vid.* Lacen, V., "Riesgos operacionales", en Garcimartín, F. (coord.), *Estudio sobre los sistemas de registro, compensación y liquidación de valores en Iberoamérica*, CNMV, Madrid, 2012, p. 171.

(por ejemplo, activos de información y activos de TI) para identificar la importancia de cada uno y sus interdependencias con los riesgos de seguridad y TI.

b. Las empresas deben identificar y medir todos los riesgos relevantes de TI y seguridad a los que están expuestos y clasificar los procesos y actividades comerciales identificados, funciones comerciales, roles y activos (por ejemplo, activos de información y activos de TI) en términos de importancia. Las empresas también deben evaluar los requisitos de protección de, al menos, la confidencialidad, integridad y disponibilidad de esos procesos y actividades comerciales, funciones comerciales, roles y activos (por ejemplo, activos de información y activos de TI). Deben identificarse los propietarios de activos, que son responsables de la clasificación de los activos.

c. Los métodos utilizados para determinar la criticidad, así como el nivel de protección requerido (en particular, con respecto a los objetivos de protección de integridad, disponibilidad y confidencialidad), deben garantizar que los requisitos de protección resultantes sean consistentes y completos.

d. La medición de los riesgos de seguridad y TI debe realizarse sobre la base de los criterios definidos de riesgo de seguridad y TI, teniendo en cuenta la importancia de sus procesos y actividades comerciales, funciones comerciales, roles y activos (por ejemplo, activos de información y activos de TI), extensión de vulnerabilidades conocidas e incidentes anteriores que impactaron en la empresa.

e. La evaluación de las TI y los riesgos de seguridad debe llevarse a cabo y ser documentada regularmente. Esta evaluación también debe realizarse antes de cualquier cambio importante en la infraestructura, procesos o procedimientos que afecten a los procesos y actividades comerciales, funciones comerciales, roles y activos (por ejemplo, activos de información y activos de TI).

f. En función de su evaluación de riesgos, las empresas deberían, al menos, definir e implementar medidas para gestionar los riesgos identificados de TI y seguridad y proteger los activos de información de acuerdo con su clasificación. Esto debería incluir la definición de medidas para gestionar los riesgos residuales restantes.

Los resultados del proceso de gestión de riesgos de TI y seguridad deben ser aprobados por la alta dirección y transferidos al proceso de gestión de riesgos operativos como parte de la gestión general de riesgos de las empresas.

La *función de auditoría* interna también cumple su función dentro del sistema. Según la directriz 5, la gobernanza, los sistemas y los procesos de las empresas para sus riesgos de TI y seguridad deben ser auditados periódicamente de acuerdo con el plan de auditoría de las empresas por auditores con suficiente conocimiento, habilidades y experiencia en TI y riesgos de seguridad, para proporcionar una garantía independiente de su efectividad para la alta dirección. La frecuencia y el enfoque de tales auditorías deben ser proporcionales a los riesgos relevantes de TI y seguridad.

La seguridad y continuidad de las operaciones deben ser entendidas como procesos a gestionar por la organización. Es decir, los requisitos de seguridad y continuidad impuestos deben ser gestionados dentro del sistema de gobernanza de la organización. Esto se consigue no solo con la implantación de los controles de seguridad y continuidad, sino también con la implicación de la alta dirección. Tal y como hemos explicado, la gestión de los procesos operativos de la entidad aseguradora les corresponde a las personas designadas, pero estableciendo un canal de implicación por parte de la alta dirección.

Debido a la entidad que recobra la seguridad de la información, la directriz 6 impone a las entidades la creación de una *función de seguridad de la información* que se incluya dentro del sistema de gobernanza y goce de los principios de autonomía e independencia. Entendemos, por lo tanto, que a esta función se le aplicará por analogía las disposiciones generales del artículo 268 del Reglamento de Solvencia II. Las obligaciones de esta función vendrían a ser (directriz 7):

- definir y mantener la política de seguridad de la información para las empresas y controlar su despliegue;

- informar y asesorar a la alta dirección periódicamente, y según sea necesario, sobre el estado de la seguridad de la información y su evolución;

- supervisar y revisar la implementación de las medidas de seguridad de la información;

- garantizar que se cumplan los requisitos de seguridad de la información al utilizar proveedores de servicios;

- garantizar que todos los empleados y proveedores de servicios que acceden a la información y los sistemas estén adecuadamente informados de la política de seguridad de la información, por ejemplo, a través de sesiones de capacitación y sensibilización sobre seguridad de la información; y

- coordinar el examen de incidentes operacionales o de seguridad e informar sobre los relevantes a la alta dirección.

Por último, los sistemas de control interno también juegan su papel en el control del cumplimiento de la estrategia de TI de la organización, tal y como dice la directriz 2. Por eso la entidad aseguradora debe adoptar un sistema de control interno de TI que permita verificar el cumplimiento del objetivo comentado anteriormente[78].

La gestión de las TI de la organización juega un papel primordial a la hora de prestar el soporte adecuado a las funciones críticas y fundamentales existentes en la entidad aseguradora. La externalización de estas funciones debe hacerse siguiendo la sección 11 de las Directrices sobre gobernanza de la EIOPA[79], y en caso de que esta externalización se efectúe en favor de proveedores *cloud,* deberán seguirse las Directrices sobre la externalización a proveedores de servicios en la nube[80].

[78] A estos efectos, el marco de control interno COBIT 2019 nos proporciona unas directrices para el establecimiento de un marco de control interno de las TI basado en la evaluación periódica de unos objetivos de control sobre los procesos de gobernanza y la gestión, sin embargo, no es posible demostrar la conformidad por una entidad externa, al no estar bajo el objeto de acreditación de un organismo nacional de acreditación.

[79] EIOPA-BoS-14/253 ES.

[80] EIOPA-BoS-20-002.

Respecto a la evaluación interna de los riesgos y de la solvencia, la EIOPA, en la *Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector*[81], especifica que se "debe incluir en dicha evaluación los riesgos materiales a los cuales está expuesta la entidad aseguradora". No se puede negar que los riesgos de TI actualmente tienen una gran incidencia en la consecución de los objetivos de la entidad, por lo que insta a estas a incluir en la evaluación interna de los riesgos y de la solvencia la evaluación de estos riesgos.

Las obligaciones recogidas no han sido escogidas al azar, sino que están basadas fundamentalmente en los estándares internacionales que rigen tanto para la continuidad de las operaciones como para la seguridad de la información. Para demostrar el cumplimiento de estas obligaciones, la adopción de sistemas de gestión basados en estándares internacionales permite certificar la conformidad con el esquema presentado. En este sentido, contamos con diversos sistemas de gestión emitidos por la ISO que permiten certificar los siguientes sistemas de gestión:

- *ISO/IEC 27001:2013 - Sistemas de Gestión de Seguridad de la Información (SGSI).* El objetivo de la norma es prestar guías y directrices a una organización para que adopte un SGSI basado en la mejora continua, que proteja la confidencialidad, integridad y disponibilidad de la información.

- *ISO 22301:2019 - Sistemas de Gestión de Continuidad de Negocio (SGCN).* La norma aporta guías y directrices para la adopción de un SGCN con el fin de asegurar la continuidad de los servicios tras la existencia de un incidente.

- *ISO/IEC 20000-1:2018 – Sistemas de Gestión de Servicios de TI (SGTI).* La norma presenta guías y directrices para la implementación de un SGTI con el objetivo de gestionar un servicio de TI sobre la base de diferentes prácticas que sostienen un servicio de TI con el fin de generar valor.

[81] JC 2019 26.

Los sistemas de gestión basados en la mejora continua de la ISO se caracterizan por lo siguiente:

- La implicación de la alta dirección mediante la asignación de recursos, establecimiento de políticas y supervisión del desempeño del sistema.

- La gestión de los riesgos que afectan a los objetivos de la organización.

- La exigencia de auditar la eficacia del sistema anualmente.

- La necesidad de establecer indicadores de eficacia y desempeño para determinar el cumplimiento de los objetivos.

Se puede demostrar la conformidad con el estándar mediante una auditoría externa de una entidad de certificación acreditada por un organismo nacional de acreditación, como puede ser ENAC según el Reglamento (CE) 765/2008 del Parlamento Europeo y el Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos. La certificación acreditada por ENAC, o entidad similar, si bien tiene el valor probatorio de un documento privado, el Tribunal Supremo, en la STS 1623/2016, de 4 julio de 2016, de la Sala Tercera, establece que merece de un valor añadido por la intervención de un organismo nacional de acreditación[82].

Las certificaciones emitidas por entidades de certificación acreditadas tienen las siguientes características[83]:

- Reconocimiento internacional a través de un sistema de acuerdos internacionales entre organismos nacionales de acreditación.

[82] FJ 14.º: "La consecuencia de lo expuesto es que los trabajos –documentos de inspección y certificaciones– de las entidades de inspección y certificación acreditadas no tienen el valor de documento público, sino privado, pero con el valor de que en ellos se hacen constar datos por unas entidades que sí han sido acreditadas para tal fin porque la ENAC como acreditadora entiende que reúnen las condiciones de imparcialidad y suficiencia técnica para asumir tal cometido".

[83] Disponible en: https://www.enac.es/documents/7020/15700/diferencias_certificacion_acreditada_no_creditada/1b14b86d-c848-4a24-9493-5df9ba9662b1 (fecha de consulta: 1-10-2021).

- Confianza en la capacidad técnica del certificador.

- Confianza añadida en los clientes, que aceptarán con más fiabilidad la información contenida en un certificado acreditado.

- Defensa ante posibles malas prácticas, ya que tanto las empresas certificadas como los usuarios finales de productos o servicios cubiertos por un certificado acreditado pueden presentar reclamaciones ante el organismo si consideran que un certificador ha incumplido los criterios de acreditación.

- Reducción de los niveles de riesgo de producir o proveer un producto defectuoso o ante daños a terceros al basar las tomas de decisiones en información de confianza. Además, permite demostrar la "diligencia debida" en el caso de acción legal al ser la acreditación la herramienta universalmente aceptada como más fiable a la hora de demostrar la competencia de un evaluador.

Las certificaciones emitidas por entidades de certificación acreditadas demuestran que estas han superado un proceso independiente que asegura independencia en el proceso de certificación, pero no todas las entidades certificadoras están acreditadas, por lo que los efectos de los certificados de estos últimos son diferentes, y permiten con alta fiabilidad demostrar el cumplimiento de las obligaciones en materia de gobernanza del marco Solvencia II y, más concretamente, sobre los sistemas de IA en tanto en cuanto no esté en vigor el proceso de evaluación de la conformidad del artículo 43 de la propuesta de reglamento sobre inteligencia artificial.

5.2. EL CUMPLIMIENTO NORMATIVO BASADO EN LA GESTIÓN DE RIESGOS

Durante este último lustro, han surgido en España nuevas apuestas por parte del legislador tendente a imponer a las organizaciones una serie de obligaciones dirigidas a la prevención de un resultado lesivo contrario a la norma. Estas obligaciones se construyen sobre la adopción de conductas autoorganizativas, con el fin de prever y tratar la posibilidad de que determinadas conductas no se materialicen, basadas en un modelo autorregulatorio.

Esta práctica, que nos puede parecer muy novedosa en países como España, es conocida como programas de cumplimiento normativo o programas de *compliance,* y ha venido a implementar una nueva base regulatoria en los Estados para extender las obligaciones a lugares donde el Estado no puede actuar. Es decir, el Estado ha delegado parte del cumplimiento en las propias organizaciones, que serán las encargadas de detectar posibles incumplimientos. Este modelo está actualmente en expansión en diversas ramas jurídicas, como es en la legislación ambiental, penal y protección de datos, al exigir a las organizaciones programas basados en una gestión de riesgos, con la obligación ante la autoridad correspondiente de demostrar que la gestión realizada ha sido eficaz para haber tratado los riesgos identificados.

En el ámbito asegurador, la gestión de riesgos supone un elemento nuclear en su marco legal, marcado por Solvencia II –que será explicado en el presente capítulo–, puesto que otorga una ventaja competitiva ante otros operadores con estructuras de gestión deficientes[84].

5.2.1. Origen y concepto del cumplimiento normativo

La primera regulación sobre las organizaciones se detalla en Estados Unidos con las primeras regulaciones antimonopolio y para la fabricación de alimentos y medicamentos, y la creación de las correspondientes autoridades regulatorias[85]. A mediados del siglo XX, se ejecutan importantes procesos penales contra empresas estadounidenses, que utilizan como medio de exoneración de las penas que puedan llegar a recibir. Esto era, en un principio, la motivación extrínseca que las organizaciones sufrían para llevar a cabo la adopción de estos programas centrados en el cumplimiento del ordenamiento jurídico, una suerte de "*compliance* objetivo".

[84] *Vid*. Pérez Pérez, J. (coord.), *Gestión de riesgos en entidades aseguradoras. Solvencia II y su impacto regulatorio,* Delta Publicaciones, Madrid, 2016, p. 394.

[85] *Vid*. Del Rosal Blasco, B., "El origen de los programas de cumplimiento normativo penal *(compliance program)*", en Bacigalupo Saggese, S., Feijoo Sánchez, B. y Echano Basaldua, J. I. (coord.), *Estudios de Derecho Penal: homenaje al profesor Miguel Bajo,* p. 543.

Actualmente, se ha avanzado en el perfilamiento del alcance de lo que realmente se considera "cumplimiento normativo". La evolución de un concepto deriva siempre de experiencias pasadas, buenas o malas, que permiten perfeccionar y adecuar las cosas a un estado, como mínimo, adecuado para la situación actual.

Pero estos estándares éticos no pueden quedarse solo en el papel. De las enseñanzas del caso Enron mostraban que los códigos éticos por sí solos no demostraban a una organización comprometida. Los "valores" de Enron estaban sustentados en un código de 64 páginas, pero que en la práctica no se reflejaba forzando al máximo la aplicación de la ley para aprovecharse de las lagunas legales. Por eso la ética empresarial ha modulado el principio empresarial de maximización de beneficios, supeditándolo a un comportamiento socialmente aceptado y ligado a unos principios éticos.

A partir de la adopción del componente ético en los programas de cumplimiento normativo, se amplió el alcance que cubren los programas. No solo se cubrían las *obligaciones* legales (leyes, reglamentos, resoluciones del regulador, contratos, sentencias, etc.), sino también aquellos compromisos adquiridos internos o externos (códigos de conducta propio o del sector, política, procedimientos internos, estándares, etc.). Estos últimos compromisos son aquellos que son asumidos por los máximos órganos de la organización, como son los órganos de administración o la junta de accionistas, y es considerado este último colectivo como el principal *stakeholder* de una organización[86]. Tanto los compromisos como las obligaciones legales son considerados las obligaciones de *compliance* existentes[87].

Como hemos visto, el cumplimiento normativo ha ido evolucionando a lo largo del tiempo, pero no solo respecto a su alcance, sino a su aplicación en las organizaciones. Es decir, la madurez del cumplimiento normativo en las organizaciones.

[86] *Vid.* Banks, T. y Liipfer, C., "General principles behind a Compliance Program: the case of compliance", en Banks, T. y Banks, F. (coords.), *Corporate Legal Compliance Handbook,* Wolters Kluwer, New York, 2020, pp. 1-4.

[87] *Vid*. Casanova, A., *Autonomía e independencia en compliance,* ASCOM, Madrid, 2019, p. 7.

La madurez del cumplimiento normativo se ha tratado por fases en su aplicación, destacando las siguientes[88]:

- *Primera fase:* la adopción de los programas de *compliance* estaban destinados al cumplimiento de sectores marcados por la fuerte protección hacia los consumidores, como el sector asegurador, farmacéutico, alimenticio, etc., pero marcado por la obligación impuesta por las autoridades reguladoras y bajo la amenaza de potentes sanciones que amenazan la continuidad del negocio.

- *Segunda fase:* el conjunto normativo aplicable a las empresas aumenta considerablemente, expandiéndose a sectores no regulados y aplicándose transversalmente. Esto puede ser la prevención del soborno o la protección de la privacidad, ampliando la aplicación a la esfera administrativa.

- *Tercera fase:* las organizaciones sufren el peso de la exigencia de los mercados, sobre todo en aquellos donde los usuarios se encuentran especialmente protegidos, por lo que estas buscan diferenciarse mediante la aplicación de buenas prácticas legales que sobrepasen a los actuales requisitos legales. Esto se logra mediante la creación de códigos de conducta tanto propios como sectoriales, aumentando el umbral de exigencia para satisfacer a las partes interesadas.

- *Cuarta etapa:* las organizaciones son el punto de mira de la sociedad. Esta ya no es conformista con el mero cumplimiento de la ley. Atrás queda el axioma donde se consideraba que la ley era el acuerdo llegado por la sociedad, debido al distanciamiento del legislador con la sociedad. Ahora, las organizaciones deben evitar realizar acciones éticamente reprobables bajo la amenaza de una pérdida global de la reputación debido a la enorme difusión en el mundo actual.

El cumplimiento normativo debe tratarse como una función, un proceso más que la organización debe gestionar, con el fin de prevenir, detectar y gestionar riesgos de *compliance* para cumplir con los objetivos de *compliance* determinados por la organización[89].

---

[88] *Op. Supra*, p. 5.

[89] *Vid*. ASCOM, *Libro Blanco de la función de compliance,* Madrid, 2017, p. 19.

5.2.2. La gestión de riesgos como base de los programas de cumplimiento normativo

5.2.2.1. La idoneidad de los estándares internacionales. La norma ISO 37301:2020

Desde los organismos internacionales han proliferado numerosas declaraciones y estándares para unificar la definición de *compliance* y unos criterios unificados para la adopción de programas de cumplimiento normativo.

Si bien existían marcos nacionales, en 2014 la International Standard Organization dictó la norma ISO 19600:2014 - Directrices para la implantación de un sistema de gestión de *compliance,* siendo el primer estándar internacional en cumplimiento normativo, y estableciendo un lenguaje común sobre qué se entiende como el idealismo de los programas de cumplimiento normativo. Debido al paso del tiempo, esta norma fue sustituida por la ISO 37301:2021 - Sistemas de gestión de cumplimiento: requisitos con orientación para su uso.

Los sistemas de gestión emitidos por la ISO se basan fundamentalmente en el concepto de mejora continua de procesos del ciclo de Demming con el objetivo de implementar, evaluar, mantener y desarrollar la función de *compliance*. Esta idea es acorde con el concepto de la función de *compliance* como un proceso que debe ser gestionado por la organización, centrado en la mejora continua.

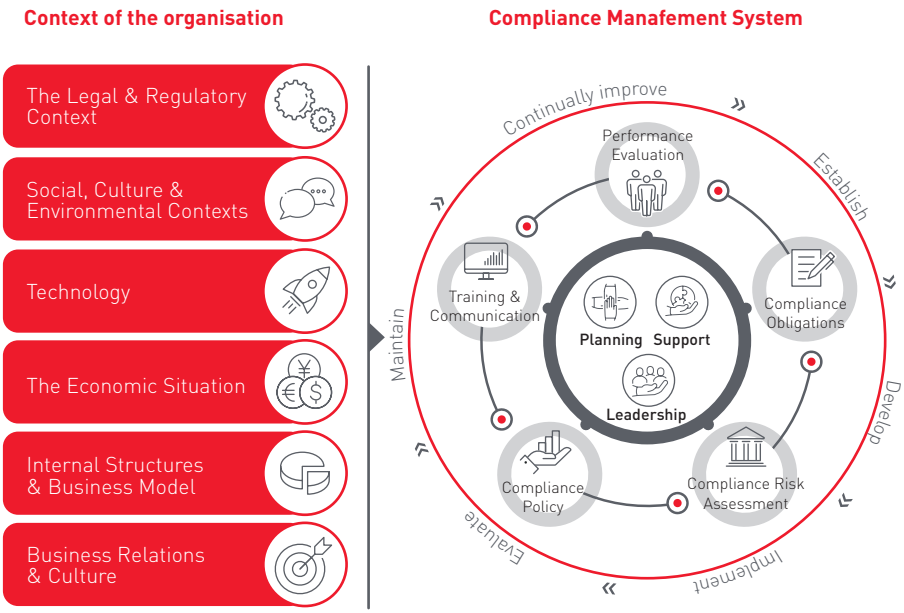
La principal diferencia de la ISO 37301:2021 con la ISO 19600:2014, aparte de la actualización de sus contenidos, es la posibilidad de que esta norma sea *certificable,* demostrando así la conformidad con la norma mediante una auditoría de certificación.

Mediante el esquema presentado a continuación, se pretende integrar una cultura del cumplimiento en las personas pertenecientes a la organización, creando una función de *compliance* integrada en los procesos operacionales de esta[90], actuando de forma transversal, puesto que el cumplimiento no debe ser nunca una traba

[90] *Vid*. ASCOM, *Manual de estudio para la certificación CESCOM*, Madrid, 2018, p. 104.

para los objetivos de negocio, sino una herramienta de salud corporativa que apoye la toma de decisiones.

Sistema de gestión de cumplimiento



Fuente: ISO 37301.

Como se muestra en la imagen anterior, la ISO 37301:2021 especifica unas directrices que toda organización debería acatar para lograr la aplicación de un sistema de gestión de cumplimiento normativo de forma iterativa.

La norma parte de unas definiciones que perfilan el objeto de gestión de esta, que es el *riesgo de cumplimiento,* definido como la probabilidad de ocurrencia y las consecuencias del incumplimiento con la organización de las obligaciones de cumplimiento[91]. La gestión de estos riesgos es clave en la implantación del sistema

[91] Requisitos que una organización obligatoriamente debe cumplir, así como aquellos que la organización elige voluntariamente cumplir.

de gestión de cumplimiento normativo, mediante la identificación de las obligaciones de cumplimiento, la valoración de las consecuencias y la probabilidad del riesgo, y la evaluación por la organización. A este proceso se le denomina *apreciación del riesgo,* y será explicado más adelante.

Llegados a este punto, se ponen en valor modelos en los que confluyen varias funciones de control en una organización basadas en el concepto de gobierno, riesgo y cumplimiento (GRC)[92]. Desde la función de *gobernanza* se impulsa la aplicación de las buenas prácticas en la gestión e implementa los valores rectores que seguirán todos sus miembros, siendo también compromisos dentro del alcance del concepto de *compliance*. Por otro lado, la función de gestión de riesgos debería contemplar en todo momento los riesgos legales, al igual que los riesgos típicos que las empresas de centran en primer lugar en gestionar, como son los riesgos financieros u operativos.

La clave de esta gestión se centra en operarlos de forma conjunta, puesto que, de hacerlo de forma separada, se esperan lagunas en su consistencia y duplicidades en los *outcomes* que se obtienen de estos procesos.

En este sentido, hemos observado que el uso de la IA por parte de las organizaciones hace surgir nuevos riesgos legales que deben ser identificados y tratados. Los programas de cumplimiento normativo no pueden obviar las actividades derivadas del uso de esta tecnología. La función de *compliance,* dentro de un modelo de gestión GRC, debe actuar para arrojar luz a la dificultad que supone la gestión de esta tecnología para afrontar los retos regulatorios que el legislador implementará.

5.2.2.2. La gestión de los riesgos legales. Los estándares ISO 31000:2018 e ISO 31022

El concepto de riesgo se deviene como elemento central a lo largo del presente estudio. En puntos anteriores, hemos precisado de forma práctica los riesgos asociados al uso de sistemas de IA mediante métodos directos.

[92] *Vid.* Casanova, A., *Autonomía e independencia en compliance,* ASCOM, Madrid, 2019.

