

ABEL B. VEIGA COPO

SEGURO E INTELIGENCIA ARTIFICIAL

EL IMPACTO DE LA DIGITALIZACIÓN
EN EL CONTRATO DE SEGURO

III CIVITAS

© Abel B. Veiga Copo, 2025
© ARANZADI LA LEY, S.A.U.

ARANZADI LA LEY, S.A.U.

C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
www.aranzadilaley.es

Atención al cliente: <https://areacliente.aranzadilaley.es/>

Primera edición: Mayo 2025

Depósito Legal: M-10454-2025

ISBN versión impresa: 978-84-1085-107-8

ISBN versión electrónica: 978-84-1085-108-5

Diseño, Preimpresión e Impresión: ARANZADI LA LEY, S.A.U.

Printed in Spain

© ARANZADI LA LEY, S.A.U. Todos los derechos reservados. A los efectos del art. 32 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba la Ley de Propiedad Intelectual, ARANZADI LA LEY, S.A.U., se opone expresamente a cualquier utilización del contenido de esta publicación sin su expresa autorización, lo cual incluye especialmente cualquier reproducción, modificación, registro, copia, explotación, distribución, comunicación, transmisión, envío, reutilización, publicación, tratamiento o cualquier otra utilización total o parcial en cualquier modo, medio o formato de esta publicación.

Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la Ley. Diríjase a **Cedro** (Centro Español de Derechos Reprográficos, www.cedro.org) si necesita fotocopiar o escanear algún fragmento de esta obra.

El editor y los autores no asumirán ningún tipo de responsabilidad que pueda derivarse frente a terceros como consecuencia de la utilización total o parcial de cualquier modo y en cualquier medio o formato de esta publicación (reproducción, modificación, registro, copia, explotación, distribución, comunicación pública, transformación, publicación, reutilización, etc.) que no haya sido expresa y previamente autorizada.

El editor y los autores no aceptarán responsabilidades por las posibles consecuencias ocasionadas a las personas naturales o jurídicas que actúen o dejen de actuar como resultado de alguna información contenida en esta publicación.

ARANZADI LA LEY no será responsable de las opiniones vertidas por los autores de los contenidos, así como en foros, chats, u cualesquiera otras herramientas de participación. Igualmente, ARANZADI LA LEY se exime de las posibles vulneraciones de derechos de propiedad intelectual y que sean imputables a dichos autores.

ARANZADI LA LEY queda eximida de cualquier responsabilidad por los daños y perjuicios de toda naturaleza que puedan deberse a la falta de veracidad, exactitud, exhaustividad y/o actualidad de los contenidos transmitidos, difundidos, almacenados, puestos a disposición o recibidos, obtenidos o a los que se haya accedido a través de sus PRODUCTOS. Ni tampoco por los Contenidos prestados u ofertados por terceras personas o entidades.

ARANZADI LA LEY se reserva el derecho de eliminación de aquellos contenidos que resulten inveraces, inexactos y contrarios a la ley, la moral, el orden público y las buenas costumbres.

Nota de la Editorial: El texto de las resoluciones judiciales contenido en las publicaciones y productos de ARANZADI LA LEY, S.A.U., es suministrado por el Centro de Documentación Judicial del Consejo General del Poder Judicial (Cendoj), excepto aquellas que puntualmente nos han sido proporcionadas por parte de los gabinetes de comunicación de los órganos judiciales colegiados. El Cendoj es el único organismo legalmente facultado para la recopilación de dichas resoluciones. El tratamiento de los datos de carácter personal contenidos en dichas resoluciones es realizado directamente por el citado organismo, desde julio de 2003, con sus propios criterios en cumplimiento de la normativa vigente sobre el particular, siendo por tanto de su exclusiva responsabilidad cualquier error o incidencia en esta materia.