El riesgo es inherente a una organización respecto al desempeño de cada actividad que esta desempeñe, aunque su concepto y aplicación difiera dependiendo de la materia en la que nos encontremos, por ejemplo, en materia de seguridad de la información ambiental, o financiera, cada uno con una definición adaptada a la materia gestionada, y ayuda a mejorar el desempeño en estas áreas de gestión[93].

La gestión del riesgo es un elemento que forma parte de la gobernanza de la organización[94] y afecta tanto a los gestores como a las partes interesadas de la organización. En caso de estos últimos, el proceso de gestión de riesgos sirve para acreditar, tanto ante la junta de accionistas como ante los clientes y Administraciones públicas, una gestión solvente de la organización; por ello se requiere un lenguaje común entre las partes para entender las interpretaciones en los resultados de la organización ante terceros. Un proceso de gestión de riesgos ininteligible disminuirá la confianza ante terceros o, incluso, podrá conllevar sanciones administrativas.

De esta necesidad, surgen propuestas internacionales que pretenden unificar la terminología y el proceso de gestión de riesgo para crear estándares internacionalmente aceptados por las organizaciones. De todos, destacamos el estándar ISO 31000:2018 Gestión de riesgos.

Dicho estándar recomienda una metodología de apreciación y tratamiento de riesgos asimilado a un proceso de mejora continua de un sistema de gestión, asumiendo la premisa de la gestión de riesgos como un proceso que debe ser gestionado. Mediante esta metodología, propone un concepto unificado de riesgo, definiéndolo como "el efecto de la incertidumbre sobre los objetivos". No siempre un riesgo tiene una connotación negativa. Según la propia norma, el efecto es "una desviación respecto a lo previsto, positivo o negativo, y puede abordar, crear o resultar en oportunidades o amenazas".

Según esta definición, por ejemplo, la retirada de un competidor del mercado constituye un riesgo respecto a la consecución de los objetivos, que pueden ser el aumento de la cuota de mercado, por lo que se crean nuevas oportunidades.

---

[93] *Vid*. Escorial, Á., *et. al. Guía para la aplicación de UNE-ISO 31000:2018*, AENOR ediciones, Madrid, 2018, p. 35.

[94] *Vid. Op. Supra,* p. 13.

A todo esto, debido a los avances respecto al desarrollo de la función de cumplimiento normativo y las exigencias normativas que exigen a las organizaciones implantar una función de gestión de riesgos para atajar determinados riesgos legales, surge la necesidad de proporcionar un marco estandarizado para entender el proceso de análisis y gestión de riesgos desde un punto de vista regulatorio. Para ello, la ISO emitió la ISO 31022:2020 Gestión de riesgos legales.

Este estándar se presenta como un complemento a la norma ISO 31000, que interpreta los requisitos de esta norma conforme a las recomendaciones propias del análisis y gestión de los riesgos legales.

La gestión de riesgos legales tiene como fin la creación y protección de valor en las organizaciones sobre la base de los siguientes principios del sistema de gestión de riesgos legales:

a. *Integrado.* La gestión de riesgos legales debe ser parte de la estrategia global de planificación, toma de decisiones y gestión diaria. Debe estar embebida en responsabilidades plasmadas en normativas y procedimientos, e incluidas en el sistema de control interno y cumplimiento normativo.

b. *Estructurado y exhaustivo.* La gestión de riesgos legales debe seguir un marco genérico de gestión de riesgos, produciendo resultados coherentes y comparables, y considerar diferentes escenarios plausibles y factores de riesgo.

c. *Personalizado.* La gestión de riesgos legales debe ajustarse al contexto definido por la organización, en particular, sobre la comprensión del impacto de los riesgos y la prevención de su ocurrencia.

d. *Inclusivo.* La gestión de riesgos legales debe involucrar a todos los *stakeholders,* incluir a juristas en el trabajo de los jefes de negocio y medir los beneficios de compartir información legal ante la confidencialidad.

e. *Dinámico.* La gestión de riesgos legales debe anticipar, detectar, reconocer y responder a eventos y cambios en el contexto como nueva legislación o políticas públicas, incluyendo mecanismos de alerta temprana para riesgos emergentes.

f. *Mejor información disponible.* La gestión de riesgos legales debe usar información de fuentes internas y externas, primar la experiencia de asesores jurídicos internos, *business intelligence,* bases de datos legales, consejeros y firmas externas.

g. *Factores humanos y culturales.* La gestión de riesgos legales debe evitar sesgos en las diferentes opiniones de los *stakeholders,* hacer que la junta de accionistas se conciencie sobre los efectos legales de sus acciones y considerar la influencia de la cultura de cumplimiento normativo.

h. *Mejora continua.* La gestión de riesgos legales debe aprender de revisiones posteriores, mejores prácticas y consejo profesional de personal interno o externo a la organización.

i. El principio de *equidad* debe guiar la gestión del riesgo legal, incluye gestionar los conflictos de intereses y proporciona una opinión independiente en las decisiones y apoyo en la debida diligencia y justicia para los mejores intereses de la organización.

Tradicionalmente, el riesgo legal se ha incluido en el concepto de riesgo operacional, a ello apunta el Comité de Supervisión Bancaria de Basilea, con la definición de "riesgo de pérdida debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos"[95], similar a la recogida en el artículo 13.33) de la directiva Solvencia II.

En este sentido, la ISO 31022 aporta una definición de riesgo legal[96,97], que queda estipulado como "el efecto de la incertidumbre sobre los objetivos en relación con

[95] *Vid.* Comité de Supervisión Bancaria de Basilea, *Basilea III: finalización de las reformas poscrisis,* 2017, p. 143.

[96] La definición de *riesgo legal* es similar a la recogida en el documento *El cumplimiento y la función de cumplimiento en los bancos* del Comité de Basilea de Supervisión Bancaria de 2005, que lo define como "riesgo de sanciones legales o normativas, pérdida financiera material o pérdida de reputación que un banco puede sufrir como resultado de incumplir con las leyes, regulaciones, normas, estándares de autorregulación de la organización y códigos de conducta aplicables a sus actividades bancarias".

[97] En este sentido, el concepto de riesgo legal es asimilable al concepto de riesgo de cumplimiento de la ISO 37301:2020.

las materias legales, regulatorias y no contractuales". A continuación, la norma crea una clasificación de las fuentes de riesgos legales que, a su vez, podemos clasificarlas dependiendo del impacto en la organización según sean riesgos directos o indirectos[98]:

- Como *riesgo indirecto,* destacamos las incidencias legales que puedan tener su origen en decisiones políticas, leyes nacionales o internacionales, incluyendo leyes estatutarias, jurisprudencia o derecho consuetudinario, actos administrativos, órdenes regulatorias, sentencias y laudos, reglas procesales, memorandos de entendimiento o contratos. El riesgo legal crece con la incertidumbre sobre las leyes, normativa y acciones legales aplicables. Por tanto, el riesgo legal incluye la exigibilidad legal, la legalidad de los instrumentos y la exposición a cambios no anticipados en leyes y regulaciones[99].

- En cuanto a *riesgos directos,* destacamos los siguientes:

    a. El riesgo respecto a asuntos contractuales que se relacionan con las situaciones en que la organización no cumple con sus obligaciones contractuales, no hace cumplir sus derechos contractuales o celebra contratos con términos y condiciones onerosos, inadecuados, injustos y/o inaplicables.

    b. El riesgo de los derechos no contractuales es el riesgo de que la organización no haga valer sus derechos no contractuales. Por ejemplo, el hecho de que una organización no haga cumplir sus derechos de propiedad intelectual, como sus derechos relacionados con derechos de autor, marcas registradas, patentes, secretos comerciales e información confidencial contra un tercero.

    c. El riesgo de las obligaciones no contractuales es el riesgo de que el comportamiento y la toma de decisiones de la organización puedan dar lugar a un comportamiento ilegal, un incumplimiento del deber de cuidado (o

[98] *Vid*. Ceballos, D., "Una propuesta de indicador de riesgo legal", *2.ª Reunión de Investigación en Seguros y Gestión de Riesgos*, Castro Urdiales (Cantabria), abril de 2007.

[99] *Vid*. Puyol, J., *El modelo de evaluación de riesgos en la protección de datos EIPD/PIA's*, Tirant lo Blanch, Valencia, 2018, p. 82.

deber civil) no legislativo a terceros. Esto podría incluir una organización que infringe los derechos de propiedad intelectual de terceros, el incumplimiento de las normas de atención requeridas debido a los clientes (como la venta incorrecta) o el uso o la administración inapropiados de las redes sociales que resultan en un reclamo de difamación o difamación de terceros.

El concepto de riesgo en sí existe sobre la base de la existencia de vulnerabilidades en los procesos de la organización que son explotadas por las amenazas que atentan contra los objetivos de la organización.

a. Una *vulnerabilidad* es un factor de riesgo interno de un sistema o sujeto expuesto a una amenaza, correspondiente a su predisposición intrínseca a ser afectado o de ser susceptible de sufrir un daño[100].

b. Una *amenaza* es cualquier acción tanto interna como externa que explota una vulnerabilidad.

La relación existente entre ambos términos deriva de la propia convocación de ambos, siendo una relación de continencia intrínseca en la que si no existe amenaza, ningún elemento puede ser vulnerable, y sin vulnerabilidad, no puede ser amenazado[101].

Por ejemplo, una entidad aseguradora debe cumplir las obligaciones de identificación del titular derivadas de la Ley 10/2010 de prevención de blanqueo de capitales. Esta entidad puede no haber implementado correctamente las políticas por falta de cultura y concienciación (vulnerabilidad). Posteriormente, un empleado de la entidad no tiene en cuenta esta obligación a la hora de la tramitación (amenaza), procediendo a la contratación del producto sin la solicitud de los documentos pertinentes, por lo que si la organización hubiese adquirido dicha cultura, la amenaza no habría podido explotar la vulnerabilidad de la organización.

[100] *Vid*. Cardona, O., *Estimación holística del riesgo sísmico utilizando sistemas dinámicos complejos,* Tesis doctoral presentada ante la Universidad Politécnica de Cataluña, Barcelona, 2002, p. 11.

[101] *Vid. Op. Supra.*

5.2.3. La implementación de la gestión de los riesgos legales dentro de Solvencia II de acuerdo con la ISO 31022:2020

El marco Solvencia II proporciona un punto de partida privilegiado para la implantación del proceso de gestión de riesgos legales por el sistema de gobernanza exigido, explicado en los puntos anteriores. A su vez, la ISO 31022 estipula unos requisitos mínimos que deben implementarse. Estos requisitos se incluyen en el denominado marco de referencia de la gestión del riesgo de la norma ISO 31000:2018, con el fin de asistir a la organización en integrar la gestión del riesgo en todas sus actividades y funciones significativas.

Marco de referencia de gestión de riesgos legales

Fuente: ISO 31022.

El marco de referencia está formado por los siguientes elementos:

1. *Integración.* La integración de la gestión del riesgo depende de la comprensión de las estructuras y el contexto de la organización. Partiendo de la existencia de liderazgo y compromiso, la alta dirección puede hacerla patente mediante una asimilación del riesgo dentro de las actividades de la organización y de las partes interesadas en relación con la organización. Por ello, debe

establecerse un marco de gestión de riesgos legales en línea con los objetivos establecidos.

2. *Diseño.* Consiste en establecer una estructura personalizada de la gestión del riesgo legal en la organización, para lo que es necesario:

   a. Establecer el *contexto de la organización,* también fase primordial del proceso de gestión de riesgos.

   b. Demostrar el compromiso de la alta dirección mediante *la adopción de una política por parte de la alta dirección* con referencia específica a la gestión de los riesgos legales. Esta política refleja el compromiso de la alta dirección con la gestión del riesgo legal. Se deberá reflejar en dicha política la integración de la gestión de los riesgos en referencia a los objetivos en conflicto, el compromiso de medición, supervisión y mejora continua. La adopción de políticas por parte de la alta dirección consiste en uno de los requisitos principales del sistema de gobernanza de Solvencia II. En concreto, tal y como dictan las Directrices sobre el sistema de gobernanza de la EIOPA, la alta dirección es el último responsable de garantizar la eficacia del sistema de gestión de riesgos, establecer el perfil de riesgo de la empresa y los límites de tolerancia al riesgo, así como de aprobar las principales estrategias y políticas de gestión de riesgos. En su directriz 18, se contemplan los requisitos que debe contener la política de gestión de riesgos:

      – definir las categorías de riesgo y los métodos para medir los riesgos;

      – determinar cómo gestiona la empresa cada categoría, área de riesgos y cualquier agregación potencial de riesgos;

      – describir la conexión con la evaluación de las necesidades globales de solvencia según se identifican en la evaluación prospectiva de los propios riesgos de la empresa, los requisitos legales de capital y los límites de tolerancia al riesgo de la empresa;

- especificar los límites de tolerancia al riesgo para cada tipo de riesgo de acuerdo con el perfil de riesgo global de la empresa; y

- describir la frecuencia y el contenido de las pruebas periódicas de tensión y las situaciones que requieren pruebas de tensión específicas.

Esta política debe recoger aspectos de gestión en relación con los siguientes riesgos:

- Riesgo de suscripción y constitución de reservas.

- Riesgo operacional.

- Técnicas de reducción del riesgo.

- Riesgo estratégico y de reputación.

- Gestión de activos y pasivos.

- Riesgo de liquidez.

c. Asignar los roles y responsabilidades pertinentes por parte de la alta dirección, y que estas se comuniquen adecuadamente. Las responsabilidades designadas deberán desempeñar las siguientes actividades, según su asignación:

    - Revisar periódicamente el progreso de la implementación de los planes para la gestión de los riesgos legales.

    - Desarrollar planes de gestión de la continuidad integrados para asegurar que las consecuencias derivadas de la materialización de los riesgos legales son gestionadas adecuadamente.

- Clarificar las responsabilidades y rendición de cuentas de los miembros que son responsables de la ejecución de las medidas de tratamiento de los riesgos legales, sistema de reporte y mantenimiento del marco de riesgo legal.

- Registrar e informar sobre los riesgos legales.

Estas responsabilidades pueden ser efectuadas por las diferentes funciones que una entidad aseguradora debe tener de acuerdo con el marco de Solvencia II (gestión de riesgos, verificación del cumplimiento, seguridad de la información, actuarial y auditoría interna). Si bien estas actividades pueden ser desarrolladas individualmente, se vuelve complicado cuando para su correcta ejecución deben intervenir dos o más funciones, por lo que se ve conveniente que estas funciones puedan ser coordinadas por un órgano dentro de la organización, un *comité de gestión integral,* donde puedan intervenir todas las funciones y el delegado de la alta dirección responsable del compromiso con la gestión del riesgo. Sin embargo, se ve necesario individualizar a los propietarios de los riesgos, quienes tienen la función de implementar las medidas designadas en el plan de tratamiento de los riesgos, como parte de la primera línea de defensa, cuya propiedad recaerá en los responsables operativos de la organización.

d. Asignar los recursos por parte de la alta dirección, ya sea mediante recursos humanos, financieros o formativos.

e. Establecer la comunicación y la consulta, asegurando los canales de comunicación adecuados, el público objetivo y recabando las opiniones de las partes interesadas. Esta comunicación debe ser vertical entre la alta dirección, gestores del riesgo legal, los propietarios del riesgo y operarios, y horizontalmente hacia las partes interesadas.

3. *Implementación.* Una vez diseñado el marco, se debe planificar su implementación en la organización mediante un plan apropiado y los recursos pertinentes, estableciendo mecanismos de verificación que permita asegurarse de

que las disposiciones de la organización se emplean en la práctica, por ejemplo, mediante la función de auditoría interna.

4. *Valoración.* Tras la implementación, debe medirse el desempeño del marco de referencia de la gestión del riesgo en relación con su propósito y el plan estratégico de la organización mediante el establecimiento de indicadores y métricas, y promover su actualización para adecuarse a la consecución de los objetivos. El sistema de gobernanza de Solvencia II exige que todas sus funciones y sistemas que lo componen sean eficaces, por lo que las entidades aseguradoras deben implementar mecanismos de evaluación del desempeño, evaluándose de manera planificada y reportando los resultados a la alta dirección.

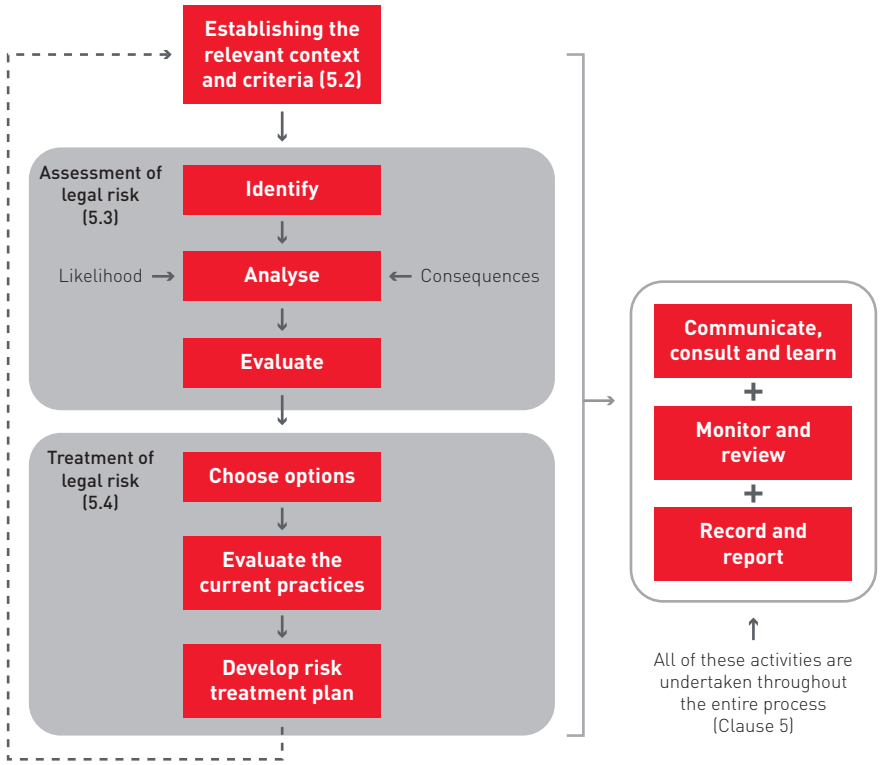
5. *Mejora.* El marco de referencia debe adaptarse puntualmente a los cambios en el contexto de la organización, los procesos, las estructuras y los servicios. La mejora continua del marco de referencia de gestión de riesgos es un proceso que la organización debe asimilar y debe tomarse como base los objetivos de negocio estipulados.

Sobre la base de este marco adaptado, la organización debe emprender el proceso de gestión de riesgos.

5.2.4. El proceso de gestión de los riesgos legales

Como se ha explicado anteriormente, el proceso de análisis y gestión de riesgos es un proceso iterativo y debe estar integrado en todas las actividades y operaciones de la organización con el fin de integrarse en el proceso de toma de decisiones, no solo en las estratégicas.

Proceso de gestión de riesgos legales



Fuente: ISO 31022.

A su vez, para abordar cada proceso, es necesario que la organización utilice técnicas que ayuden a mejorar la forma en la que la incertidumbre es tenida en cuenta y ayuda a entender el riesgo. Las técnicas de apreciación de riesgo son utilizadas para asistir en la toma de decisiones en las que existe incertidumbre. Respecto a las técnicas de apreciación de riesgo, se utiliza la IEC 31010 Gestión de riesgos - Técnicas de apreciación de riesgos para seleccionar las técnicas que consideramos más adecuadas para abordar el proceso.

CASO PRÁCTICO

Se presenta la siguiente organización sita en España, México, Colombia y Argentina, con la necesidad de gestionar los riesgos legales de un sistema de IA basado en el tratamiento de datos personales para la aplicación de toma de decisiones automatizadas con el fin de determinar la prima aplicable al tomador del seguro.

5.2.4.1. Comprensión de la organización y su contexto

Cuando se lleva a cabo el proceso de apreciación de riesgos, aquellos involucrados deben tener una visión amplia de las circunstancias por las que se toman las decisiones; por eso se deberán identificar y entender las cuestiones internas y externas de la organización. El contexto de la organización determina el marco ambiental en el que una organización busca definir sus objetivos.

Los *objetivos* pueden ser de diferentes categorías, por ejemplo, financieros, operacionales, sociales, ambientales, comerciales, de recursos humanos, seguridad e higiene. Son expectativas basadas en las creencias, que nos proporcionan un grado de certeza, y en las preferencias, que construyen la magnitud del impacto esperado. Pero estas creencias y preferencias están sujetas a errores, riesgos y sesgos basados en nuestra experiencia y en la información considerada, que nunca pueden ser exhaustivas ni veraces; con lo que nuestras expectativas diferirán del resultado alcanzable si no se corrigen[102].

Puesto que el riesgo se debe tomar sobre la base de los objetivos, estos deben entenderse en el contexto de la organización, basado en factores internos como externos, ya sean negativos o positivos.

[102] *Vid*. Escorial, Á. *et. al. Guía para la aplicación de UNE-ISO 31000:2018*, *op. cit*., p. 119.

Los *factores internos* son aquellos que se encuentran bajo el control de la organización. Desde el punto de vista de la gestión de los riesgos legales, se deben tener en cuenta los siguientes elementos:

- La naturaleza legal de la entidad y la estructura de esta.
- El modelo de negocio o actividad principal.
- La normativa interna aplicable por la organización.
- Los activos legales de la organización (datos personales, propiedad intelectual e industrial, licencias, etc.).
- Experiencias pasadas.
- Obligaciones contractuales actuales.

Los *factores externos* son aquellos que no se encuentran bajo el control de la organización, pero afectan a la organización. Ejemplos de estos factores serían:

- Leyes nacionales e internacionales que afectan a la organización en los Estados donde se desempeñan las actividades.
- Cambios normativos.
- Acuerdos internacionales bilaterales o multilaterales.
- Reclamaciones por terceras partes.
- Leyes aplicables a los integrantes de la cadena de valor.
- Partes interesadas, como sindicatos, patronal, asesores externos, reguladores.

Respecto a los factores externos, se debe lograr la intervención de los *stakeholders* en el proceso debido a su conocimiento y perspectiva considerada. Su inclusión

ayuda a asegurar que la información utilizada sea válida, y que los *stakeholders* entiendan las razones detrás de las decisiones.

CASO PRÁCTICO

La entidad determina los siguientes factores tanto internos como externos sobre la base de reuniones mantenidas con los *stakeholders* de la organización:

a. Factores internos
   - La organización es una sociedad anónima.
   - Presta servicios en el sector asegurador, operando en los ramos de vida, daños.
   - Se tienen los siguientes activos: programas informáticos, propiedad de activos de hardware, derechos de cobros.
   - Existen numerosos litigios contra la organización debido a irregularidades en la concesión de las indemnizaciones correspondientes; ha conllevado a resoluciones judiciales en su contra.
   - La organización tiene implementadas políticas y procedimientos relacionados con la gestión del sector asegurador, blanqueo de capitales.
   - Contrae obligaciones con sus clientes, regidas por la Ley de Contrato del Seguro.

b. Factores externos
   - Las principales legislaciones que aplican a la organización son: protección de datos, asegurador, sociedades de capital, solo en España.
   - Los grupos de interés son: Dirección General del Seguro, AEPD, junta de accionistas, clientes, proveedores y empleados.

5.2.4.2. Definición de los criterios de riesgo para la toma de decisiones

Los criterios de riesgo para la toma de decisiones son unidades de medidas que son identificadas y definidas para evaluar un nivel de riesgo importante o aceptable de un riesgo legal para la organización. Deben reflejar los objetivos, valores, recursos, preferencias y la tolerancia general al riesgo en relación con el riesgo legal.

Tradicionalmente, se ha venido utilizando los conceptos de probabilidad e impacto como definición matemática del riesgo, donde el riesgo es la función de la probabilidad por el impacto:

$$Rx = P * I$$

La *probabilidad* se refiere a la posibilidad de materialización de un evento. En el ámbito de la gestión de riesgos legales, nos referimos a la probabilidad de la materialización de un incumplimiento legal. En este punto, la organización debe determinar la fórmula más adecuada para obtener un valor lo más realista posible. Por ello, se plantean diferentes criterios que permiten alcanzar un valor de carácter objetivo:

- Las reclamaciones legales recibidas.

- El estado de madurez del Estado de derecho, como criterio comparativo en el caso de que se quiera analizar la probabilidad de materialización del evento en diferentes Estados. Se pueden utilizar series históricas o índices de referencia para alcanzar el dato, por ejemplo, el Rule of Law Index del World Justice Project[103], que proporciona un valor sobre el Estado de derecho.

- El grado de frecuencia de ejecución de la actividad objeto de análisis.

- El error humano[104], calculado a través de metodologías reconocidas, por ejemplo, mediante el método Human Error Assessment And Reduction Technique (HEART), que podemos ver en la siguiente tabla.

[103] Es una técnica de evaluación de confiabilidad humana desarrollada para ayudar a los analistas de riesgos a identificar las principales influencias en el desempeño humano y la probabilidad de error, de manera sistemática y repetible. Se basa en el principio general de que para cada tarea en la vida hay una probabilidad básica de fallo. *Vid*. William, J., "Heart—A Proposed Method for Achieving High Reliability in Process Operation by Means of Human Factors Engineering Technology", *Safety and Reliability,* vol. 3, n. 35, 2015, pp. 5-25.

[104] El riesgo legal está principalmente marcado por un factor humano que causa el riesgo, puesto que el origen de un incumplimiento se debe a una acción humana. Por ello, debe estimarse una variable respecto a la importancia del factor humano en la materialización del riesgo.

Característica de las tareas	Valor
Totalmente inhabitual realizada de forma rápida sin una idea real de las consecuencias	0,55
Desplazar o restituir el sistema a un estado nuevo u original en un único intento, sin supervisión ni procedimientos	0,26
Tarea compleja requiriendo un alto nivel de comprensión y de habilidad	0,16
Tarea sencilla realizada rápidamente o con un nivel de atención limitado	0,09
Tarea monótona y rápida de un perfil de bajo nivel	0,02
Desplazar o restituir el sistema a un nuevo estado u original según procedimientos definidos y con algunas comprobaciones	0,003
Tarea rutinaria, familiar, bien diseñada, con experiencia, ocurriendo varias veces por hora, realizada según estándares por personal muy motivado, muy formado y con mucha experiencia, totalmente consciente de las implicaciones de un fallo, con tiempo para corregir un error potencial, pero sin el beneficio de una asistencia técnica	0,0004
Responder correctamente al comando del sistema incluso cuando hay un sistema de supervisión automático que facilite una interpretación precisa del sistema	0,00002
Cualquier tarea que no se ajuste a ninguna disposición	0,03

Fuente: elaboración propia.

Por otro lado, el *impacto* refiere a las consecuencias generadas por la materialización del evento derivado de una vulnerabilidad explotada por una amenaza. El impacto puede consistir en la existencia de diferentes impactos que otorguen un enfoque global, como, por ejemplo, las consecuencias reputacionales, financieras[105] y operativas.

En la materia que nos atañe, el impacto en la materialización del incumplimiento de una norma legal es la consecuencia asociada al incumplimiento de esta, que pueden ser la pérdida de licencias de actividad, la imposición de multas administrativas, el cierre de locales y la pérdida de activos legales, como son los derechos de propiedad intelectual o de autor.

[105] Atendiendo a la ISO 37301:2020, niega la posibilidad de utilizar para obtener el impacto las consecuencias financieras del incumplimiento, puesto que la toma en consideración de este criterio excluye la existencia de los peores escenarios, y generalmente conduce a medidas de tratamiento de riesgo inadecuadas, si bien se pueden identificar.

Tras el establecimiento de los criterios para determinar las variables y, por tanto, el nivel de riesgo, la organización debe establecer el valor medible por el cual, una vez que un riesgo haya alcanzado ese umbral[106], se considera que sobre ese riesgo debe tomarse una decisión. Es decir, definir la tolerancia al riesgo. Esto no significa que, para situaciones de bajo riesgo de cumplimiento, la organización acepte el incumplimiento; en este sentido, y a diferencia de la gestión de otros riesgos donde cualquier riesgo por debajo del umbral supone la aceptación de estos, el umbral del riesgo debe servir para establecer prioridades respecto al tratamiento de los riesgos.

CASO PRÁCTICO

La organización ha establecido una metodología cualitativa basada en valores objetivos y su traslación a escalas para facilitar la toma de decisiones. Los criterios para el cálculo del riesgo son:

a. Probabilidad

La organización ha determinado una escala del 1 al 5 para determinar el valor. Para la obtención del presente valor, se utilizarán los siguientes criterios:

- La frecuencia de ejecución del servicio (F), siendo:

Valor	Descripción
1	La frecuencia de la actividad se produce entre 1 y 49 días
2	La frecuencia de la actividad se produce entre 50 y 99 días
3	La frecuencia de la actividad se produce entre 100 y 149 días
4	La frecuencia de la actividad se produce entre 150 y 249 días
5	La frecuencia de la actividad se produce entre 250 y 365 días

[106] El umbral de riesgo puede definirse como el equilibrio aceptable del crecimiento, los riesgos y el retorno, o como una medida de valor agregado a los accionistas ajustada al riesgo.

- La frecuencia estimada sobre la base de reclamaciones recibidas respecto a la rama jurídica a la que pertenece la obligación (T):

Valor	Descripción
1	No se han recibido reclamaciones
2	Se ha recibido alguna reclamación el año anterior
3	Se han recibido más de una reclamación el año anterior
4	Se han recibido hasta 20 reclamaciones el año anterior
5	Se han recibido más de 20 reclamaciones el año anterior

- El cálculo del error humano mediante la metodología HEART:

Valor	Descripción
1	El valor se encuentra entre 0,69 y 1
2	El valor se encuentra entre 0,49 y 0,68
3	El valor se encuentra entre 0,28 y 0,48
4	El valor se encuentra entre 0,14 y 0,27
5	El valor se encuentra entre 0 y 0,13

La probabilidad se obtiene sobre la base de la siguiente fórmula:

$$P = \frac{F + R + T}{3}$$

b. Impacto

- Consecuencias legales (L):

Valor	Descripción
1	Multas o indemnizaciones de hasta 55.000 €
2	Multas o indemnizaciones desde 55.001 hasta 100.000 €
3	Multas o indemnizaciones desde 100.001 hasta 300.000 € o pérdidas de activos jurídicos
4	Multas o indemnizaciones desde 300.001 hasta 600.000 € o pérdidas de activos jurídicos críticos o cierre de locales, o limitación parcial de la actividad
5	Multas o indemnizaciones de más de 600.000 €, o disolución de la persona jurídica, o clausura del servicio

- Criterio reputacional de la sanción (R):

Valor	Descripción
1	Reclamaciones contractuales o extracontractuales sin repercusión mediática
2	Reclamaciones administrativas sin repercusión mediática
3	Reclamaciones contractuales, extracontractuales, administrativas con repercusión mediática nacional
4	Reclamaciones contractuales, extracontractuales, administrativas con repercusión mediática internacional
5	Delitos

El impacto se obtiene sobre la base de la siguiente fórmula:

$$O = \frac{L * R}{2}$$

c. Criterio de aceptación

Se especifican los criterios de tolerancia al riesgo:

- Riesgos con un valor de superior a 10.
- Aquellos riesgos cuyo impacto es superior a 4.

5.2.4.3. Identificación de riesgos

Para asegurar que los riesgos legales son identificados exhaustiva, sistemática y exactamente, la norma ISO 31022 exige que la organización establezca una metodología con sus necesidades de gestión, proporcionando diferentes aproximaciones para su identificación, por ejemplo, no solo desde una perspectiva regulatoria, sino incluyendo también las consecuencias operativas de la norma. Una organización puede identificar riesgos legales relacionados con:

- sus objetivos operacionales y prioridades;

- su estructura de gobernanza, actividades y operaciones, tales como ventas, servicios, entrega, *marketing,* cálculo de primas, contratación, gestión de recursos humanos, tratamiento de información y gestión de TI;

- ciberataques, ingeniería social y otras ciberamenazas;
- las partes interesadas, como los accionistas, autoridades regulatorias, empleados, sindicatos y socios de negocio;
- la mala aplicación o interpretación del contexto legal, incumplimiento de las leyes, incumplimiento contractual, infracción de propiedad intelectual o incorrecto ejercicio de derechos;
- las responsabilidades y rendición de cuentas por la gestión de los riesgos legales después de su manifestación, que pueden desembocar en responsabilidades civiles, administrativas, penales y otras penalizaciones; y
- la aplicación de normas específicas o del Derecho internacional privado.

Los riesgos legales pueden agruparse en:

- Corporativos.
- Activos.
- Contractuales.
- Litigio.
- Regulatorios.
- Constitutivos.
- Territoriales.
- Extintivos.

5.2.4.4. Análisis del riesgo

El análisis de riesgos legales puede hacerse desde una perspectiva cualitativa o cuantitativa sobre la base de la obtención de las consecuencias asociadas a la materialización del riesgo, su probabilidad de ocurrencia y sus escenarios de riesgo. El escenario de riesgo legal estaría compuesto por el supuesto de hecho contrario a la norma y la forma en que la organización puede cometerlo.

En este punto, una vez establecidos los criterios de cálculo y los escenarios de riesgo, se debe ejecutar la fórmula acordada por la organización. Si bien la organización debe calcular el nivel de riesgo existente, el cálculo puede derivar de una concepción teórica del riesgo, actual o residual, según decidamos qué queremos calcular:

a. El *riesgo teórico* consiste en el cálculo de un riesgo potencial sobre la probabilidad e impacto del escenario de riesgo sin tener en cuenta las medidas que la organización tenga implementadas o vaya a implementar en el futuro.

b. El *riesgo real* consiste en el producto de la probabilidad e impacto teórico ponderado por el efecto mitigador de las medidas actuales y su nivel de eficacia actual.

$$Rr = Pr\left[\left(\left(Pt - VMx_1\right) - VMx_2\right) - \cdots VMx_e\right] * Ir\left[\left(\left(It - VMx_1\right) - VMx_2\right) - \cdots VMx_e\right]$$

Donde:

- *Pr*: probabilidad real;
- *Ir*: impacto real;
- *Pi*: probabilidad teórica;
- *VM*: valor de mitigación de las medidas en un valor porcentual, formado por:
  - VMt (valor teórico de mitigación de las medidas) y E (grado de eficacia), donde E + X = VMt-X

c. El *riesgo residual* consiste en el producto de la probabilidad e impacto teórico ponderado por el efecto mitigador de todas las medidas que puedan atenuar el riesgo, entendiendo que la eficacia de las medidas siempre será del cien por cien.

$$Pre = \left[\left(\left((Pt - VMx_1) - VMx_2\right) - \cdots VMx_e\right)\right] * Ire\left[\left(\left((It - VMx_1) - VMx_2\right) - \cdots VMx_e\right)\right]$$

Donde:

- *Pre*: probabilidad residual;
- *Ire*: impacto residual;
- *Pt*: probabilidad teórica;
- *VM*: valor de mitigación de las medidas, con un grado de eficacia teórica del cien por cien.

5.2.4.5. Evaluación del riesgo

En la última fase del proceso de apreciación del riesgo, la organización posee el cálculo del riesgo y se encuentra en posición de tomar una decisión respecto al valor que se ha obtenido de los riesgos según los criterios establecidos. Las operaciones anteriores han tenido el objetivo de cualificar o cuantificar el riesgo, pero la organización no ha individualizado el significado del riesgo para la toma de decisiones. La decisión de la organización respecto a la evaluación de los riesgos debe tener en cuenta:

- El contexto de la organización.
- Los objetivos estratégicos y prioridades.
- Los valores de las partes interesadas.
- El nivel de tolerancia al riesgo asumido que conforma la estrategia de la organización.

CASO PRÁCTICO
Análisis de riesgos. Cálculo del riesgo teórico

La organización ha establecido un catálogo de riesgos legales y los correspondientes escenarios de riesgos de acuerdo con la actividad analizada.

Se han tenido en cuenta los siguientes datos para precisar las variables:

- Se han tomado los riesgos manifestados en España.
- Se ha estimado que la actividad se ejecuta diariamente.
- Las multas en materia de protección de datos se estiman entre 400.000 y 600.000 €.
- Se han recibido únicamente diez reclamaciones administrativas en materia de protección de datos y cinco relacionadas con la relación contractual.

Actividad	Categoría de riesgo	Obligación	Escenario de riesgo	Pf	Pt	Pr	Pt	Il	Ir	It	Rt
Proceso de cálculo de la prima	RGPD (protección de datos)	Art. 13: Se deberá proporcionar al usuario la información correspondiente al tratamiento	El área de desarrollo no ha incorporado en los formularios de solicitud de datos personales las cláusulas informativas.	5	3	1	3	4	3	3,5	**10,5**
	Ley de contrato de seguro	Art. 5: Obligación de formulación del contrato por escrito	Desde el área de desarrollo no se ha incluido la funcionalidad de generar un documento que deje constancia de la formalización de una relación contractual	5	2	1	2,5	2	2	2	**5,2**
	Código Civil	Responsabilidad extracontractual	Debido a errores en la interpretación de los datos personales, se ha denegado la posibilidad de que el usuario pueda volver a contratar con la organización	5	2	1	2,6	2	2	2	**5,2**

CASO PRÁCTICO
Análisis de riesgos. Cálculo del riesgo real y residual

Una vez calculados los riesgos teóricos, cabe analizar los riesgos real y residual. Para ello, se tienen en cuenta los siguientes datos:

- Se tienen actualmente implantadas dos medidas que mitigan la probabilidad en un 10 %, con una eficacia actual del 100 %.
- Se han propuesto en total dos medidas adicionales con el fin de reducir los riesgos: la primera con un 15 % de mitigación sobre el impacto, y la segunda con un 5 % de mitigación sobre la probabilidad.

Actividad	Categoría de riesgo	Obligación	Escenario de riesgo	Pt	It	Rt	Pr	Ir	Rr	Pre	Ire	Rre
Proceso de cálculo de la prima	RGPD (protección de datos)	Art. 13: Se deberá proporcionar al usuario la información correspondiente al tratamiento	El área de desarrollo no ha incorporado en los formularios de solicitud de datos personales las cláusulas informativas.	3	3,5	**10,5**	**2,43**	**3.5**	**8,5**	**2,3**	**2,97**	**6,83**
	Ley de contrato de seguro	Art. 5: Obligación de formulación del contrato por escrito	Desde el área de desarrollo no se ha incluido la funcionalidad de generar un documento que deje constancia de la formalización de una relación contractual	2,6	2	**5,2**	**2.1**	**2**	**4,12**	**1,99**	**1,7**	**3,38**
	Código Civil	Responsabilidad extracontractual	Debido a errores en la interpretación de los datos personales, se ha denegado la posibilidad de que el usuario pueda volver a contratar con la organización	2,6	2	**5,2**	**2,1**	**2**	**4,12**	**1,99**	**1,7**	**3,38**

5.2.4.6. Tratamiento de los riesgos legales

Tras terminar el proceso de apreciación de riesgos, con la cuantificación y valoración de los diferentes niveles de riesgo, la organización debe tomar decisiones con el fin de determinar qué opción es la más adecuada para abordar el riesgo.

Esto pasa, en primer lugar, por determinar las estrategias de tratamiento del riesgo, que pueden implicar alguna o varias de las siguientes:

- Evitar o eliminar la fuente de riesgo.
- Aceptar o aumentar el umbral de riesgo.
- Modificar la probabilidad o impacto.
- Transferir el riesgo a un tercero.
- Retener el riesgo, asumiendo las pérdidas que se obtienen por su materialización.

La justificación depende de múltiples variables, como la relación coste/beneficio, prioridades establecidas por los *stakeholders* o compromisos adquiridos voluntariamente. Una vez acordadas las opciones de tratamiento de riesgo, la organización debe implementar el *plan de tratamiento de riesgos.* Su propósito es especificar la manera en la que se implementarán las opciones elegidas para el tratamiento.

Para la implementación del plan de tratamiento del riesgo, la organización debe tener en cuenta los siguientes elementos:

1. *Normativas y procesos:* desarrollando o mejorando su normativa y procesos relacionados con los riesgos legales.
2. *Procedimientos estandarizados de trabajo:* por ejemplo, destinados a los empleados en relación con procesos operativos.

3. *Técnicas y tecnología:* mediante la aplicación de medidas de seguridad de la información para reducir el acceso por parte de terceros sin autorización.

4. *Información:* proporcionando su disponibilidad para la gestión del riesgo legal.

5. *Actividades:* revisión de contratos por terceros expertos, seleccionando métodos de resolución de disputas adecuados.

6. *Formación mediante ejemplos*: cursos de formación a la dirección con el objetivo de concienciarla.

Desde el punto de visa de la gestión, el riesgo supone potenciales pérdidas económicas anuales debido a la incertidumbre y falta de previsión, por lo que con cada medida aplicable tiende a reducir las pérdidas que puedan derivarse de la materialización del riesgo. La aplicación de las medidas debe entenderse como una inversión de la organización tendente.

Debemos partir de que la organización ha establecido una partida presupuestaria para hacer frente a las infracciones o indemnizaciones pertinentes con el fin de prever y mitigar el impacto del riesgo sobre toda la operativa de la organización. Si la organización sufre la imposición de una multa administrativa sin que se haya previsto, inevitablemente este siniestro tendrá un impacto en la operativa; sin embargo, mediante esta previsión, se consigue mitigar el hipotético impacto siempre que no se supere la partida presupuestaria prevista, por otro lado, la organización no puede destinar recursos para el tratamiento de los riesgos más allá de las consecuencias de los riesgos, dando lugar a un sobredimensionamiento de las medidas implementadas, por ello, conviene establecer ratios de inversión para controlar los recursos destinados a mitigar los riesgos sin que con ello se asuman pérdidas inaceptables; en este sentido, podemos establecer un Return of Legal Investment (ROLI) sobre la base de las consecuencias económicas que supone la materialización del riesgo. Esta variante del clásico Return of Investment no tiene el objetivo de determinar los beneficios que se consiguen tras la inversión en las medidas, sino las pérdidas evitadas tras la implementación de las medidas.

CASO PRÁCTICO

La entidad aseguradora asume que la materialización del riesgo de incumplimiento del deber de información del artículo 13 del RGPD en el momento del cálculo de la prima puede generar pérdidas de hasta 25.000 € por infracción, estimando que al año se producen cinco infracciones, suponen unas pérdidas de 125.000 € anuales, cuando la organización tiene un presupuesto para infracciones económicas de 85.000 €. Para ello, se dispone a contratar un servicio de asesoría en materia de protección de datos para establecer una revisión de todos los procesos con los interesados en los que se traten datos personales. Se ha estimado que esta medida cuesta en el momento de su contratación 45.000 € anuales, pero evita el 70 % de las infracciones.

Nos disponemos a evaluar la solvencia de la medida presentada:

$$ROLI = \frac{[(Frecuencia * Impacto) * Mitigación - Costes]}{Costes}$$

$$94{,}4\,\% = \frac{[(5 * 25.000) * 0.7 - 45.000]}{45.000}$$

La medida implementada proporciona una buena relación coste-beneficio. Las pérdidas evitadas han sido de 42.500 €, sin embargo, el impacto total del riesgo ha sido reducido a 82.500 €, superando el umbral establecido por la organización. Si el gestor optase por un servicio cuya mitigación sea del 60 %, pero con un coste de 30.000 €, el resultado quedaría así:

$$150\,\% = \frac{[(5 * 25.000) * 0.6 - 30.000]}{30.000}$$

La medida implementada sigue proporcionando una buena relación coste-beneficio. Las pérdidas evitadas han sido de 45.000 €, y el impacto total del riesgo ha sido reducido a 80.000 €, estando por debajo del umbral establecido en la partida presupuestaria para infracciones, permitiendo a la compañía ahorrar 5.000 € anualmente.

5.2.4.7. Comunicación, consulta y reporte

Esta etapa es transversal en todo el proceso de gestión de riesgos, por lo que en cada fase debe asegurarse una adecuada comunicación, consulta y reporte. La organización debe comunicar y consultar con las partes interesadas más significativas en cada etapa del proceso de gestión de riesgos legales para asegurarse que comprendan los riesgos legales y sus efectos en la organización, las bases de la toma de decisiones y las razones por las que se toman las acciones.

El proceso de comunicación busca promover la concienciación, la consulta y la obtención de la información, para lo que se necesita identificar la información que se aporta y los datos necesitados. Las partes interesadas tienen diferentes perspectivas y valores, y esta característica influye en el proceso de toma de decisiones. Para facilitar una efectiva comunicación y consulta, la organización debería dirigirse a proporcionar la información necesaria a todos aquellos con responsabilidad y autoridad para la gestión del riesgo legal y supervisión. La función de gestión debe también comunicar con las partes interesadas más relevantes, incluyendo las autoridades reguladoras, legislativas y judiciales.

Para construir una cultura de gestión del riesgo a través de toda la organización, el aprendizaje debe:

- Ocurrir en todas las fases de la gestión de riesgos legales.
- Estar promovido para concienciar y entender la exposición al riesgo legal.
- Usarse para proporcionar claridad en la gobernanza y en el liderazgo, la conformidad con normativas, procesos y procedimientos.

5.2.4.8. Seguimiento y revisión

La segunda fase transversal consiste en asegurar y mejorar la eficacia y calidad del diseño, la implementación y los resultados del proceso de gestión de riesgos. Esta actividad debe ser planificada dentro del proceso de gestión de riesgos y

ejecutarse en todas las etapas de este, que incluye planificar, recopilar, analizar información, registrar y proporcionar retroalimentación.

El seguimiento y revisión permite conocer qué funciona, qué puede mejorar y qué se puede modificar durante todo el proceso. De ahí la necesidad de su ejecución en cada fase. El seguimiento y revisión de los riesgos legales debe incluir lo siguiente:

- Estar al frente de los cambios en el ambiente, tales como la introducción de nuevas leyes y su exigencia, para ajustar la estrategia de la organización de acuerdo con ello.

- Seguir los eventos desencadenados por un riesgo legal, analizando su frecuencia y patrones, y esbozando sus conclusiones.

- Considerar un sistema de alerta temprana con partes interesadas claves para identificar señales de peligro de riesgos legales significativos que pueden ocurrir.

- Seguir y revisar:

  – resultados derivados del tratamiento del riesgo;

  – cambios en el entorno;

  – la construcción de planes de tratamientos de riesgos;

  – la resignación de responsables.

- Comparar el progreso con el plan de tratamiento de riesgos, revisando y actualizando el plan periódicamente y de manera oportuna para asegurarse de su adecuación, idoneidad y efectividad en relación con la gestión de los riesgos legales.

5.2.4.9. Registro e informe

El proceso de la gestión del riesgo y sus resultados deben documentarse e informar a través de mecanismos apropiados. La etapa de registro e informe es la

última de las etapas de la gestión del riesgo, y una de las más críticas, puesto que consiste en poner en valor todo el trabajo realizado. Se debe tener en cuenta los siguientes elementos respecto a la conservación de registros e informe:

- La relación abogado-cliente en relación con sus deberes de confidencialidad.
- La destrucción, conservación y normativas de privacidad de acuerdo con la legislación de privacidad.
- La disponibilidad y accesibilidad de documentación a las partes interesadas para mejorar la toma de decisiones y para fines de auditoría interna y externa.
- Si la documentación relevante necesita conservarse de forma segura, mediante una cadena de custodia documentada, que ninguna alteración haya sido efectuada en los documentos, información o evidencias.
- Las medidas de confidencialidad y seguridad en relación con la documentación confidencial.

5.3. LA GESTIÓN DE RIESGOS, LA RESPONSABILIDAD MIXTA Y LA DILIGENCIA EN LA CADENA DE SUMINISTRO COMO RESPUESTA

5.3.1. La debida diligencia en la IA y su relación con la gestión de riesgos

Con la llegada de las nuevas tecnologías han aflorado una gran cantidad de retos y riesgos derivados de su uso, convirtiendo la seguridad jurídica, que ofrece la exhaustiva regulación a través de normas que requieren de un procedimiento de elaboración, enmienda y aprobación, en un auténtico obstáculo para el verdadero desarrollo de las nuevas tecnologías y sus oportunidades.

En síntesis, el regulador se enfrenta a un marco donde la tecnología avanza y evoluciona a un ritmo que nuestro sistema normativo actual no puede seguir por estar construido, mayoritariamente, sobre un sistema basado en formalismos inherentes a la elaboración y aprobación de normas, lo que, en la práctica, dificulta y obstaculiza el

desarrollo y uso de las nuevas soluciones tecnológicas, incluida la IA, al no contar los interesados (diseñadores, desarrolladores, usuarios, etc.) con un marco que permita generar seguridad en el uso de la IA y confianza en las consecuencias.

Como resultado de lo anterior, y ante la cada vez mayor implementación de la IA en el mercado, el regulador, tanto nacional como comunitario, ha decidido adoptar una vía de regulación, similar a la que actualmente es aplicable a la protección de datos y la privacidad: dentro de un marco legal mínimo impuesto por el regulador (p. ej., normas marco), la persona o entidad interesada en la implementación de sistemas tecnológicos en su modelo de negocio debe asumir una conducta proactiva *(accountability),* destinada a la adopción de medidas que garanticen el despliegue y uso dentro de unos estándares de fiabilidad y seguridad.

Aunque pueda ser objeto de regulación más específica, todos los informes, guías y propuestas publicadas por la Unión Europea en materia de IA coinciden en que uno de los requisitos que se exige a todos los sujetos que intervengan en el ciclo de vida de la IA es el de adoptar una conducta proactiva, es decir, orientada a la actuación diligente en la implementación, mantenimiento, uso y responsabilidad que pudiera ocasionar la IA.

En este sentido, el regulador articula el cumplimiento legal a través de una serie de normas donde de define el objetivo a alcanzar (p. ej., disponer una IA fiable), pero delegando en la organización los medios para alcanzarlo. Este método regulatorio, ya utilizado en campos como el de la protección de datos de carácter personal, se construye sobre un sistema basado en la gestión, por parte de cada organización, de los riesgos que soporta, derivado de su contexto y actividad desarrollada.

De esta forma, y ante una realidad cambiante, como consecuencia del cada vez mayor desarrollo de las tecnologías, el regulador delega en los operadores la tarea de adoptar las medidas que consideren necesarias, en función de las circunstancias propias de cada operador, para alcanzar un objetivo prefijado en vez del mero cumplimiento de hitos regulatorios[107], es decir, se obliga a los operadores a asumir un papel proactivo: una debida diligencia.

[107] *Vid*. Kishnani, P., Turley, M., y Eggers, M., *El futuro de la regulación. Principios para regular tecnologías emergentes*, Deloitte Insights, Londres, 2018, p. 9.

No en pocos casos, la materialización de un riesgo y la responsabilidad del operador como sujeto causante del daño pueden verse reducidas o eliminadas si se prueba que, a través de la debida diligencia, se han adoptado las medidas necesarias para identificar, analizar y tratar los riesgos derivados del contexto y la actividad desarrollada.

La figura de la debida diligencia adquiere especial relevancia en el campo del desarrollo y uso de la IA, pues, como ya se ha expuesto previamente, la transversalidad en el uso y aplicación de la IA y la orientación del sistema de responsabilidad a un régimen de solidaridad incrementan el número de riesgos y, en consecuencia, de las probabilidades de encontrarse ante un supuesto de responsabilidad por daños o la comisión de una infracción sancionable.

Sin embargo, y con el objetivo de acreditar la adopción de las citadas medidas proactivas en el marco de la IA, la Unión Europea plantea la consecución de certificaciones (validación obligatoria para los sistemas de IA de alto riesgo) o etiquetado (validación voluntaria para los sistemas de IA no considerados como de alto riesgo) con el objetivo de permitir a los agentes económicos mostrar que la IA utilizada es fiable. Esto contribuirá a incrementar la confianza de los operadores en los sistemas de IA.

Más allá de la mera aproximación teórica realizada en los párrafos anteriores, y como se analizará en los siguientes apartados, la adopción de una conducta proactiva por parte de los sujetos intervinientes en el ciclo de vida de la IA se encuentra ampliamente amparada por la normativa que, como ya se ha visto anteriormente, es de aplicación a la IA.

Las propuestas de la Unión Europea proponen un enfoque basado en el riesgo como método de imputación objetiva[108] a lo largo de la cadena de valor, donde cada agente interviniente debe responder sobre el hecho causante del daño y asegurar la responsabilidad en la cadena de suministro del sistema de IA, consiguiendo

[108] *Vid*. Navas, S., "Sistemas expertos basados en inteligencia artificial y responsabilidad civil", *Diario La Ley*, 2020, p. 5.

un modelo híbrido entre una responsabilidad objetiva y otra subjetiva[109]. La responsabilidad en la cadena de suministro se basa en tres pasos lógicos para imputar la responsabilidad al agente[110]:

1. Establecer la *existencia de un indelegable deber de cuidado, o diligencia debida,* basado en tres requisitos: a) que el daño es previsible; b) la proximidad de la relación entre el demandante y el demandado; y c) que es justo y razonable que la ley imponga un deber de un alcance determinado a una de las partes en beneficio de la otra.

2. El *quebrantamiento* de ese deber de cuidado cuando efectivamente se ha atribuido al agente.

3. Que ese quebrantamiento del deber de cuidado haya *causado el resultado ilícito.*

En ese deber de cuidado se espera que la organización adopte, como una práctica adecuada del agente, un proceso de apreciación y tratamiento de riesgos como parte de su responsabilidad personal[111]. Podemos presentar, como ejemplo, las obligaciones en materia de diligencia debida en la cadena de suministro del Reglamento (UE) 2017/821, por el que se establecen obligaciones en materia de diligencia debida en la cadena de suministro por lo que respecta a los importadores de la Unión de estaño, tantalio y wolframio, sus minerales y oro originarios de zonas de conflicto o de alto riesgo[112]. Según este reglamento, la debida diligencia en la cadena de suministro está formada por:

- Las medidas en materia de gestión de riesgos.

- Las auditorías externas, siendo estas tanto de segunda parte como de tercera parte.

---

[109] *Vid. Op. Supra.*

[110] *Vid*. Terwindt, C. *et. al.*, "Supply chain liability: pushing the boundaries of the common law?", *Journal of European Tort Law*, vol. 8, n. 3, 2018, pp. 18-20.

[111] *Uren v Corporate Leisure (UK) Ltd [2011] EWCA Civ 66.*

[112] DOUE L 130/1 de 19.5.2017.

- La comunicación de información con el fin de identificar y abordar los riesgos reales y potenciales para impedir o reducir los efectos negativos asociados.

Debemos entender la mención a este reglamento como ejemplo ilustrativo de las exigencias en materia de gestión de riesgos en la cadena suministros, que es recogido en el artículo 5, pero que, análogamente, la presentación de un programa siguiendo estas directrices puede poner al operador aplicable en una posición ventajosa a la hora de demostrar su debida diligencia[113].

Si bien el término de gestión de riesgos no nos es desconocido a los juristas por su inclusión en diferentes normas, su construcción va más allá de la obligación recogida en la norma, debiéndonos atener a metodologías y estándares internacionalmente reconocidos para definirlo. Para ello, utilizaremos la definición del estándar ISO 31000:2018 sobre gestión de riesgos, emitida por la International Standard Organization; organización internacional reconocida por sus estándares mundialmente reconocidos, puesto que, para su elaboración, intervienen los organismos nacionales de estandarización de todo el mundo. Este estándar define la gestión de riesgos como "actividades coordinadas para controlar la organización en relación con el riesgo". A pesar de la definición corporativa recogida en su cláusula 3, la gestión es entendida como un proceso que se encuentra embebido en el sistema de gobernanza y, siguiendo el presente estándar, para la correcta adopción del proceso de gestión de riesgos, la organización que posea un sistema de IA debe identificar, analizar, evaluar, comunicar y tratar los riesgos relacionados con los sistemas de IA.

[113] El Reglamento (UE) 2017/821 coincide con la norma ISO 31000:2018 respecto a los elementos que un programa de debida diligencia debe tener y las actividades del proceso de gestión de riesgos que recomienda aplicar: una política de cadena de suministro con el compromiso de adoptar un sistema de gestión de riesgos; adoptar las estrategias para la gestión de los riesgos, comunicando el resultado de la evaluación de los riesgos a la alta dirección y a las partes interesadas; adoptar las medidas de gestión de riesgos; aplicar el plan de tratamiento del riesgo, supervisando y registrando la eficacia de los esfuerzos de reducción de riesgos e informar a los altos directivos designados a ese fin; y llevar a cabo nuevas evaluaciones de los hechos y riesgos en relación con los riesgos que deban reducirse, o a raíz de un cambio de circunstancias.

No aparece como tal una definición del concepto de riesgo[114] en la propuesta de reglamento, sino que delimita de una forma abstracta el principio por el cual se determina la existencia de un alto riesgo, como es que dicho sistema pueda causar un perjuicio a la salud y la seguridad o el riesgo de tener repercusiones negativas para los derechos fundamentales. Los criterios para determinar la existencia de este perjuicio son detallados en el artículo 7:

a. la finalidad prevista del sistema de IA;

b. la medida en que se haya utilizado o sea probable que se utilice un sistema de IA;

c. la medida en que la utilización de un sistema de IA ya haya causado un perjuicio a la salud y la seguridad, haya tenido repercusiones negativas para los derechos fundamentales o haya dado lugar a problemas importantes en relación con la materialización de dicho perjuicio o dichas repercusiones negativas, según demuestren los informes o las alegaciones documentadas que se presenten a las autoridades nacionales competentes;

d. el posible alcance de dicho perjuicio o dichas repercusiones negativas, en particular en lo que respecta a su intensidad y su capacidad para afectar a una gran variedad de personas;

[114] Podemos partir del concepto de riesgo contemplado en el informe aprobado por el Parlamento Europeo con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial (2020/2014(INL) que se refiere a una concepción basada en la combinación de las consecuencias sobre los derechos protegidos y la probabilidad de ocurrencia de estos. Esta formulación del concepto de riesgo promueve una concepción negativa del riesgo que, si bien es fruto de una concepción tradicional de riesgo respecto a modelos más antiguos, difiere de la concepción ambivalente presentada por la norma ISO 31000:2018, donde lo define como "el efecto de la incertidumbre sobre los objetivos", concretando que la incertidumbre es "cualquier variación, positiva o negativa, que afecta al cumplimiento de los objetivos". Por lo que el implementador deberá identificar, analizar, evaluar y tratar los riesgos que puedan generar un daño indemnizable sobre la base de la vulneración de un derecho. Estos derechos, como se ha mencionado, pueden ser los relacionados con la seguridad de la información o protección de datos personales que, en caso de un incumplimiento que genere un daño, pueden generar un derecho a indemnizar al sujeto. Sobre la base del anterior concepto de riesgo propuesto por el informe, atendiendo al considerando 16 de este, el programa de diligencia debida debe efectuarla el implementador de la solución de IA sobre la base de los siguientes elementos: la naturaleza del sistema de IA (las finalidades, la infraestructura informática utilizadas y los procesos existentes que lo operan); el derecho protegido jurídicamente potencialmente afectado (la identificación de los derechos fundamentales en los que el sistema de IA pueda incidir); el daño o perjuicio potencial que podría causar el sistema de IA; y la probabilidad de dicho perjuicio.

e. la medida en que las personas que podrían sufrir dicho perjuicio o dichas repercusiones negativas dependan de la información de salida generada con un sistema de IA, en particular porque, por motivos prácticos o jurídicos, no sea razonablemente posible renunciar a dicha información;

f. la medida en que las personas que podrían sufrir dicho perjuicio o dichas repercusiones negativas se encuentren en una posición de vulnerabilidad respecto del usuario de un sistema de IA, en particular debido a un desequilibrio en cuanto al poder o los conocimientos que ambos poseen, sus circunstancias económicas o sociales, o su edad;

g. la medida en que sea fácil revertir la información de salida generada con un sistema de IA, habida cuenta de que no se debe considerar que la información de salida que afecta a la salud o la seguridad de las personas es fácil de revertir.

En el artículo 9 de la Propuesta de Reglamento por el que se establecen normas armonizadas sobre la inteligencia artificial se configura el modelo de gestión de riesgos que el operador deberá aplicar siempre y cuando el sistema de IA sea considerado de alto riesgo:

a. la identificación y el análisis de los riesgos conocidos y previsibles vinculados a cada sistema de IA de alto riesgo;

b. la estimación y la evaluación de los riesgos que podrían surgir cuando el sistema de IA de alto riesgo en cuestión se utilice conforme a su finalidad prevista y cuando se le dé un uso indebido razonablemente previsible;

c. la evaluación de otros riesgos que podrían surgir a partir del análisis de los datos recogidos con el sistema de seguimiento posterior a la comercialización;

d. la adopción de medidas oportunas de gestión de riesgos tendentes a reducir o eliminar los riesgos.

Como observamos, este proceso de gestión de riesgos es *multinivel.* Por un lado, la Comisión Europea clasifica mediante criterios objetivos aquellos sistemas basados en sus finalidades y en su impacto y probabilidad de causar un perjuicio y, en caso de que este sistema sea clasificado como "alto riesgo", deberá aplicar el proceso de gestión de riesgos del artículo 9. Esta obligación no incumbe solo al operador, sino también al proveedor en tanto en cuanto este desarrolle un sistema de IA clasificado como "alto riesgo", extendiéndose la obligación del artículo 9 a estos.

En la gran mayoría de ocasiones, la contratación de proveedores conlleva la externalización de los procesos, y este tipo de sistemas suele ofrecerse a través de proveedores *cloud*. El uso de la externalización de procesos mediante sistemas *cloud* de terceros es sensible para los organismos reguladores. En este sentido, las Directrices sobre la externalización a proveedores de servicios en la nube de la EIOPA[115] determina las condiciones en las que debe regirse la externalización de los servicios. Entre ellas, destacan la directriz 8, sobre evaluación de riesgos de la externalización en la nube, y la directriz 9, sobre diligencia debida del proveedor de servicios en la nube.

La intervención de numerosos actores en la cadena de suministro conlleva la existencia de dificultades en la atribución de responsabilidad ante la existencia de un daño cuya atribución es difusa; sin embargo, no todos los intervinientes en la cadena de suministro poseen el mismo grado de "importancia" en el desarrollo del producto, ni mucho menos independencia entre las partes, pudiendo influir en los procesos de una parte a otra de la misma cadena de suministro por diferentes motivos, ya sean económicos, laborales o estratégicos. Bajo este axioma, se ha desarrollado el concepto de "esfera de influencia" para atribuir dicha intervención en los procesos de una parte sobre la otra. Este concepto fue introducido, dentro del mundo corporativo, por la United Nations Global Compact. Esta teoría permite entender que la parte que ejerce la influencia sobre la otra puede llegar a ser responsable por los daños atribuidos a esta última[116]. Sin embargo, este concepto ha sido aclarado posteriormente por el Consejo de Derechos Humanos en el Informe del Representante Especial del Secretario General: *Aclaración de los conceptos de*

[115] EIOPA-BoS-20-002.

[116] *Vid*. Chen, S., "Multinational Corporate Power, Influence and Responsability in Global Supply Chains", *Journal of Business Ethics*, n. 148, 2018, p. 369.

"esfera de influencia" y "complicidad". Este informe diferencia el concepto de influencia *(Leverage)* en dos significados distintos:

- El "impacto", es decir, el perjuicio que las actividades o las relaciones de las empresas causan en la materia concreta.

- La "autoridad" que una empresa puede ejercer sobre otros agentes que causan un perjuicio o podrían evitarlo.

El impacto siempre entra en el ámbito de la responsabilidad de respetar la ley, mientras que la autoridad solo en circunstancias determinadas. No se puede responsabilizar a las empresas del impacto derivado del incumplimiento ejercido por cada entidad sobre la que tengan alguna autoridad, pues comprendería también los casos en que no están contribuyendo al daño ni son causa de él. Tampoco es conveniente exigir a las empresas que actúen siempre que tengan influencia. La esfera de influencia debe entenderse como la relación causal sobre la materialización de un impacto. Sin embargo, el propio informe especifica que, si no existe una situación legal de control a un proveedor, no tendría sentido incluirlo dentro del alcance del programa de debida diligencia.

Una vez determinada la relación de la gestión de riesgos dentro del deber de diligencia que debe existir en la cadena de suministro, las organizaciones se plantean herramientas concretas que permitan una adecuada apreciación del riesgo, fácilmente integradas en los sistemas de gobernanza, de manera que estas herramientas no se conviertan en un requerimiento burocrático que obstaculice la consecución de los objetivos operativos de la organización, y sea fácilmente demostrable ante terceros la debida diligencia que una entidad aseguradora soporta. En este contexto, el concepto de "debida diligencia" se torna en un concepto jurídico indeterminado, que podemos entender como la intención deliberada del legislador de no cerrar las opciones que un implementador posee a la hora de poder demostrar la debida diligencia[117] ante esos terceros, ya sean clientes, órganos jurisdiccionales o Administraciones públicas.

[117] *Vid*. Martínez Estay, J. I., "Los conceptos jurídicos indeterminados en el lenguaje constitucional", *Revista de Derecho Político*, n. 105, 2019, p. 165.

En cualquier caso, el proceso de gestión de riesgos y debida diligencia que una entidad aseguradora realice en su condición de operador de sistemas de IA deberá incluir en su programa las directrices de externalización de la EIOPA, siempre y cuando el uso del sistema de IA sea mediante un servicio en la nube de un tercero.

5.4. LA EVALUACIÓN DE IMPACTO COMO MEDIDA PROPUESTA PARA GESTIONAR LOS RIESGOS DERIVADOS DE LA IA EN UN MARCO DE SISTEMA DE CUMPLIMIENTO NORMATIVO GESTIONADO

A lo largo de este trabajo, hemos observado una gran complejidad en cuanto a la identificación de los riesgos que los sistemas de IA generan en la operativa de una organización, siendo estos éticos, legales o en materia de ciberseguridad. Las herramientas generadas no deben tener una aplicación *ad hoc,* sino estar integradas en las herramientas de gobernanza en el caso de que estas existan, como es el caso de las entidades aseguradoras mediante el marco impuesto por Solvencia II. Por eso ofrecemos como metodología para la evaluación de riesgos de inteligencia artificial el modelo de evaluación de impacto propuesto por varias legislaciones nacionales en materia de protección de datos, pero adaptadas a la realidad de la organización bajo la propuesta de un sistema de gestión de la gobernanza y el cumplimiento normativo que incluya la gestión de los diferentes sistemas y funciones en la entidad aseguradora.

La irrupción de las nuevas tecnologías y la complejidad en la cadena de valor en la prestación de productos y servicios han permitido que el legislador pase de un modelo basado en un estricto cumplimiento de las obligaciones a un enfoque basado en el riesgo. Este enfoque parte de una creciente predisposición a permitir la autorregulación en las organizaciones. Es en Estados Unidos donde, a finales del siglo XX, impulsaron los modelos de "evaluación de impacto" como elemento regulatorio en el sector medioambiental y tecnológico[118], siendo actualmente elementos regulatorios fundamentales en materia de protección de datos y medioambiental.

[118] *Vid*. Puyol, J., *El modelo de evaluación de riesgos en la protección de datos EIPD/PIA*, *op. cit*., p. 14.

Una evaluación de impacto, más que una metodología de apreciación de los riesgos sobre una determinada materia, es, sobre todo, un proceso[119] que se inicia en las primeras etapas de la confección de un servicio o producto para influir en el resultado final de estos, mediante la inclusión en el diseño de determinados criterios[120], y servir de apoyo a los gerentes para la toma de decisiones. Este proceso no concluye con la puesta a disposición del producto o servicio, sino que debe seguir aplicándose después de este hito. Es una traslación de un proceso de gestión de riesgos en una organización a un servicio, producto o proyecto de la organización.

La evaluación de impacto, en algunos sectores, es considerada como una obligación legal que los operadores deben soportar; sin embargo, los operadores deben entender la existencia de esta obligación como una oportunidad para las organizaciones para adoptar en la gestión de la organización un enfoque basado en el riesgo que les permita afrontar los nuevos retos regulatorios y adelantarse a los riesgos que un determinado producto o servicio genera. A su vez, la evaluación de impacto se presenta como una oportunidad para cumplir el artículo 185 del Real Decreto-ley 3/2020, donde las entidades aseguradoras deben diseñar un proceso interno para la aprobación de los productos de seguro o adaptaciones significativas, que debe analizar los riesgos pertinentes, puesto que la actual función de gestión de riesgos no se entiende como un papel operativo sino, evidentemente, dedicado a la gobernanza, careciendo de herramientas y metodologías que permitan analizar a un bajo nivel los riesgos que supone un producto o servicio. En este sentido, la EIOPA publicó las Directrices preparatorias relativas a los procedimientos de gobernanza y vigilancia de productos para las empresas de seguros y los distribuidores de seguros[121], enfocadas al cumplimiento de esta obligación, derivada de la transposición de la Directiva (UE) 2016/97 sobre la distribución de seguros.

Es un proceso que debe estar basado metodológicamente en un proceso de apreciación y tratamiento del riesgo, pero como hemos observado a lo largo del

[119] *Vid*. Wright, D., y De Hert, P. (eds.), *Privacy Impact Assessment*, Springer, London, 2012, p. 9.

[120] Por ejemplo, en criterios de protección de datos o medioambiente.

[121] EIOPA BoS 16/071 ES.

trabajo, los sistemas de IA implican la existencia de diversas tipologías de riesgos, tales como los riesgos legales, seguridad de la información, o éticos, por lo que debe ser la propia organización la que determine una metodología que en la medida de lo posible pueda establecer criterios comunes para obtener una interpretación común de los impactos y las probabilidades de cada riesgo identificado. Un enfoque adecuado como metodología para el establecimiento de los criterios puede ser la propia ISO 31000, explicada en el apartado 5.2.2.2, puesto que este marco de gestión de riesgos supone un modelo polivalente para todo tipo de riesgos[122], pero con un escalado adecuado al servicio o producto, por lo que debería contener una estructura similar a la analizada:

1. La *determinación del alcance del sistema y servicio sustentado por la IA,* analizando los factores internos y externos que afectan a su alcance.

2. La *definición de una metodología de análisis y tratamiento del riesgo* cuyos criterios sean lo más uniforme posible.

3. La *identificación de los riesgos* según los factores de su contexto, definición del servicio y tecnología aplicable al sistema.

4. El *análisis y evaluación* de los riesgos identificados.

5. La determinación de las estrategias que se van a aplicar para tratar el riesgo.

6. La *continuada comunicación* entre las partes interesadas durante todo el proceso de evaluación.

7. Una *revisión del proceso periódica* para la búsqueda de fallos y oportunidades de mejora en el proceso.

[122] Sirve como referencia a los riesgos de seguridad de la información (ISO/IEC 27001), gestión medioambiental (ISO 14001), operacionales (ISO 9001), entre otros.

En este sentido, como riesgo operativo que es, debe estar sometido a lo dictado en la política de gestión de riesgos que la EIOPA recomienda en su Directrices sobre el sistema de gobernanza[123], y cuyo esquema propuesto sirve para cubrir sus exigencias en cuanto a:

- Identificar los riesgos operacionales a los que está o podría estar expuesta y la valoración de la forma de mitigarlos.

- Considerar actividades y procesos internos para la gestión de los riesgos operacionales, incluyendo el sistema informático en que se basan.

- Identificar límites de tolerancia al riesgo respecto a las principales áreas de riesgo operacional de la empresa.

- Tener procesos para identificar, analizar e informar sobre los eventos de riesgo operacional. Con este fin, debería establecer un proceso para catalogar y controlar los eventos de riesgo operacional.

- Elaborar y analizar un grupo adecuado de escenarios para el riesgo operacional basados en al menos los siguientes supuestos: a) el fallo de un proceso, personal o de un sistema importante; b) la ocurrencia de eventos externos.

Incluso la EIOPA recomienda la adopción de una evaluación de impacto en los casos de uso donde esté implicado un sistema de IA[124]. El proceso de evaluación de impacto debe ser abierto y dirigido por la transparencia, requiriendo para su efectiva implementación una serie de roles que deben intervenir en el proceso desde un punto de vista de gestión mediante un responsable de proyecto o de servicio, que definirá el alcance y la necesidad de realizar una evaluación de impacto, y otros roles tales como responsable de seguridad, delegado de protección de datos, etc.

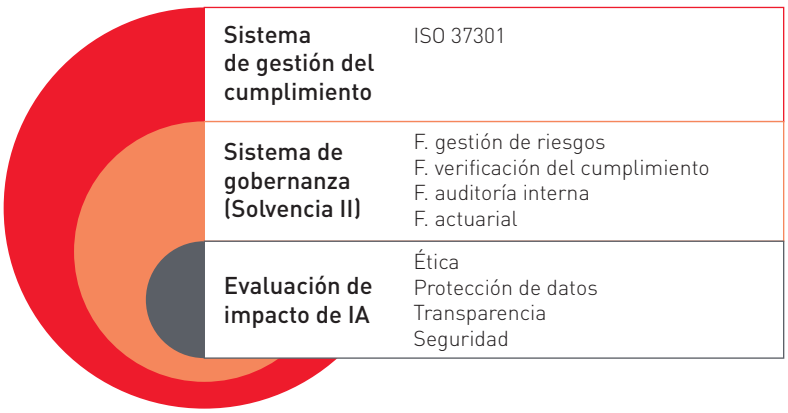
[123] EIOPA-BoS-14/253 ES.

[124] EIOPA, *Artificial intelligence governance principles: towards ethical and trustworthy artificial intelligence in the european insurance sector. A report from EIOPA´s Consultative Expert Group on Digital Ethics in insurance*, 2021, pp. 17-18.

Es evidente que, aunque sea una tarea complicada para la entidad aseguradora, esta deberá contar indudablemente con las partes interesadas en el proyecto, no limitándose exclusivamente a los actores internos, puesto que aportan beneficios en la gestión de toma de decisiones, coordinación en la implantación de los planes de tratamiento e identificación de los riesgos que de otra manera no serían tenidos en cuenta, así como en el fomento de la concienciación.

Pero aterrizando en el marco normativo que soportan las entidades aseguradoras, la evaluación de impacto encaja adecuadamente con el sistema de las Tres Líneas de Defensa al requerir la participación de cada una para un gobierno adecuado de los riesgos que el sistema de IA genera. El propio proceso derivado de la evaluación de impacto debe ser participado por las diferentes funciones y sistemas que una entidad aseguradora debe tener en función de Solvencia II. No debe ser una herramienta *ad hoc,* ni mucho menos crear nuevas funciones, sino un proceso impulsado desde la función de gestión de riesgos que asume transversalmente las funciones y sistemas mediante un *workflow* definido por la organización dentro de un sistema global de gestión del cumplimiento, como puede ser el que proporciona la ISO 37301, completando el sistema de gobernanza de una entidad aseguradora.

Esquema de la estructura del cumplimiento de un sistema de IA



Fuente: elaboración propia.

6. PROPUESTA METODOLÓGICA PARA UNA EVALUACIÓN DE IMPACTO EN SISTEMAS DE IA

A continuación, proponemos una metodología iterativa de desarrollo del proceso de evaluación de impacto para el análisis de los riesgos que implica el uso de sistemas de IA en la prestación de servicios tanto internos como externos.

Es fundamental que la metodología de la organización esté documentada[125] en forma de un procedimiento donde se determinen los roles existentes respecto a cada fase del proceso y pueda ser defendido ante las autoridades administrativas.

6.1. DETERMINACIÓN DE ROLES Y RESPONSABILIDADES EN EL PROCESO

En primer lugar, la entidad aseguradora debe determinar los roles que intervienen en el proceso de evaluación de impacto, y las responsabilidades asociadas a ellos, para lo que utilizaremos los roles existentes en una entidad aseguradora derivados de Solvencia II. Debemos destacar que, para revestir al proceso de una intervención adecuada de la alta dirección, esta debe participar en la toma de decisiones y en el seguimiento del proceso, por lo que se deberá nombrar a un *responsable operativo*[126] que defina los criterios estratégicos del servicio y de la información tratada, además de determinar el umbral de riesgo que la organización está dispuesta a asumir. La implicación de la alta dirección es fundamental a la hora de definir las estrategias de gestión de riesgos que la organización debe tomar. Demuestra, sobre todo, que la organización está concienciada sobre la importancia de este proceso ante terceros o reguladores.

[125] Obligación derivada de los artículos 24 y 35 del RGPD, respecto a la adopción de las políticas necesarias que la organización debe implementar en materia de protección de datos.

[126] Consiste en la función unificada de los responsables de servicio e información definidos en la Guía CCN-STIC 801 sobre el Esquema Nacional de Seguridad.

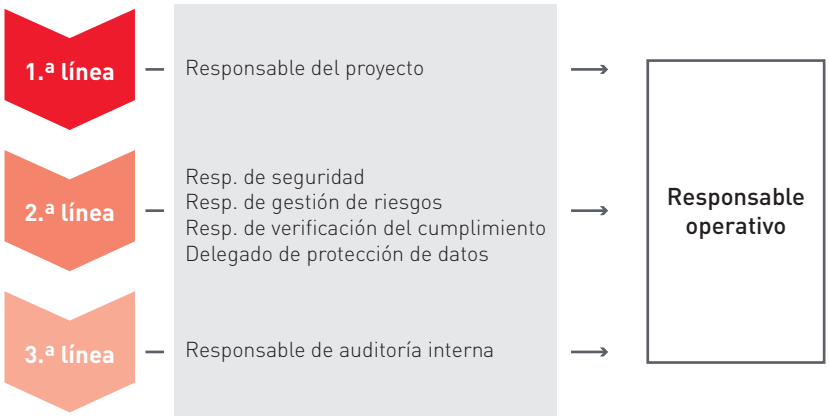
Tras establecer la implicación de la alta dirección, deberá definirse la implicación de las diferentes funciones de gobernanza y de la organización, como son el *responsable de gestión de riesgos,* como ostentador de dicha gestión, que deberá coordinar el proceso de apreciación y tratamiento del riesgo, apoyado por otros roles con el fin de unificar los criterios para la apreciación del riesgo, como son el *responsable de seguridad informática,* que también recomendará las medidas aplicables y controlará el cumplimiento del marco de gestión de la seguridad de la información en cada fase de la ejecución del proyecto.

Deberá incluirse la participación del *responsable de verificación del cumplimiento* para el apoyo al responsable de gestión de riesgos en los procesos de apreciación y tratamiento de los riesgos respecto a los riesgos legales que la entidad aseguradora pueda ser objeto. Dentro de esta función, debemos incluir las responsabilidades del *delegado de protección de datos,* en tanto en cuanto esta función debe rendir cuentas a la alta dirección[127] y desempeñar las funciones recogidas en el artículo 39 del RGPD.

Por último, el *responsable del proyecto* de IA deberá impulsar el desarrollo de la evaluación de impacto y determinar el alcance y desarrollo del sistema, e intervenir a lo largo de las fases del proceso.

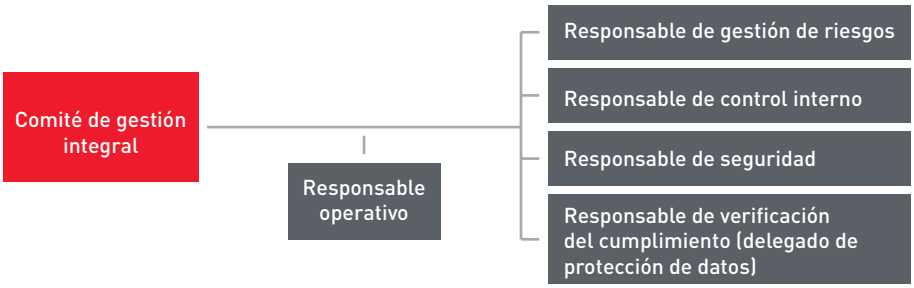
El modelo de roles y responsabilidades propuesto concuerda con el modelo de las Tres Líneas de Defensa acorde con el sistema de gobernanza de Solvencia II, al delimitar las responsabilidades en cada una de las líneas según las funciones existentes, sin la necesidad de crear funciones *ad hoc*.

[127] Artículo 38.3 del RGPD.



Fuente: elaboración propia.

Las funciones y responsabilidades intervinientes pueden agruparse en comités de gestión para aumentar la agilidad de los procesos, de forma que todas las funciones puedan integrar y complementarse en un proceso iterativo donde se pongan en común las diferentes visiones de cada uno de los roles intervinientes, creando un sistema de gobernanza del propio proceso. Este objetivo se consigue mediante la incorporación de la alta dirección en los procesos de toma de decisiones respecto de las decisiones propuestas por el resto de los responsables, creando así un *comité de gestión integral* que concentre las decisiones estratégicas, abarcando todos los ámbitos de gestión.



Fuente: elaboración propia.

Rol	Responsabilidades
Responsable del proyecto	• Evaluar la necesidad de efectuar una evaluación de impacto. • Definir el alcance del sistema y el servicio prestado. • Participar en cada fase de la evaluación de impacto. • Implementar las recomendaciones, medidas y controles propuestos.
Responsable operativo	• Definir los requisitos de seguridad del servicio. • Definir los requisitos del tratamiento de la información. • Determinar el umbral de riesgo aceptable por la organización.
Responsable de seguridad	• Proponer un marco de gestión de la seguridad de la información. • Participar en el proceso de identificación, análisis y tratamiento del riesgo en materia de seguridad de la información. • Proponer las medidas de seguridad aplicables.
Responsable de verificación del cumplimiento	• Proponer un marco de gestión del cumplimiento normativo. • Participar en el proceso de identificación, análisis y tratamiento del riesgo legal y ético. • Proponer los controles necesarios para mitigar los riesgos legales.
Responsable de gestión de riesgos	• Definir la metodología y criterios del análisis de riesgos junto con los responsables de verificación del cumplimiento y de seguridad. • Efectuar la identificación y el análisis de riesgos.
Responsable de auditoría interna	• Efectuar las revisiones del sistema y del proceso de la evaluación de impacto.
Delegado de protección de datos	• Asesorar en materia de protección de datos en la evaluación de impacto respecto de sus riesgos y medidas aplicables.

Fuente: elaboración propia.

6.2. DESCRIPCIÓN DEL SISTEMA DE IA

En este primer punto del proceso, es necesario perfilar un marco contextual sobre los elementos que conforman el sistema de IA. Profundizando en el concepto de sistema de información[128], este está formado por los denominados activos esenciales:

a. un *servicio* que se presta sobre la base del sistema, y

b. la *información* que el sistema trata.

Subordinados a los anteriores activos, se pueden identificar otros activos que prestan soporte:

1. *Datos* que materializan la información.

2. *Servicios auxiliares* que se necesitan para poder organizar el sistema.

3. Las *aplicaciones informáticas* (software) que permiten manejar los datos.

4. Los *equipos informáticos* (hardware) que permiten hospedar datos, aplicaciones y servicios.

5. Los *soportes de información* que son dispositivos de almacenamiento de datos.

6. El *equipamiento auxiliar* que complementa el material informático.

7. Las *redes de comunicaciones* que permiten intercambiar datos.

8. Las *instalaciones* que acogen equipos informáticos y de comunicaciones.

9. Las *personas* que explotan u operan todos los elementos anteriormente citados.

[128] MAGERIT e ISO/IEC 27005.

En primer lugar, se debe describir la *gestión del servicio* sustentado por el sistema de IA. Esto conllevará definir:

a. los objetivos que se persiguen mediante el desarrollo del servicio basado en sistemas de IA;

b. la descripción de los procesos internos que contribuyan a cumplir los objetivos definidos;

c. el contexto que va a operar el servicio; y

d. los umbrales de excelencia y error (expectativas) que se presumen del servicio.

En segundo lugar, se debe determinar la información que se va a tratar por parte de los sistemas. Esta información puede ser de diversa índole, como información comercial o datos personales. En caso de que el servicio utilice para su prestación datos personales, será necesario determinar los siguientes puntos:

a. categoría de datos personales;

b. categoría de interesados;

c. finalidad del tratamiento de los datos personales;

d. base legal del tratamiento;

e. existencia de comunicaciones o acceso por terceros de los datos personales.

En este punto, cabe evaluar si la finalidad del tratamiento constituye, en un primer momento, un tratamiento de alto riesgo; para ello deberá evaluar los mayores riesgos en los tratamientos que supongan, según el artículo 28 de la Ley Orgánica 3/2018, que:

a. Pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad

de datos sujetos al secreto profesional, reversión no autorizada de la pseudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b. Pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c. Se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y artículos 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

d. Implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e. Lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f. Se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g. Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

h. Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

Es aquí donde debe evaluarse la proporcionalidad del sistema de IA, para el cual puede utilizarse el tradicional juicio de proporcionalidad:

1. El sistema de IA debe ser adecuado para el fin perseguido.

2. El sistema de IA debe generar la menor injerencia posible en los derechos de los usuarios a la hora de lograr los fines.

3. El sistema de IA debe ser proporcional respecto al beneficio que persigue y los perjuicios que genera el sistema en cuanto a las amenazas existentes.

6.3. EVALUACIÓN DE LA CONFIANZA DEL SISTEMA DE IA

El fin de garantizar la confianza sobre el sistema de IA es, según el objetivo para el cual se haya desarrollado, que el sistema tome la decisión adecuada de manera segura. Para ello, en primer lugar, debe determinarse el objetivo que el sistema pretende cumplir, cómo pretende cumplirlo y cómo debe entenderse que el objetivo se ha cumplido a la hora de tomar la decisión.

Un criterio que debe afectar al objetivo propuesto del sistema y su correspondiente decisión es que, en cualquier caso, el objetivo del sistema y las decisiones que este tome no pueden permitir la posibilidad de incumplimientos legales o decisiones con dudosa base ética. Por ello el sistema debe garantizar que sus resultados nunca se contrapongan a la realidad ética o legal aplicable.

Se debe llevar a cabo una gestión del riesgo legal y ético basado en el contexto de despliegue del sistema, teniendo en cuenta dónde se aplica, cuáles son los objetos subjetivos de decisión del sistema y el marco legal aplicable de acuerdo a lo explicado en el apartado 5.

En la evaluación de la confianza del sistema, se debe analizar la probabilidad de las decisiones impredecibles del sistema; esto es, que la decisión tomada no pueda ser explicada o reproducible completamente conforme a lo esperado, y qué

impacto puede generar las decisiones impredecibles en su contexto de despliegue, junto con las medidas que deben aplicarse para mitigar este riesgo.

La confianza del sistema debe ser probada durante las fases de desarrollo, documentándolas y evaluándolas para tomar la mejor decisión respecto al tratamiento de los riesgos.

La evaluación de la seguridad consiste también en la evaluación de la confianza del sistema. Ya no solo por la relación de la seguridad de la información con las obligaciones legales, sino porque un sistema que pueda tener vulnerabilidades es un grave riesgo para la información y la toma de decisiones.

Como hemos analizado en el apartado 4, identificamos los potenciales riesgos sobre la confidencialidad, integridad y disponibilidad de los sistemas de IA, además de las posibles medidas para mitigar los diferentes riesgos de seguridad.

La EIOPA proporciona una serie de indicadores que deberían tenerse en cuenta a la hora de evaluar la probabilidad y el impacto de los riesgos sobre los sistemas de IA, basándose en los impactos diferenciados entre los consumidores y la entidad, sobre unos criterios de probabilidad comunes.

Indicadores de casos de uso en la evaluación de impacto

	AI Use case Impact Assessment	
	Impact on consumers	Impact on insurance firms
Severity	Number of consumers affected	Business continuity
	Consumer interaction and interests	Financial Impact
	Types of consumers (e.g. vulnerable consumers)	Legal Impact
	Human autonomy	Reputational Impact
	Anti-discrimination and diversity	
	Insurance line of business relevance	

Continúa

	AI Use case Impact Assessment	
	Impact on consumers	Impact on insurance firms
Likelihood	Evaluation or scoring, including profiling and predicting	
	Automated-decision making with legal or similar significant effect	
	Systematic monitoring	
	Model complexity/combining datasets	
	Innovative use or applying new technological or organisational solution	
	Type and amount of data used	
	Outsourcing datasets and AI applications	

Fuente: EIOPA.

El resultado de la evaluación de los riesgos legales, éticos y de seguridad de la información deben ser reportados al comité de gestión integral, que tratará los riesgos de acuerdo con su umbral aceptable.

6.4. EVALUACIÓN DE LA TRANSPARENCIA DEL SISTEMA DE IA

Como hemos analizado a lo largo de la obra, la transparencia es un elemento fundamental, además de obligatorio, a la hora de configurar las garantías del sistema de IA. La transparencia debe garantizarse mediante la aplicación de medidas que afecten a la trazabilidad, la explicabilidad y la auditabilidad de las decisiones.

El comité de gestión integral deberá determinar el umbral de transparencia del sistema; es decir, determinar cuándo el proceso de decisión ha sido suficientemente transparente sobre la base de las medidas y la auditoría del algoritmo.

7. DERECHO INTERNACIONAL PRIVADO E IA

En el negocio asegurador son numerosos los datos personales que se pueden recopilar, esto puede generar tantos problemas como beneficios si tales datos personales no son tratados correctamente. El uso de datos masivos personales implica un riesgo para los derechos fundamentales de los individuos, como el derecho a la intimidad y a la protección de datos. Muchos de esos datos tienen mucha incidencia en los derechos mencionados, por eso el marco jurídico de la protección de datos otorga una protección especial a tales categorías con el fin de preservar la inviolabilidad de los derechos y libertades fundamentales.

Por ello la rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales[129].

Las implicaciones derivadas del uso ilícito de los datos personales se han estudiado desde una perspectiva eminentemente jurídica y desde el punto de vista del Derecho internacional privado, ya que la situación geográfica de las partes y la pluralidad de lugares en los que se puede cometer el hecho dañoso que derive una responsabilidad civil extracontractual han demostrado que esta rama del Derecho es la más adecuada para dar respuesta a los diversos problemas que suscita la reclamación económica de los afectados.

[129] *Vid*. Considerando 6 del RGPD.

7.1. TRATAMIENTO ILÍCITO DE LOS DATOS DE CARÁCTER PERSONAL, CONTRATOS DE SEGURO Y DERECHO INTERNACIONAL PRIVADO

Los tratamientos de datos nominativos generan una serie de responsabilidades de índole administrativo, civil y, en su caso, penal; responsabilidades que recaerán, en forma individual o colectiva, sobre el titular del fichero, el responsable de este, el encargado del tratamiento, el responsable de seguridad, o sobre aquellas otras personas relacionadas directa o indirectamente con el fichero a quienes, por sus facultades o actos, pudieran serles atribuidas. Estas responsabilidades pueden dividirse en responsabilidades contractuales y responsabilidades extracontractuales.

1. *Responsabilidades contractuales*

   Respecto a las responsabilidades contractuales, los marcos normativos de referencia establecen que, cuando no sea posible obtener el cumplimiento de cualquier obligación, previamente pactada, relacionada con la protección de los datos, se sustituirá dicho cumplimiento por una indemnización a la persona concernida que deberá cubrir la totalidad de daños y perjuicios ocasionados por el incumplimiento.

   Como excepciones a la regla general de responsabilidad por incumplimiento contractual, establecida en la teoría general del contrato, se suelen establecer en el cuerpo del mismo, por un lado, mediante cláusulas de limitación de responsabilidad, un tope a la cuantía máxima de indemnización, y por otro, mediante las denominadas cláusulas penales, la fijación de una cuantía que, como compensación de los presuntos daños causados, se establece como cobertura de la responsabilidad derivada del incumplimiento, evitando los problemas que suelen surgir con la prueba de cuantificación de los daños ocasionados.

2. *Responsabilidades extracontractuales*

   En cuanto a las responsabilidades extracontractuales, estas se establecen, en lo que respecta a la protección de datos, como protección de la persona

afectada ante los daños que pueda sufrir derivados del riesgo generado por el tratamiento de sus datos nominativos. Así pues, el primer elemento a considerar, en lo que respecta a la responsabilidad civil, es la generación de un daño consumado cierto, personal, directo y que afecte a intereses legítimos de la víctima, elementos todos ellos imprescindibles para exigir esta responsabilidad.

El daño causado puede afectar tanto a la esfera patrimonial, que abarcará tanto la pérdida efectiva como el lucro cesante, como a la esfera moral, que abarcará cualquier tipo de perjuicio susceptible de incidir en el ámbito espiritual de la víctima y, en especial, dados los riesgos habitualmente generados por los tratamientos de datos, en la vulneración de sus derechos al honor, intimidad o propia imagen.

7.1.1. El derecho a la indemnización del RGPD

El RGPD regula *por primera vez el derecho a la indemnización derivado de los daños causados por el tratamiento ilegal de los datos de carácter personal en el artículo 82,* al contrario que la directiva, que se dedicaba en el artículo 23 a obligar a los Estados a configurar el derecho a la indemnización en sus ordenamientos internos. En España, la transposición se realizó en el artículo 19 de la LOPD.

El artículo 82 establece la responsabilidad del responsable del tratamiento: "Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente reglamento". Se establece la responsabilidad del responsable cuando participe en una operación en la que no cumpla, tanto por acción como por omisión, las normas del RGPD dirigidas a los encargados, o cuando el encargado obvie las indicaciones del responsable.

El RGPD establece un *sistema de responsabilidad directa* del responsable del tratamiento por los daños causados a una persona física tanto si el tratamiento se llevase a cabo en un establecimiento del responsable como si se externalizase a un tercero encargado. La responsabilidad de este último es limitada, puesto que solo responderá cuando el daño y perjuicio deriven de un incumplimiento de las

obligaciones legales del RGPD y de sus normas derivadas. Podemos entender como lógica esta limitación, puesto que el encargado del tratamiento actúa por mandato del responsable[130].

Cuando nos referimos al incumplimiento de lo dispuesto en el RGPD, incluimos las normas de desarrollo aportadas por los Estados miembros en cumplimiento del RGPD[131]. En este punto, cabe distinguir *una doble esfera de responsabilidad*[132]:

La que se deriva del incumplimiento de las disposiciones del RGPD y sus normas de desarrollo que conlleva automáticamente a indemnizar el daño.

Demostrar la ausencia de responsabilidad en el hecho que haya causado el daño y que va junto con la adopción de las medidas técnicas y organizativas que impone el artículo 24 del RGPD. Se debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta[133]. La anterior afirmación hace que nos situemos en el supuesto del artículo 1902 del CC[134], pero es un mero espejismo, puesto que el mismo artículo 24 debe demostrar, además, la conformidad de las actividades del tratamiento con el RGPD. Esto conlleva a invertir a carga de la prueba y demostrar que no se actuó con la debida diligencia.

Como hemos dicho anteriormente, podemos encontrarnos una responsabilidad subjetiva, aquella que se genera con el incumplimiento de cualesquiera obligaciones civiles legales o contractuales y asimismo de los actos u omisiones ilícitos, siempre y cuando intervenga culpa o negligencia y se produzca un daño; y una responsabilidad objetiva, aquella que se genera con la mera producción de un determinado daño concreto, sin que la causa del mismo provenga de una determinada

---

130 *Vid.* Recio Gayo, M., "Acerca de la evolución de la figura del encargado del tratamiento", *Revista de Privacidad y Derecho Digital,* n. 0, 2015.

131 *Vid.* Considerando 146 del RGPD.

132 López Álvarez, L. F., *Protección de datos personales: adaptaciones necesarias al nuevo reglamento europeo*, Francis Lefebvre, Madrid, 2016, p. 176.

133 *Vid.* Considerando 74.

134 "El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado".

infracción del ordenamiento jurídico, o de culpa o negligencia (ya sea directa o indirecta) del imputado.

El sistema introducido por el RGPD es un sistema de responsabilidad subjetiva. En este sentido, el párrafo tercero del artículo 82 del RGPD exonera de responsabilidad por los daños causados en la operación de tratamiento al responsable y encargado si se demuestra que no es responsable en modo alguno del hecho que haya causado los daños y perjuicios.

Respecto al objeto que se debe indemnizar, son indemnizables los daños y perjuicios materiales o inmateriales; es decir, se cubren tanto los daños físicos como morales, interpretándose el concepto de "daños y perjuicios" que dicta el TJUE[135], por lo que se viene a buscar una reparación integral del daño sufrido. En cuanto a los daños morales, destacamos la reciente STS 261/2017, de 26 de abril, en la que estipula los criterios para evaluar el daño moral por el incumplimiento de los requisitos de la LOPD. En ella, el Tribunal considera como relevantes:

- El tiempo de permanencia de los datos.
- El alcance de la divulgación de los datos personales a terceros.
- La inacción del responsable del tratamiento (fichero).

El RGPD regula la responsabilidad solidaria del responsable y el encargado, permitiendo al afectado demandar una indemnización total y efectiva tanto al responsable como al encargado, pudiendo repetir el sujeto que abonó la indemnización contra el resto de los sujetos intervinientes por la parte que les correspondería pagar.

La STS 574/2016 estipula que el responsable del tratamiento de esos datos es quien gestiona técnica y administrativamente los medios, el motor de búsqueda. Y es la empresa matriz quien destina los medios para gestionarlo. La empresa

[135] *Vid.* Considerando 146 del RGPD. En cuanto a la doctrina del TJUE, *vid.* STJUE *Liffers* (Asunto C-99/15). (ECLI:EU:C:2016:173).

filial no sería responsable si entre sus actividades principales no consta ninguna orientada a la indexación o almacenamiento de datos. Estas incidencias no pueden dirigirse contra la entidad filial, sino contra la matriz.

Por el contrario, la STS 210/2016 considera que el responsable del tratamiento es en la mayoría de los casos la filial, ya que, según el TJUE, interpretando la Directiva 95/46, no se exige para la aplicación del Derecho nacional que el tratamiento de los datos sea efectuado directamente por el propio establecimiento (la matriz), sino que se halle en las actividades de este. Considera que las actividades de la matriz y de la filial están ligadas porque la filial, aun no dedicándose directamente a la indexación de la información, realiza actividades de promoción del medio de indexación (motor de búsqueda), además de ofrecerle los recursos económicos, sin importar la forma jurídica de la filial. Por lo tanto, la filial y la matriz son corresponsables del tratamiento de datos, y está legitimada pasivamente para ser parte demandada en los litigios seguidos en España en que los afectados ejerciten en un proceso civil sus derechos de acceso, rectificación, cancelación y oposición.

La sentencia de la sala primera explica que las sentencias no son contradictorias; ya que ambos casos están regidos por normas y principios totalmente diferentes, por lo que, para los casos respecto a procedimientos de tutela de derechos en materia de protección de datos, el responsable será la matriz extranjera. Para el ejercicio en un proceso civil de sus derechos, lo será también la filial nacional. La postura adoptada por el TS está fundamentada en el alto coste que supondría litigar contra una persona jurídica en el extranjero; aparte, esta postura tiene el objetivo de favorecer a la parte débil (consumidor) en las transacciones internacionales de flujos de datos, permitiendo al afectado litigar en su lugar de residencia y sobre la base de su derecho nacional[136].

[136] Idea recogida en la STJUE, de 25 de octubre de 2011, *eDate Advertising y Martínez,* C-509/09 y C-161/10, y plasmada en el artículo 79.2 RGPD (TJCE\2011\331) (ECLI:EU:C:2011:685).

7.1.2. Responsabilidad contractual derivada del incumplimiento de un contrato de seguro

Un contrato de seguro implica el tratamiento de datos personales, tanto ordinarios como sensibles, para los cuales la entidad aseguradora debe proteger obligatoriamente según las disposiciones legales nacionales e internacionales. Pero eso no impide que se pueda acordar contractualmente el compromiso de la entidad aseguradora de proteger los datos personales según la legislación vigente. Es más, en el propio contrato deberán constar los fines destinados a tal tratamiento; "la naturaleza contractual o no de la acción ejercitada con fundamento en el precepto que nos ocupa dependerá de la existencia o no de una relación contractual con fundamento en la cual se hayan cedido los datos personales al responsable del fichero"[137]. Por lo tanto, "las obligaciones del responsable del fichero o del encargado del tratamiento han de integrarse, además y *ex* artículo 1258 del CC, con las obligaciones legales y reglamentarias previstas"[138].

7.1.2.1. Cláusulas de exoneración o limitación de responsabilidad

Es común por los proveedores de tecnología Big Data incluyan cláusulas de limitación o exoneración de responsabilidad, alegando que estos suministradores no tratan los datos personales, o que puede llegar a ser imposible conseguir una completa anonimización, o porque tales proveedores no tratan los datos personales. Por ello, la estipulación de dichas cláusulas puede considerarse abusivas y nulas según la legislación nacional y comunitaria.

En una relación "profesional-profesional" la empresa contratante de tecnología Big Data no puede considerar consumidores a efecto de las Directivas 93/13/CEE[139] y 2011/83/UE[140], ni tampoco de la STJUE *Costea,* en la que permite a los profesionales ser consumidores ante comerciantes si el contrato no tiene relación

[137] *Vid.* Buttarelli, G., *Banche dati e tutela della riservatezza (La* privacy *nella Società dell'Informazione),* Giuffrè Editore, Milán, 1997, pp. 351-352.

[138] *Vid.* Busto Lago, J. M., "La responsabilidad civil de los servidores y operadores de datos", en *Seminario sobre Protección de Datos*, UCLM, Ciudad Real, 2005, p. 18.

[139] DO L 95 de 21 de abril de 1993.

[140] DO L 304 de 22 de noviembre de 2011.

con la actividad profesional. Por lo tanto, desde la perspectiva española no es aplicable la Ley General para la Defensa de los Consumidores y Usuarios[141], sino la Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación[142], tal y como estipula la STS 57/2017 de 30 de enero.

Pero, tal y como dice en el preámbulo de la exposición de motivos I de esta última ley, "las cláusulas generales de contratación pueden darse entre profesionales, y en tal relación pueden existir cláusulas abusivas, pero tal régimen debe atenerse a las reglas de nulidad contractual y no la lista de cláusulas abusivas recogidas en los artículos 82-85 de la Ley General para la Defensa de los Consumidores y Usuarios". Pero en esa exposición reconoce también que pueda existir un abuso de una posición contractual dominante y una condición general que sea abusiva cuando sea contraria a la buena fe[143] y cause un desequilibrio importante entre los derechos y obligaciones de las partes, incluso aunque se trate de contratos entre profesionales o empresarios. Pero habrá de tener en cuenta en cada caso las características específicas de la contratación entre empresas.

Para obtener tal nulidad, debe tenerse en cuenta el nivel de información presentado por el empresario no adherido, y la diligencia del empresario no adherente para conocer tales consecuencias jurídicas, que dependerá, en gran medida, de sus circunstancias subjetivas, como personalidad jurídico-mercantil, volumen de negocio, estructura societaria, experiencia, conocimientos financieros, asesoramiento, etc.

Y puesto que el adherente no es consumidor, operan las reglas generales de la carga de la prueba, por lo que habrá de ser el prestatario que pretende la nulidad quien

[141] BOE, n. 287 de 30 de noviembre de 2007.

[142] BOE, n. 89 de 14 de abril de 1998.

[143] STS 367/2016 de 3 de junio: "La virtualidad del principio general de buena fe como norma modeladora del contenido contractual, capaz de expulsar determinadas cláusulas del contrato, es defendible, al menos, para las cláusulas que suponen un desequilibrio de la posición contractual del adherente, es decir, aquellas que modifican subrepticiamente el contenido que el adherente había podido representarse como pactado conforme a la propia naturaleza y funcionalidad del contrato; [...]. [...] puede postularse la nulidad de determinadas cláusulas que comportan una regulación contraria a la legítima expectativa que, según el contrato suscrito, pudo tener el adherente [...]. Conclusión que es acorde con las previsiones de los principios de Derecho europeo de los contratos, formulados por la Comisión de Derecho Europeo de los Contratos [...]" (ECLI: ES: TS: 2016:2550).

acredite la inexistencia o insuficiencia de la información y quien, ya desde la demanda, indique cuáles son sus circunstancias personales que pueden haber influido en la negociación y en qué medida la cláusula le fue impuesta abusivamente.

Pasando al régimen concreto de una cláusula de exoneración de responsabilidad, cabe recordar que si el incumplimiento contractual fuera doloso, el artículo 1102 del CC estipula que siempre es exigible toda responsabilidad (no cabe tampoco limitación) derivada del dolo, y toda renuncia de la acción es nula. Es indiferente que tales pactos se hayan estipulado en el momento de la celebración del contrato, esto es, incluyéndose en él como una de sus cláusulas o, por el contrario, hayan sido estipulados con posterioridad a la celebración de este en un documento separado[144].

En cambio, se discute la posibilidad de admitir cláusulas de limitación o exoneración de la responsabilidad si el hecho fuera negligente. En el Derecho español no existe ninguna disposición como la que se recoge en el artículo 1102 del CC, por lo que se argumenta su admisibilidad sobre la base del artículo 1003 del CC[145]. Se ha afirmado, así que, dado que el precepto permite a los contratantes pactar el grado de diligencia exigible en el cumplimiento de las obligaciones, estas pueden pactar que no les sea exigible ningún grado de diligencia en dicho cumplimiento, admitiéndose, en consecuencia, la validez general de las cláusulas de exoneración de responsabilidad procedente de culpa[146]; pero ello no significa que todas las cláusulas sean válidas, puesto que no deben ser contrarias a la buena fe del artículo 1255 del CC. En estos casos hay que distinguir entre la culpa grave y la leve:

1. En caso de *negligencia grave,* las cláusulas de exoneración de responsabilidad pueden ser declaradas nulas por ser contrarias al orden público, por ser tal culpa casi equiparable al dolo y, por lo tanto, siendo aplicable el artículo 1102 del CC (SSTS de 18 de junio de 1990 y 3 de julio de 1992). En cuanto a las

[144] *Vid.* De Verda y Beamonte, J. R., "Las cláusulas de exoneración y limitación de responsabilidad en el Derecho español", *Revista Chilena de Derecho Privado*, n. 4, Universidad Diego Portales, Santiago, 2005, p, 37.

[145] "La responsabilidad que procede de negligencia es igualmente exigible en el cumplimiento de toda clase de obligaciones".

[146] *Vid.* Álvarez Lata, N., *Cláusulas restrictivas de responsabilidad civil,* Comares, Granada, 1998, p. 84.

cláusulas de limitación, se consideran nulas cuando la responsabilidad se derive por negligencia grave.

2. Se puede admitir cuando sea por *culpa leve* en virtud del artículo 1103 del CC que permite a los tribunales moderar la responsabilidad en caso de negligencia. Además, deben ser inválidas las cláusulas de limitación de responsabilidad por daños ocasionados a las personas (muerte o lesiones) y las cláusulas de limitación por culpa leve que, encubiertamente, causan una exoneración completa. Respecto a las cláusulas de limitación, caben distinguir y analizar las siguientes variantes:

    a. *Cláusula limitativa de la cuantía del resarcimiento.* Es admisible por nuestro Derecho la existencia de cláusulas limitativas que absorban la indemnización por daños y perjuicios (artículo 1152 del CC y STS, 16 de julio de 1982), pero serán nulas si la cuantía es irrisoria o desproporcionada al daño producido.

    b. *Las cláusulas limitativas de la garantía patrimonial universal.* Son admisibles las cláusulas limitativas de la responsabilidad efectiva sobre ciertos bienes.

    c. *Las cláusulas que acortan los plazos de prescripción de la acción.* Son válidas las cláusulas que limitan la responsabilidad del deudor, acortando el largo plazo de prescripción de la acción para exigir indemnización de daños por incumplimiento, que es de cinco años, según resulta del artículo 1964 del Código Civil. No obstante, los pactos de acortamiento del plazo de prescripción serán nulos cuando el plazo señalado fuera tan breve que, en la práctica, hiciera inviable el ejercicio de la acción.

7.1.3. Protección de datos, contratos de seguro y Derecho internacional privado

7.1.3.1. Competencia judicial internacional y RGPD

El artículo 82 del RGPD remite al artículo 79.2 el lugar donde debe dirigirse el afectado derivado de un supuesto de responsabilidad del artículo 82. En este sentido, el artículo 82.6 nos remite al artículo 79.2, que dispone que las acciones

dirigidas contra encargados o responsables deberán dirigirse ante los tribunales competentes del Estado miembro donde tengan su establecimiento, o del Estado miembro donde el reclamante tenga su domicilio, en concordancia con lo estipulado en el considerando 145[147].

Las reclamaciones legales en materia de protección de datos pueden ser tanto contractuales como extracontractuales. Es posible que ese tratamiento de datos se produzca en el contexto de un contrato, y según la jurisprudencia del TJUE, una acción de responsabilidad civil de naturaleza extracontractual deberá entenderse incluida en la materia contractual a los efectos del artículo 7 del Reglamento "Bruselas I Bis" si el comportamiento recriminado comporta un incumplimiento de las obligaciones contractuales cuando se estudie caso por caso el objeto del contrato[148]. Puesto que en un contrato se puede pactar el compromiso del cumplimiento de la legislación sobre la materia, o bien el compromiso de la adopción de medidas de seguridad que, en caso de revisarse que la contraparte no las ha aplicado, insta el cumplimiento o reclamación en su caso[149].

El artículo 79.2 permite demandar en el Estado miembro en el que el responsable o el encargado tengan un establecimiento, pero debe entenderse "establecimiento" como "lugar donde se realice cualquier actividad real y efectiva, aun mínima, ejercida mediante una instalación estable", y el "grado de estabilidad de la instalación como la efectividad del desarrollo de las actividades tomando en consideración la naturaleza específica de las actividades económicas y de las prestaciones de servicios en cuestión"[150].

---

147 Por lo que respecta a las acciones contra los responsables o encargados del tratamiento, el reclamante debe tener la opción de ejercitarlas ante los tribunales de los Estados miembros en los que el responsable o el encargado tenga un establecimiento o resida el afectado, a menos que el responsable sea una autoridad pública de un Estado miembro que actúe en el ejercicio de poderes públicos.

148 *Vid*. STJUE, de 13 de marzo de 2014, *Brogsitter*, C-548/12; 14 de julio de 2016, *Granarolo*, C-196/15.

149 *Vid.* Gonzalo Domenech, J. J., "Algunas cuestiones relevantes de Derecho internacional privado del Reglamento General de Protección de Datos", *Revista Boliviana de Derecho*, n. 26, 2018, p. 418.

150 *Vid.* Apartados 31 de la STJUE *Weltimmo,* y 75 de la STJUE *Amazon EU Sàri*.

El foro alternativo que prevé el RGPD permite a los afectados demandar en los tribunales del Estado donde tengan su residencia habitual. Para su consideración, será necesario que el afectado tenga un grado de permanencia que revele una situación de estabilidad[151].

El RGPD pone a disposición de los afectados la posibilidad puedan utilizar los foros de competencia del artículo 79.2, en contra del inciso imperativo que recoge ese mismo párrafo. Por lo tanto, cabe afirmar que los foros recogidos en el RGPD son complementarios a los recogidos por el Reglamento "Bruselas I bis" que explicamos a continuación:

1. *Sumisión expresa* (artículo 25 del "Bruselas I bis"). Es lo que se conoce como una prolongación de la autonomía de la voluntad al campo de la competencia judicial internacional[152].

2. *Sumisión tácita* (artículo 26 del "Bruselas I bis"). La siguiente conducta procesal de las partes significará que estamos ante una sumisión tácita cuando el demandante presenta una demanda ante el tribunal de un Estado miembro y la comparecencia del demandado ante ese tribunal no tiene por objeto impugnar su competencia judicial[153]; es decir, entra a discutir sobre el fondo del asunto.

3. *Foro del domicilio del demandado* (artículo 4 del "Bruselas I bis"). Este foro de competencia es un clásico de los instrumentos normativos de atribución de competencia. A falta de pacto expreso o tácito, el criterio atributivo de competencia es el del domicilio del demandado, que hace competentes a los tribunales del domicilio del demandado. El propio Reglamento "Bruselas I bis" nos da una definición de domicilio en el artículo 63, el cual se entenderá que una persona jurídica está domiciliada en el Estado en el que se encuentra: a) su sede estatutaria; b) su Administración central, o c) su centro de actividad

[151] *Vid*. STJUE, 22 de diciembre de 2010, C-497/10, *Mercredi* (ECLI: EU: C: 2010:829).

[152] *Vid.* Ortega Giménez, A., "Imagen y circulación internacional de datos", *Revista Boliviana de Derecho*, n. 15, Fundación Iuris Tantum, Santa Cruz (Bolivia), 2013, p. 138.

[153] *Vid. Op. Supra,* p. 139.

principal. En cuanto a la residencia habitual de una persona física, el artículo 62 nos remite a la ley interna del propio Estado[154], puesto que el Reglamento "Bruselas I bis" no nos aporta una noción autónoma del concepto.

4. *Foro especial en materia de obligaciones extracontractuales:* el "lugar donde se hubiere producido o pudiere producirse el hecho dañoso" (artículo 7.3 del "Bruselas I bis"). Consiste en un foro especial regido por el principio de ubicuidad que, en el caso de efectuar una acción por daños y perjuicios, el demandante tiene derecho a elegir entre los tribunales del lugar donde se produjo el hecho dañoso (ya sea donde se haya producido el hecho generador del daño o donde se padezca el daño). Constituye la solución tradicional en esta materia[155]:

    a. El principal problema que plantea el *forum locus delicti commissi* es el de determinar si por país en que se produce el daño debemos entender el del lugar en el que se localiza el hecho causal (p. ej., el Estado donde se recaban los datos).

    b. O el del lugar en que se verifica el resultado dañoso (p. ej., el Estado donde se acceden a los datos).

Debemos destacar que podemos encontrarnos, además de los supuestos del artículo 79 del RGPD y los propios de "Bruselas I bis", que tal perjuicio se materialice en el marco de una relación contractual, por lo que debemos atenernos a los foros concretos en materia contractual del Reglamento "Bruselas I bis" (competencia especial en materia contractual del artículo 7.1); foros especiales de protección en materia de seguros de los artículos 10-16; foros especiales de protección en materia de contratos celebrados por los consumidores de los artículos 17-19; y foros especiales de protección en materia de contratos individuales de trabajo de los artículos 20-23), que pueden actuar con una doble función: por un lado, establecer un

[154] En el caso de España, el artículo 40 CC señala que "para el ejercicio de los derechos y el cumplimiento de las obligaciones civiles, el domicilio de las personas naturales es el lugar de su residencia habitual y, en su caso, el que determine la Ley de Enjuiciamiento Civil".

[155] *Vid.* Ortega Giménez, A., "Imagen y circulación internacional de datos", *Revista Boliviana de Derecho*, p. 142.

foro de protección especial para la parte que ha sufrido el daño y perjuicio, en casos en los que una parte de una relación contractual es la parte débil, como en los contratos de seguro o celebrados por los consumidores; y por el otro, suplir la ausencia de unos foros especiales para los responsables del tratamiento cuando estos pretendan ejercitar alguna acción contra los afectados[156].

7.1.3.2. Competencia judicial internacional y otros instrumentos normativos derivada de la consideración de contrato internacional de seguro

A la hora de enfrentarnos al estudio del contrato internacional de seguro, cabe tener en cuenta los siguientes elementos[157]:

- Podemos encontrar varios elementos subjetivos en los que suele haber una parte más fuerte que la otra, como es el asegurador, frente a una parte más débil, como pueden ser el tomador, el asegurado y el beneficiario.

- La existencia de resoluciones en las que haya normas más flexibles que permitan proteger a dichas partes débiles.

- La existencia de contratos de seguro en los que no existe parte débil, como los relativos a los grandes riesgos, por lo que se asemejan al resto de contratos internacionales.

En cuanto a las normas aplicables al contrato de seguro, son aplicables respecto a la competencia judicial internacional: 1) el Reglamento "Bruselas I bis" en el ámbito institucional; 2) el Convenio de Lugano de 2007 en el ámbito convencional, y 3) la LOPJ cuando ninguna de las normas anteriores encaje en el ámbito de aplicación[158].

---

[156] *Vid.* Gonzalo Domenech, J. J., "Algunas cuestiones relevantes de Derecho internacional privado del Reglamento General de Protección de Datos", *Revista Boliviana de Derecho,* n. 26, p. 421.

[157] *Vid.* Carrascosa González, J. y Calvo Caravaca, A.-L. (dirs.), *Derecho internacional privado,* vol. II, 16.ª ed., Comares, Granada, 2016, p. 1058.

[158] No será de aplicación el Convenio de La Haya de 2005 sobre elección de foro, puesto que la Unión Europea efectuó una reserva respecto a la aplicación del convenio a los contratos de seguro debido a que quiere preservar las normas recogidas en el Reglamento "Bruselas I bis".

El Reglamento "Bruselas I bis" tiene como uno de sus objetivos principales la protección de la parte débil de los contratos de seguro mediante la disposición de normas más beneficiosas[159], puesto que no goza de la facultad de negociar las cláusulas del contrato al ser económicamente más débil[160]. Serán de aplicación los foros contenidos en los artículos 6 y 7.5, en los que cabe encontrar: sumisión tácita, sumisión expresa y foros alternativos. Cabe decir que la aplicación de este reglamento solo será posible si las partes están domiciliadas en un Estado miembro.

1. *Sumisión tácita (artículo 26.1).* Es destacable la existencia de la posibilidad de aplicación de la sumisión tácita del artículo 26.1 a partir de la STJUE *Bilas,* C-111/09. Por lo que un tribunal de un Estado miembro, *a priori* incompetente, podrá obtener la competencia si: a) el demandado comparece ante el tribunal sin impugnar la competencia; b) el tribunal pertenece a un Estado miembro, y c) en caso de que el demandado sea el tomador, asegurado o beneficiario, deberá ser informado de las consecuencias de su comparecencia o incomparecencia ante el órgano jurisdiccional. En el caso de que no exista la sumisión tácita, la competencia podrá ser atribuida por una cláusula expresa. La sumisión expresa se encuentra regulada, como norma general, en el artículo 25 del Reglamento "Bruselas I bis", pero en materia de seguros, se aplicará el artículo 15, cuyos acuerdos no podrán ser contrarios a las disposiciones del artículo 25. Existen cinco supuestos de sumisión expresa válidos, constituyendo así una "autonomía limitada para elegir el tribunal competente"[161].

2. *Sumisión expresa anterior al nacimiento del litigio (artículo 15.2-15.5):*

    a. *Sumisión expresa mediante la oferta de foros adicionales a la parte débil demandante (artículo 15.2)*. Se admiten los acuerdos "que permitan al tomador del seguro, al asegurado o al beneficiario formular demandas ante órganos judiciales distintos de los indicados en la presente sección".

---

[159] *Vid.* Considerando 8.

[160] *Vid.* STJCE C-201/82, *Gerling Vs. Amministrazione del Tesoro dello Stato,* apartado 17 (EU: C: 1983:217).

[161] *Vid.* Carrascosa González, J. y Calvo Caravaca, A.-L. (dirs.), *Derecho internacional privado,* vol. II, 16.ª ed., Comares, Granada, 2016, p. 1062.

Deben cumplirse determinadas condiciones:

- El demandante debe ser tomador, asegurado o beneficiario.

- La decisión viene de la parte débil, en relación con la ampliación de foros que estos disponen.

b. *Sumisión expresa a los tribunales a los tribunales del Estado miembro del domicilio o residencia común del tomador y asegurador (artículo 15.3)*. se admitirán como válidas las sumisiones expresas "que, habiéndose celebrado entre el tomador y el asegurador, ambos domiciliados, o con residencia habitual en el mismo Estado miembro en el momento de la celebración del contrato, atribuyan, aunque el hecho dañoso se haya producido en el extranjero, competencia a los órganos jurisdiccionales de dicho Estado miembro, a no ser que la ley de este prohíba tales acuerdos". Las condiciones necesarias para acordar tal acuerdo son:

   - Tanto tomador como asegurador deben estar domiciliados o tener la residencia habitual en el mismo Estado miembro.

   - El tribunal del Estado miembro ha de ser común al domicilio o residencia habitual del tomador y asegurador.

   - El acuerdo de sumisión expresa solo resulta vinculante para las dos partes, sin que pueda oponerse al asegurado-beneficiario que no haya aceptado la cláusula y tenga un domicilio en un Estado miembro diferente al de los anteriores162.

c. *Sumisión expresa celebrada con un tomador no domiciliado en un Estado miembro (artículo 15.4)*. El tomador no ha de estar domiciliado en un Estado miembro. Significa también que no existen vínculos fuertes con los tribunales de los Estados miembros. En esta situación a un tomador le perjudicaría gravemente cualquier litigio en la Unión; pero el tomador es considerado parte

[162] *Vid*. STJCE, *Société financière et industrielle du Peloux v Axa Belgium*, C-112/03, apartado 43.

débil y se le vincula al reglamento. Esta sumisión no puede referirse ni a un seguro obligatorio ni a de un inmueble sito en la Unión.

d. *Sumisión expresa en un contrato de seguro que cubre uno o varios riesgos del artículo 16 (artículo 15.5)*. Esos supuestos son los referidos a los grandes riesgos, como los daños a buques de navegación marítima, instalaciones costeras y en altamar o aeronaves, causados por hechos sobrevenidos en relación con su utilización para fines comerciales (artículo 16.1.a).

3. *Demandas del tomador, asegurado o beneficiario contra el asegurador.* Cuando los sujetos débiles en esta relación jurídica buscan emprender determinadas acciones, el reglamento pone a su disposición dos foros aplicables con independencia de la materia del propio seguro y otros foros adicionales según la materia del seguro.

   a. *Foro del Estado miembro del domicilio del asegurador (artículo 11.1.a)*. Este foro opera cuando el demandado es el asegurador, y el tribunal competente será el del Estado miembro en el que se encuentre domiciliado el asegurador. Puede darse el caso de que el asegurador no esté domiciliado en un Estado miembro, según el artículo 63, el artículo 11.2 permite demandar a las sucursales, agencias o cualquier tipo de establecimiento, con el mismo efecto que si el asegurador estuviera domiciliado en la Unión. Se mantiene así el mismo concepto flexible de "establecimiento" que hemos estudiado.

   b. *Foro del lugar del domicilio del tomador, asegurado o beneficiario (artículo 11.1.b)*. Si estos sujetos se encuentran domiciliados en Estados miembros diferentes al del asegurador, pueden usar su propio domicilio como foro. Para delimitar el domicilio del tomador, asegurado o beneficiario se hará de acuerdo a los criterios de los artículos 62 (persona física) y 63 (persona jurídica).

4. *Demandas del asegurador contra el tomador, asegurado o beneficiario.* Cuando el asegurador pretenda ejercer alguna acción contra ellos, los foros disponibles se reducen al foro del Estado miembro del domicilio del demandado, sea

el tomador, asegurado o beneficiario del artículo 14.1, el cual será determinado según las normas de los artículos 62 y 63 en su caso.

5. *Foro para los casos de reconvención (artículo 14.2).* En el caso de una reconvención, el artículo 14 no establece ningún foro especial para ello, por lo que hay que acudir al artículo 8.3 que indica que el tribunal que deberá reconocer la demanda reconvertida será el tribunal del Estado miembro que conoce la demanda inicial.

6. *Foro del artículo 7.5.* Este artículo permite demandar en otro Estado miembro si el litigio versa sobre la explotación de sucursales, agencias o cualquier otro establecimiento ante el órgano jurisdiccional en el que se hallen sitos. Este foro opera tanto para el asegurador, como para el tomador, asegurado o beneficiario.

7. *Contratos internacionales de seguro en el Convenio de Lugano de 2007.* Los foros establecidos en el Convenio de Lugano son los mismos que los establecidos en el Reglamento "Bruselas I bis", que podemos resumir de forma esquemática para su mejor entendimiento en:

    a. *Foros de sumisión expresa (artículo 13):*

        - Sumisión expresa posterior al nacimiento del litigio (artículo 13.1).

        - Sumisión expresa mediante la oferta de foros adicionales a la parte débil demandante (artículo 13.2).

        - Sumisión expresa a los tribunales del Estado miembro del domicilio o residencia común del tomador y asegurador (artículo 13.3).

        - Sumisión expresa celebrada con un tomador no domiciliado en un Estado miembro, salvo si se tratase de un seguro obligatorio o se refiera a un inmueble sito en un Estado miembro (artículo 13.4).

        - Sumisión expresa en un contrato de seguro que cubre uno o varios riesgos del artículo 14 (artículo 13.5).

b. *Demandas del tomador, asegurado o beneficiario contra el asegurador (artículos 9 y 10):*

   – Foro del tribunal del Estado miembro donde el asegurador tuviera su domicilio (artículo 9.1.a).

   – Foro del tribunal del Estado miembro donde el tomador, asegurado o beneficiario tuviera su domicilio (artículo 9.1.b).

   – Foro del Estado miembro del domicilio del asegurado cuando tuviera establecimientos en los Estados miembros (artículo 9.2).

c. *Demandas del asegurador contra el tomador, asegurado o beneficiario* (artículo 12):

   – Foro del Estado miembro del domicilio del demandado, sea el tomador, asegurado o beneficiario (artículo 12.1).

d. *Demandas formuladas indistintamente el sujeto entre las partes*:

   – Foro para los casos de reconvención (artículo 12.2).

   – Foro especial para litigios sobre la explotación de establecimientos (artículo 5.5).

8. *Contratos internacionales de seguro en la LOPJ de 2015.* Las normas autónomas se limitan a atribuir la competencia a los tribunales españoles[163]; además funcionan a modo subsidiario. El artículo 22 quinquies e) establece que en materia de seguros, cuando "el asegurado, tomador o beneficiario del seguro tuviera su domicilio en España, también podrá el asegurador ser demandado ante los tribunales españoles si el hecho dañoso se produjere en territorio español y se tratara de un contrato de seguro de responsabilidad o de seguro relativo a inmuebles, o

[163] Tanto el Reglamento "Bruselas I bis" como el Convenio de Lugano de 2007 determinan en sus artículos 6 y 4 respectivamente que si el demandado no se encuentra domiciliado en un Estado miembro, será la legislación interna quien determine la competencia.

tratándose de un seguro de responsabilidad civil, si los tribunales españoles fueran competentes para conocer la acción entablada por el perjudicado contra el asegurado en virtud de lo dispuesto en la letra b) de este artículo". La letra b) hace competentes a los tribunales españoles en materia de obligaciones extracontractuales si el hecho dañoso se ha producido en territorio español. En el último inciso del artículo señala que serán competentes los tribunales españoles cuando el tomador o asegurado sea demandante y la sumisión sea posterior al nacimiento de la controversia; y si fuera una sumisión expresa anterior al nacimiento, cuando ambas partes tuvieran ya su domicilio en España en el momento de celebración del contrato o el demandante fuera el asegurado o tomador del seguro.

7.1.4. Determinación de la ley aplicable

7.1.4.1. Determinación de la ley aplicable a la acción de responsabilidad extracontractual del RGPD

Hay supuestos de responsabilidad extracontractual, como es el caso de las transferencias internacionales de datos, que plantean importantes problemas en cuanto al Derecho aplicable. La ley que resuelve esta controversia es el Reglamento (CE) 864/2007 "Roma II"[164]. El Reglamento "Roma II" es un texto legal con carácter *universal*[165]; es decir, la ley designada por el reglamento se aplica, aunque no sea de un Estado miembro, y permite una mayor y mejor unificación del mercado anterior[166]; pero que excluye de su aplicación en su artículo 1.2.g "las obligaciones extracontractuales que se deriven de la violación de la intimidad o de los derechos relacionados con la personalidad, en particular, la difamación".

Debemos destacar que actualmente existe una propuesta de reforma del Reglamento "Roma II" en el que pretende incluir estos supuestos, motivada por la STJUE *eDate Advertising*[167], tendente a unificar la norma de conflicto y desplazar a la legislación interna.

---

[164] DOCE L 199/40, de 31 de julio de 2007.

[165] *Vid*. artículo 3.

[166] *Vid*. Ortega Giménez, A., *Transferencias internacionales de datos de carácter personal ilícitas,* Aranzadi, Cizur Menor, 2017, p. 138.

[167] P7_TA-PROV (2012)0200.

La reforma del Reglamento "Roma II" incluye un nuevo artículo 5 bis en el que introduce dos nuevos supuestos: 1) la ley del país en el que se produzcan o sea más probable que se produzcan el elemento o los elementos más significativos del daño o perjuicio, o 2) la ley del país de residencia habitual del demandado, en su defecto, si el demandado no hubiera podido haber previsto razonablemente consecuencias importantes de su acto en dicho país.

La adición de este doble criterio a la hora de la determinación de la ley aplicable puede llegar a prejuzgar el caso en una fase muy temprana del proceso, además de favorecer al presunto responsable del daño con la opción de litigar con la ley del país de residencia. La consecuencia de la no regulación conlleva a *la aplicación de normas autónomas como el artículo 10.9 del Código Civil,* que hace que apliquemos la ley del lugar donde se ha cometido el hecho *(lex loci delicti commissi)*[168]. Pero en este ámbito, la precisión del lugar en el que se produce el daño puede resultar controvertida en situaciones en las que las consecuencias lesivas del hecho dañoso no son de carácter material, y esta norma no precisa cuál es el lugar del daño en las situaciones en las que el hecho causal y el resultado lesivo se producen en distintos países[169].

El artículo 10.9 del CC nos otorga dos opciones para determinar la ley aplicable: 1) la aplicación de la *lex loci actus* (ley del Estado en el que se produce el hecho del que deriva la responsabilidad) o 2) la aplicación de la *lex loci damni* (aplicación de la ley del lugar donde se materializa el daño para las víctimas).

En la primera opción *(lex loci actus),* el mayor problema que encontramos es determinar cuál es el Estado en el que se ha realizado el hecho dañoso, esto es, el tratamiento automatizado de datos personales se rige por la ley del Estado en cuyo territorio tiene lugar dicho tratamiento de datos que ha provocado el daño[170,171].

---

[168] "Las obligaciones no contractuales se regirán por la ley del lugar donde hubiere ocurrido el hecho de que deriven".

[169] *Vid.* De Miguel Asensio, P. A., *Derecho privado de internet,* 4.ª ed., Civitas, Madrid, 2011, p. 201.

[170] *Vid*. Ortega Giménez, A., *Transferencias internacionales de datos..., op. cit.,* p. 143.

[171] Respecto al caso BGH NJW 2011, 2059 comentado anteriormente, el *Bundesgerichtshof* señaló explícitamente que la aceptación de la jurisdicción también conduciría a la aplicación del derecho alemán (artículo 40 (1) del EGBGB).

En cuanto a la segunda opción *(lex loci damni),* y en concreto en los supuestos de mero acceso, debe rechazarse que cualquier lugar de recepción de los contenidos o la información transmitidos por internet sea por esa simple circunstancia lugar del daño debido a 1) que muchas veces ese acto no genera un daño "real" al titular y 2) la aplicación de la ley de cada uno de los múltiples lugares de manifestación del daño puede conducir a una excesiva fragmentación normativa[172]. Por eso se afirma que el lugar donde se manifiesta la consecuencia directa para la víctima se corresponde con el lugar de su residencia habitual como el centro de las relaciones sociales, personales y económicas susceptibles de verse afectadas por un atentado contra la intimidad u otros derechos de la personalidad.

El artículo 79.2 del RGPD invita a aplicar "la ley del lugar donde sufren el daño o lesión los bienes o derechos del perjudicado"[173]. Su postura se basa en el objetivo que tiene la norma de proteger al afectado; una de las maneras de plasmarlo es la aplicación de un derecho que sea familiar al afectado que se correspondan con el del Estado de la residencia habitual (o del centro de intereses del afectado). En la práctica podemos prever que el demandante inicie las acciones bien en el Estado de la residencia habitual, bien en el centro de intereses del afectado; se aplicará la ley del Estado que asumió la competencia *(lex fori).*

7.1.4.2. Determinación de la ley aplicable a la acción de responsabilidad contractual por el incumplimiento del contrato internacional de seguro

En cuanto a la ley aplicable, el instrumento de referencia es el Reglamento (CE) 593/2008[174] y la Directiva (UE) 2016, centrándonos en la ley aplicable a los contratos internacionales de seguro que cubren otros riesgos distintos a los "grandes riesgos", que estén localizados en la Unión Europea.

[172] *Vid.* De Miguel Asensio, P. A., *Derecho privado..., op., cit.,* p. 203.

[173] *Vid.* De Miguel Asensio, P. A., "Competencia...", *op. cit.,* p. 42.

[174] DOUE L 177/6 de 4 de julio de 2008.

El ámbito de aplicación de la ley reguladora del contrato, que resulta de lo dispuesto en los arts. 10.1, 12 y 18.1 del reglamento, se refiere en particular a[175]:

- la formación y la validez sustancial (artículo 10.1);
- la interpretación (artículo 12.1 a);
- el cumplimiento de las obligaciones derivadas de él (artículo 12.1 b);
- dentro de los límites de las competencias atribuidas al tribunal por la respectiva ley de procedimiento, las consecuencias del incumplimiento total o parcial de dichas obligaciones, incluida la evaluación del daño, en la medida en que esta evaluación esté regulada por la ley (artículo 12.1 c);
- las diversas causas de extinción de las obligaciones (artículo 12.1 d);
- las consecuencias de la invalidez del contrato (artículo 12.1 e);
- las presunciones legales y el reparto de la carga de la prueba (artículo 18.1).

La situación del riesgo no es un concepto fáctico, sino un concepto técnico-jurídico que debe interpretarse con normas jurídicas que expresan una valoración[176]. La finalidad que subyace de este artículo 7 es tuitiva respecto al asegurado, ya que el mismo responde claramente a un interés de protección del asegurado.

Las normas que determinan la localización del riesgo se encuentran en los artículos 13 y 14 de la Directiva 2009/138/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre el seguro de vida, el acceso a la actividad de

[175] *Vid.* De Lima Pinheiro, L., "Sobre a lei aplicável ao contrato de seguro perante o Regulamento Roma I", *Cuadernos de Derecho Transnacional*, vol. 4, n. 2, Área de Derecho Internacional Privado, UC3M, Madrid, 2012, p. 204.

[176] *Vid. Op. Supra*, p. 291.

seguro y de reaseguro y su ejercicio (Solvencia II), remitidos por el artículo 7.6 del Reglamento "Roma II":

a. Si se trata de un seguro de vida, el riesgo se localiza en el país de compromiso, que se define como el país de residencia habitual del tomador (artículo 14).

b. En caso de seguros distinto al de vida, podemos encontrar cuatro reglas diferentes del tipo de seguro:

   - Si se trata de un seguro relativo a bienes inmuebles y su contenido, siempre que se encuentren cubiertos por la misma póliza de seguro, se considerará localizado en el Estado en el que estén sitos los bienes.

   - Si se trata de un seguro relativo a vehículos, el riesgo se considerará el Estado de matriculación del vehículo.

   - Si se trata de un seguro de duración igual o inferior a cuatro meses, que cubra riesgos sobrevenidos durante un viaje o vacaciones, el riesgo se situará en el Estado donde se suscribió la póliza.

   - Si se trata de un seguro no enmarcable en los anteriores, el riesgo se situará en el Estado en el que resida el tomador.

El artículo 7.3. I regula un conjunto de normas de manera alternativa que las partes pueden elegir, existiendo así una "autonomía de la voluntad limitada":

a. La ley del Estado miembro en que se localice el riesgo en el momento del contrato (artículo 7.3.1.a). Para localizar el riesgo, aplicamos la remisión del 7.6. Se debe atender a la localización del riesgo en el momento de celebración del contrato, por lo que un cambio posterior de la localización del riesgo no permite modificar la ley elegida.

b. La ley del país donde el tomador del seguro tenga su residencia habitual (artículo 7.3.1.b). Al referirse de forma genérica a la ley del país de la residencia del tomador, puede ser la de un tercer Estado (artículo 3). La residencia

habitual se determina mediante el artículo 19; y aunque no se concrete el artículo 7.3.1.b, sí se ha de tener en cuenta la residencia habitual del tomador en el momento de celebración del contrato, debemos considerar que sí por: 1) la analogía 7.3.1.a y 2) por el artículo 19.3., un cambio posterior de residencia no modificará la ley aplicable.

c. En el caso de un seguro de vida, la ley del Estado miembro del que sea nacional el tomador del seguro (artículo 7.3.1.c). Es necesario que el tomador posea la nacionalidad de algún Estado miembro. Un cambio de nacionalidad no conllevaría a un cambio de la ley aplicable.

d. Por lo que respecta a los contratos de seguro que cubran riesgos limitados a siniestros que ocurran en un Estado miembro distinto del Estado miembro en que se sitúe el riesgo, la ley de dicho Estado miembro (artículo 7.3.1.d).

e. Cuando el tomador de un contrato de seguro cubierto por el presente apartado ejerza una actividad comercial o industrial o una profesión liberal y el contrato de seguro cubra dos o más riesgos que estén relacionados con dichas actividades y estén situados en Estados miembros diferentes, la ley de cualquiera de los Estados miembros en cuestión o la ley del país en el que el tomador del seguro tenga su residencia habitual (artículo 7.3.1.e).

El artículo 7.3. del Reglamento "Roma II" admite un reenvío que opera en caso de que la ley a la que remiten las letras a), b) o e) conceda una mayor autonomía conflictual. Para que opere, deben darse las siguientes condiciones[177]:

- La norma de conflicto de la ley a la que remiten las letras a), b) o e) ha de permitir la elección de otras leyes.

- El reenvío solo se aplica a los supuestos de las letras a), b) o e).

- La ley a la que remiten debe ser de un Estado miembro.

[177] *Vid.* Carrascosa González, J. y Calvo Caravaca, A.-L. (dirs.), *Derecho*..., *op. cit.,* p. 1080.

En defecto de ley aplicable, el artículo 7.3.III, el contrato se regirá por la ley del Estado miembro donde esté localizado el riesgo. Para ello, volvemos a hacer mención la remisión del artículo 7.6. Cabe decir que nuestra LCS dispone de un régimen propio de ley aplicable cuando no sea posible determinar la ley aplicable mediante instrumentos institucionales o convencionales en los artículos 107 y 108 de la LCS. El primero trata sobre la ley aplicable a los contratos de seguro de daños. Se aplicará la ley española cuando:

a. Se refiera a riesgos que estén localizados en territorio español y el tomador del seguro tenga en él su residencia habitual, si se trata de persona física, o su domicilio social o sede de gestión administrativa y dirección de los negocios, si se trata de persona jurídica.

b. El contrato se concluya en cumplimiento de una obligación de asegurarse impuesta por la ley española.

Fuera de los casos anteriores, regirán las siguientes normas para determinar la ley aplicable al contrato de seguro contra daños:

a. Cuando se refiera a riesgos que estén localizados en territorio español y el tomador del seguro no tenga en él su residencia habitual, domicilio social o sede de gestión administrativa y dirección de los negocios, las partes podrán elegir entre la aplicación de la ley española o la ley del Estado en que el tomador del seguro tenga dicha residencia, domicilio social o dirección efectiva.

b. Cuando el tomador del seguro sea un empresario o un profesional y el contrato cubra riesgos relativos a sus actividades realizadas en distintos Estados del Espacio Económico Europeo, las partes podrán elegir entre la ley de cualquiera de los Estados en que los riesgos estén localizados o la de aquel en que el tomador tenga su residencia, domicilio social o sede de gestión administrativa y dirección de sus negocios.

c. Cuando la garantía de los riesgos que estén localizados en territorio español se limite a los siniestros que puedan ocurrir en un Estado miembro del

Espacio Económico Europeo distinto de España, las partes pueden elegir la ley de dicho Estado.

En cuanto a la localización del riesgo, el artículo 107.4 nos remite al artículo 1.3 d de la Ley de Ordenación y Supervisión de los Seguros Privados.

La ley debe pactarse en el contrato; a falta de elección, se regirá por la ley del Estado que presente un vínculo más estrecho en función de los supuestos del párrafo 3.

En relación con los seguros de vida, la ley aplicable se regula por el artículo 108 de la LCS, la cual se aplicará cuando:

a. El tomador del seguro sea una persona física y tenga su domicilio o su residencia habitual en territorio español. No obstante, si es nacional de otro Estado miembro del Espacio Económico Europeo distinto de España, podrá acordar con el asegurador aplicar la ley de su nacionalidad.

b. El tomador del seguro sea una persona jurídica y tenga su domicilio, su efectiva administración y dirección o su principal establecimiento o explotación en territorio español.

c. Cuando el tomador del seguro sea una persona física de nacionalidad española con residencia habitual en otro Estado y así lo acuerde con el asegurador.

d. Cuando el contrato de seguro de grupo se celebre en cumplimiento o como consecuencia de un contrato de trabajo sometido a la ley española.

CONCLUSIONES

PRIMERA. El reto normativo que suponen las nuevas tecnologías es mayúsculo en relación con los riesgos existentes para los actores intervinientes. La incertidumbre en la regulación de las tecnologías emergentes se presenta tanto como una oportunidad con el fin de proporcionar seguridad jurídica y un marco normativo adecuado a su desarrollo, como una amenaza respecto a una regulación restrictiva o tardía que neutralice el impacto positivo de las tecnologías emergentes; por ello, el modelo regulatorio debe centrarse en la autorregulación basado en un marco legal proporcionado por el legislador.

SEGUNDA. En esta última década, el sector asegurador está sufriendo cambios por las tecnologías emergentes, creando una industria aseguradora tecnológica conocida como *insurtech*. La revolución tecnológica ha llevado a reformular los pilares de negocio fundamentales y su cadena de valor, transformando las relaciones existentes tanto vertical como horizontalmente. Es la inteligencia artificial, como última tecnología disruptiva, la que amenaza con una readaptación empresarial y jurídica que impacta directamente a todos los sujetos de la cadena de valor. La existencia de importantes incertidumbres por los operadores económicos a la hora de afrontarlos en el contexto asegurador implica transformar la manera en la que se gestionan las obligaciones y responsabilidades legales. En la actualidad, la aparición de la IA no debe implicar de por sí una reordenación de los principios legales y marco normativo existente. Los principios de la gestión de riesgos a la hora de la determinación de la responsabilidad existen en otros sectores económicos, por lo que deberán establecerse estos mismos principios a los riesgos generados por la aplicación de una tecnología que implica a un gran número de actores.

TERCERA. La gestión de riesgos y cumplimiento derivada del uso de la IA debe entenderse siempre dentro del marco establecido por Solvencia II y su normativa de desarrollo. Solvencia II hace partir de una base madura y consolidada un modelo de control y gestión interna con potencial para adaptarse a los nuevos retos normativos sin perder el control necesario y exigido por la legislación.

CUARTA. Con el fin de demostrar la adecuada diligencia debida y proceso de gestión de riesgos, se ha propuesto un modelo basado en las evaluaciones de impacto de varios sectores que sirva como herramienta de gestión para demostrar una responsabilidad proactiva ante los órganos de control existentes, que cumplan con los futuros marcos legales actualmente en desarrollo.

QUINTA. La IA tiene un marcado componente de externalización y multilocalización que obliga a (re)pensar si los instrumentos de resolución de conflictos presentados por el Derecho internacional privado pueden hacer frente al reto que presenta la IA en las relaciones jurídicas. Si bien existen afecciones multidisciplinares como la concurrencia de regulación en materia de protección de datos y sector asegurador, no implica esto una necesidad de reformulación de los principios para poder atajar con contundencia los retos que la tecnología presenta, puesto que el *expertise* obtenido por la resolución de controversias en relación con otras tecnologías permite afrontar los conflictos con cierto conocimiento de causa. Dichas relaciones privadas internacionales, es decir, aquellas que contienen un elemento extranjero, presentan mayor complejidad ya que en estas relaciones se cruzan distintos ordenamientos jurídicos, y es ahí donde entra en juego el Derecho internacional privado con el objetivo de aportar soluciones a las relaciones jurídicas que surgen en el ámbito transfronterizo, con principales cuestiones jurídicas a resolver como es la competencia judicial internacional y la determinación de la ley aplicable.

BIBLIOGRAFÍA

AEPD. *Adecuación al RGPD de tratamientos que incorporan inteligencia artificial. Una introducción.*

Aguilar Grieder, H.: "Alcance de la regulación europea relativa a la competencia judicial internacional en materia civil y mercantil en el marco del nuevo Reglamento "Bruselas I Bis" (1215/2012): una apuesta parcialmente frustrada", *Revista Aranzadi doctrinal*, n. 9, Aranzadi, Cizur Menor, 2015.

Aguilar Grieder, H.: "Problemas de Derecho internacional privado en la contratación de seguros: especial referencia a la reciente Directiva (UE) 2016/97 sobre la distribución de seguros", *Cuadernos de Derecho Transnacional*, vol. 9, n. 2, Área de Derecho Internacional Privado, UC3M, Madrid, 2017.

Álvarez Hernando, J. y Cazurro Barahona, V.: *Practicum Protección de datos 2016,* Aranzadi, Cizur Menor, 2015.

Álvarez Lata, N.: *Cláusulas restrictivas de responsabilidad civil*, Comares, Granada, 1998.

ASCOM, *Libro blanco de la función de compliance*, Madrid, 2017.

ASCOM, *Manual de estudio para la certificación CESCOM,* Madrid, 2018.

Baena Álvarez de Quevedo, F. J., "Solvencia II y gestión del riesgo tecnológico en las compañías de seguros", *CSTIC 2012*, 18 de septiembre de 2012.

Banks, T. y Banks, F. (coords.), *Corporate Legal Compliance Handbook,* Wolters Kluwer, New York, 2020.

Beltrán Aguirre, J. L.: "La protección de los datos personales relacionados con la salud", en *Jornada sobre Protección de Datos Personales,* Defensor del Pueblo de Navarra-INAP, Navarra, 2012.

Brkan, M.: "Data protection and conflict-of-laws: a challenging relationship", *European Data Protection Law Review*, vol. 2, n. 3, 2016.

Brkan, M.: "Data Protection and European Private International Law", *Robert Schuman Centre for Advanced Studies,* Research Paper No. RSCAS 2015/40, jul. 2015.

Busto Lago, J. M.: "La responsabilidad civil de los servidores y operadores de datos", en *Seminario sobre Protección de Datos*, UCLM, Ciudad Real, 2005.

Buttarelli, G.: *Banche dati e tutela della riservatezza (La privacy nella Società dell'Informazione)*, Giuffrè Editore, Milán, 1997.

Buyya, R., *Big Data: Principles and Paradigms,* Morgan Kaufmann*,* 2016.

Carrascosa González, J. y Calvo Caravaca, A. L. (dirs.), *Derecho internacional privado*, vol. II, 16.ª ed., Comares, Granada, 2016.

Casanova, A., *Autonomía e independencia en* compliance, ASCOM, Madrid, 2019.

Ceballos, D., "Una propuesta de indicador de riesgo legal", *2.ª Reunión de Investigación en Seguros y Gestión de Riesgos,* Castro Urdiales (Cantabria), abril de 2007.

Chatzara, V. "FinTech, InsurTech, and the Regulators", en Marano, P. y Noussia, K. (eds.), *InsurTech: A Legal and Regulatory View,* Springer, Cham, 2019.

Chen, S., "Multinational Corporate Power, Influence and Responsability in Global Supply Chains", *Journal of Business Ethics,* n. 148, 2018.

Comisión Europea, *Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza,* COM (2020) 65 final, 2020.

Comité de Supervisión Bancaria de Basilea, *Basilea III: finalización de las reformas poscrisis*, 2017.

De Lima Pinheiro, L.: "Sobre a lei aplicável ao contrato de seguro perante o Regulamento Roma I", *Cuadernos de Derecho Transnacional,* vol. 4, n. 2, Área de Derecho Internacional Privado, UC3M, Madrid, 2012.

De Miguel Asensio, P. A., "*Smart contracts, blockchain,* derechos de autor y Derecho internacional privado", disponible en: https://pedrodemiguelasensio.blogspot.com/2019/06/smart-contracts-blockchain-derechos-de.html (fecha de consulta: 4-10-2021).

De Miguel Asensio, P. A.: "Aspectos internacionales de la protección de datos: las sentencias Schrems y Weltimmo del Tribunal de Justicia", *La Ley Unión Europea,* La Ley, Madrid, n. 31, 2015.

De Miguel Asensio, P. A.: "La contradictoria doctrina del Tribunal Supremo acerca del responsable del tratamiento de datos por el buscador Google", *Diario La Ley,* n. 8773, La Ley, Madrid, 2016.

De Miguel Asensio, P. A.: "Competencia y Derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea", *Revista Española de Derecho Internacional,* vol. 69, n. 1, Madrid, 2017.

Deloitte, *El impacto de la digitalización en España*. *Contribución de las empresas DigitalES a la economía española,* informe ejecutivo, 2019.

Díaz González, G. M. (coord.), *La regulación de los algoritmos*, Thomson Reuters Aranzadi, Madrid, 2020.

EIOPA, *Artificial Intelligence Governance Principles: Towards Ethical and Trustworthy Artificial Intelligence in The European Insurance Sector*, 2021.

Escorial, Á. *et. al. Guía para la aplicación de UNE-ISO 31000:2018*, AENOR ediciones, Madrid, 2018.

Fuentes, O. (dir.), *Era digital, sociedad y derecho,* Tirant lo Blanch, Valencia, 2020.

Garcimartín, F. (coord.), *Estudio sobre los sistemas de registro, compensación y liquidación de valores en Iberoamérica,* CNMV, Madrid, 2012.

Gil González, E., *Big Data, privacidad y protección de datos,* AEPD, Madrid, 2015.

Goergen, M., *International Corporate Governance,* Prentice Hall, 2012.

Gonzalo Domenech, J. J., "Algunas cuestiones relevantes de Derecho internacional privado del Reglamento General de Protección de Datos", *Revista Boliviana de Derecho*, n. 26, 2018.

Guasch Portas, V.: *Las transferencias internacionales de datos en la normativa española y comunitaria,* AEPD, Madrid, 2014.

IBM Institute for Business Value, *La evolución de la automatización de procesos*. Informe ejecutivo, 2018.

ICO y Alan Turing Institute, *Project explAIn Interim report,* informe ejecutivo, 2019.

IIA, *El modelo de las tres líneas del IIA 2020. Una actualización de las tres líneas de defensa,* IIA, 2020.

Kaplan, S. y Garrick, B. J., *On the Quantitative Definition of Risk. Risk Analysis. An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants,* US Nuclear Regulatory Commission, Washington D. C, 1975.

Kishnani, P., Turley, M., y Eggers, M., *El futuro de la regulación. Principios para regular tecnologías emergentes,* Deloitte Insights, Londres, 2018.

Lesmes Serrano, C. (coord.), *La ley de protección de datos. Análisis y comentario de su jurisprudencia,* Lex Nova, Valladolid, 2008.

López Álvarez, L. F.: *Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo,* Francis Lefebvre, Madrid, 2016.

Martínez Estay, J. I., Los conceptos jurídicos indeterminados en el lenguaje constitucional, *Revista de Derecho Político*, n. 105, 2019.

Mays. E. (ed.), *Handbook of Credit Scoring,* Glenlake, Chicago, 2001.

McKinsey & Company, *Insurance 2030 - The impact of AI on the future of insurance.* Informe ejecutivo, 2018.

Mendoza, I. y Bygrave, L., "The Right not to be Subject to Automated Decisions based on Profiling", *University of Oslo Faculty of Law Research Paper No. 2017-20*, 2017.

Muñoz Paredes, M. L. *Algoritmos y seguro: la fijación de la prima atendiendo a factores ajenos al riesgo,* Almacén de Derecho, Madrid, 2020.

Navas, S., "Sistemas expertos basados en inteligencia artificial y responsabilidad civil", *Diario La Ley,* 2020.

NIST Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations. A System Life Cycle Approach for Security and Privacy*. Rev. 2, 2018.

OCDE, *Technology and innovation in the insurance sector*, 2017.

Orejudo Prieto de los Mozos, P., "La vulneración de los derechos de la personalidad en la jurisprudencia del tribunal de justicia", *La Ley Unión Europea,* n. 4, 2013.

Ortega Giménez, A., "Imagen y circulación internacional de datos", *Revista Boliviana de Derecho,* n. 15, Fundación Iuris Tantum, Santa Cruz (Bolivia), 2013.

Ortega Giménez, A., "La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita en Derecho internacional privado español", *Diario La Ley,* n. 8661, La Ley, Madrid, 2015.

Ortega Giménez, A., "Propuestas ante un futuro incierto para la protección en la Unión Europea del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita: ¿unificación de la norma de conflicto vs. armonización a través de unos principios comunes?", *Revista Aranzadi Unión Europea,* n. 10, Aranzadi, Cizur Menor, 2016.

Ortega Giménez, A., *El nuevo régimen jurídico de la Unión Europea para las empresas en materia de protección de datos de carácter personal,* Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2017.

Ortega Giménez, A., *Transferencias internacionales de datos de carácter personal ilícitas,* Aranzadi, Cizur Menor, 2017.

Ortega Giménez, A., "El Reglamento General de Protección de Datos de la UE en la empresa: novedades prácticas", *Diario La Ley,* n. 15, sección Ciberderecho, 7 de marzo de 2018, Editorial Wolters Kluwer.

Ortega Giménez, A., *La aplicación del Big Data en el ámbito asegurador y el tratamiento legal de sus datos. Una perspectiva desde el derecho internacional privado*, Cuadernos de la Fundación, C/229, Fundación MAPFRE, Madrid, 2019.

Pérez Pérez, J. (coord.), *Gestión de riesgos en entidades aseguradoras. Solvencia II y su impacto regulatorio,* Delta Publicaciones, Madrid, 2016.

Pinar Mañas, J. L. (dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad,* editorial Reus, Madrid, 2016.

PWC, *Sizing the prize. What is the real value of AI for your business and how can you capitalize*. Informe ejecutivo, 2017.

Qiang, L., *et al*., "A Survey on Security Threats and Defensive Techniques of Machine", *IEEE Access*, 2018.

Recio Gayo, Miguel, "Acerca de la evolución de la figura del encargado del tratamiento", *Revista de Privacidad y Derecho Digital,* n. 0, 2015.

Rodríguez-Prado, J. M., "Los seguros gamificados de vida y salud. *Insurance telematics* (tendencias actuales y oportunidades en seguros de personas)", *Revista Española de Seguros: publicación doctrinal de derecho y economía de los seguros privados,* n. 167, SEAIDA, Madrid, 2016.

Sánchez Bravo, A. (ed.), *Derechos humanos y protección de datos personales en el siglo XXI. Homenaje a Cinta Castillo Jiménez,* Punto Rojo Libros, Sevilla.

Soares, S., *Big Data Governance. An Emerging Imperative,* MC Press, Boise (ID), 2012.

Troncoso Reigada, A. (dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas, Madrid, 2010.

Tschider, C., "Regulating the Internet of Things: discrimination, Privacy, and Cybersecurity in the Artificial Intelligence age", *Denver Law Review,* vol. 96, n. 1.

Tweneboah-Koduah, S., "Cyber Security Threats to IoT Applications and Service Domains", *Wireless Personal Communications,* 2017.

William, J., "Heart—A Proposed Method for Achieving High Reliability in Process Operation by Means of Human Factors Engineering Technology", *Safety and Reliability*, vol. 3, n. 35, 2015.

Wolfensohn, J., "The critical study of corporate governance provisions in India", *Financial Times,* 25, 4, 1999.

Wright, D., y De Hert, P. (eds.), *Privacy Impact Assessment,* Springer, Londres, 2012.

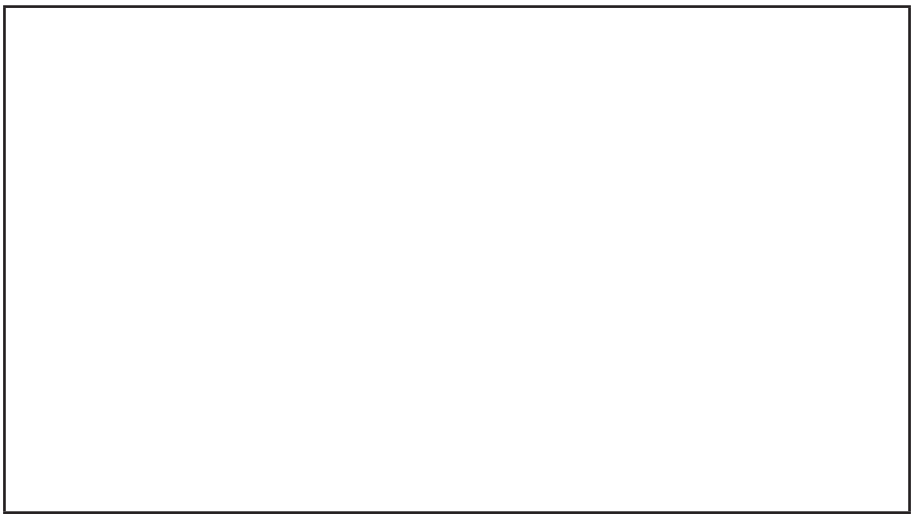
Zabihollah, R., *Financial Statement Fraud,* John Wiley & Sons, Sussex, 2002.

ANEXO. PLANTILLA DOCUMENTAL PARA LA REALIZACIÓN DE LA EVALUACIÓN DE IMPACTO DEL SISTEMA DE IA

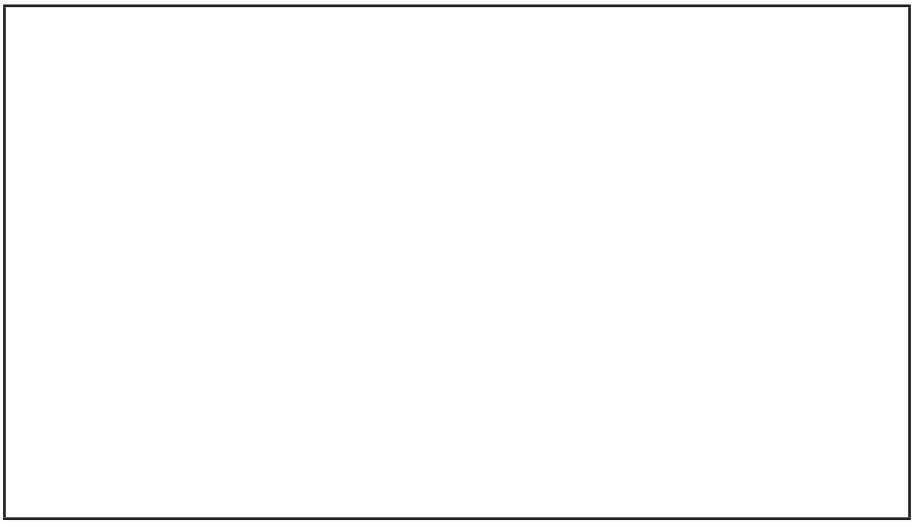
1. Descripción de las finalidades de tratamiento de los datos y del proceso de tratamiento de datos

2. Justificación positiva o negativa sobre la consideración del sistema de IA como "alto riesgo"

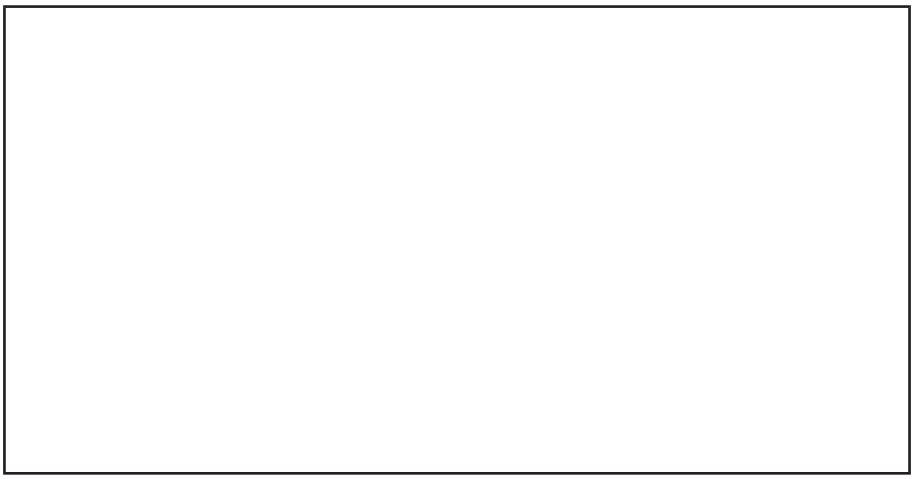
3. Descripción y desarrollo de los sistemas de información que soportan el servicio de IA



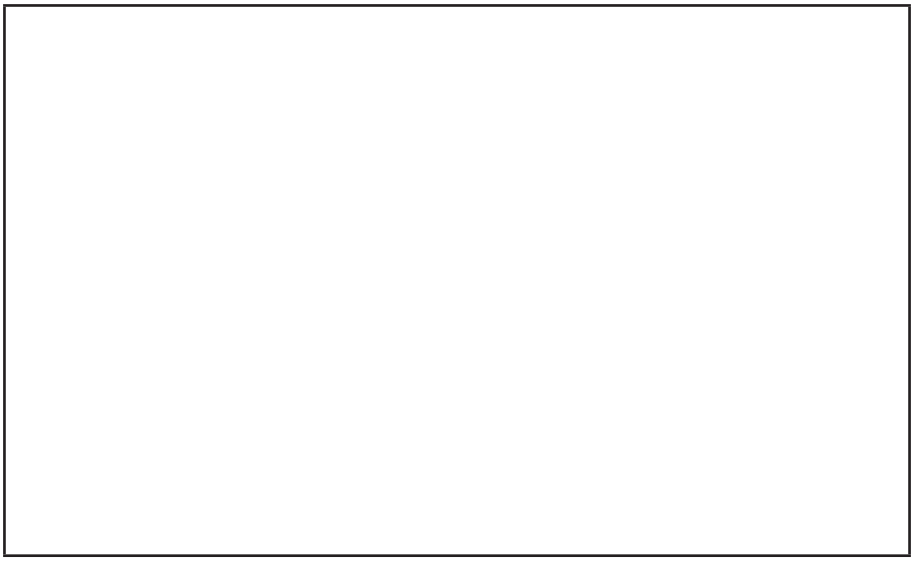
4. Descripción de los diferentes roles y responsabilidades que han intervenido en el desarrollo del sistema IA



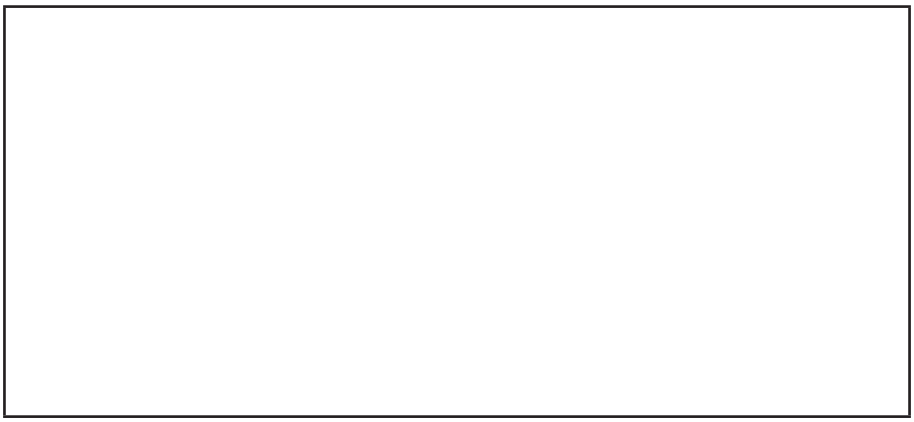
5. Resultado del análisis de riesgos de seguridad de la información del sistema de IA y las medidas que mitigan el riesgo



6. Resultado del análisis de riesgos de cumplimiento y las medidas que mitigan el riesgo



7. Registro de pruebas realizadas sobre el sistema, conclusiones sobre estas y medidas impuestas en caso de resultados no satisfactorios



CENTRO DE DOCUMENTACIÓN

Todas nuestras publicaciones a tu alcance

Además del acceso gratuito a nuestro fondo documental especializado en:

- Seguros
- Gerencia de riesgos
- Prevención

Fundación **MAPFRE**

Centro de Documentación

documentacion.fundacionmapfre.org

Fundación **MAPFRE**

23/C

Paseo de Recoletos, 23
28004 Madrid (España)
www.fundacionmapfre.org

P.V.P.: 20 €
ISBN 978-84-9844-758-3