ÍNDICE GENERAL

	<u>Página</u>
ABREVIATURAS	13
NOTA DE AUTOR	19
DISCURSO ENTREGA DEL X PREMIO INTERNACIONAL DE SE- GUROS JULIO CASTELO MATRÁN	23

PARTE PRIMERA

I	
INTRODUCCIÓN	29
II	
ENTRE LO DESBORDANTE Y LO ENUCLEADOR. EL HILAZÓN TECNOLÓGICO DONDE LA CENTRALIDAD ES EL DATO	109
III	
EL DATO Y LA DECISIÓN RACIONALIZADA POR EL PRISMA TECNOLÓGICO	117
IV	
UN DESIDERÁTUM REAL Y POSIBLE: LA TRANSPARENCIA ALGORÍTMICA. MÁS ALLÁ DE LA ETICIDAD	127
1. Una evolución sin fronteras cognoscibles, pero de momento solo incipiente	145
2. Derecho y tecnología. Seguro y disrupción	167

V

UNA IRRUPCIÓN IGNOTA, PERO EXPANSIVA	187
---	------------

VI

LA INADECUACIÓN DEL DERECHO POSITIVO	193
---	------------

VII

UN CAMBIO DE PARADIGMA IRREAL	209
--	------------

VIII

PERSONALIZACIÓN VERSUS DESINTERMEDIACIÓN. ¿MITO O REALIDAD? EL COSTE DE LA TRANSFORMACIÓN	219
--	------------

IX

LA MUERTE DEL CONTRATO TRADICIONAL O LA MERA SUPLANTACIÓN. ¿INCÓGNITA?	233
---	------------

X

LA ASIMETRÍA INFORMATIVA: LA DISTORSIÓN ENTRE LA SELECCIÓN ADVERSA Y EL RIESGO MORAL EN LA ERA DIGITAL	249
---	------------

XI

LA FUNCIÓN DEL SEGURO EN LA ERA DIGITAL Y DEL BIG DATA	273
---	------------

XII

ALEATORIEDAD Y TECNOLOGÍA. EL USO MASIVO DE LOS DATOS	301
--	------------

1. El uso masivo de datos. Una nueva redimensión del análisis de los riesgos	301
---	------------

2. El riesgo del <i>big data</i> hacia una optimización de las primas. ¿Discriminación encubierta y consentida?	329
2.1. <i>El sesgo discriminatorio. Jugando con datos sesgados o buscando una discriminación enmascarada</i> ⁹²	329
2.2. <i>La ecuación transparencia versus discriminación enmascarada</i>	358

PARTE SEGUNDA

I

SMART CONTRACT Y CONTRATO DE SEGURO	375
1. El complejo enroque de incrustar el <i>smart contract</i> en la arquitectura del derecho contractual	391
2. Mas allá de una forma o formalidad digital. El condicionado de una póliza de seguros	406
2.1. <i>El Smart contract no es una mera forma digital</i>	406
2.2. <i>Propuesta de seguro. Función de la póliza y Smart contract. El contenido documental</i>	423
2.3. <i>Las funciones de la póliza escrita. ¿Y lo digital?</i>	428
2.4. <i>El condicionado de una póliza y el Smart contract</i>	442
2.5. <i>La necesidad de ciertos controles. ¿Puede un Smart contract activar los mecanismos de control de los condicionados?</i>	457
3. ¿Tiene sentido el parámetro <i>ad solemnitatem/ad probationem</i> en la contratación inteligente? O ¿hasta dónde rigen las formalidades en la documentación del seguro que marca la LCS?	479
4. Negociación, consentimiento, complitud/incomplitud de la contratación inteligente y análisis económico del derecho	484
5. La contratación inteligente ¿erradicará la interpretación contractual y presumirá el cumplimiento de hablar claro en la contratación?	505
6. Los límites a la automatización. La ejecución del <i>Smart contract</i>. ¿queda hueco para la disputa?	519
7. <i>Smart contract</i> y el incumplimiento	528

II

INSURTERCH Y EL IMPACTO DE LAS NUEVAS TECNOLOGÍAS EN LA DISTRIBUCIÓN POSDIRECTIVA DE 2016	531
1. Clases de distribuidores	541
2. La distribución de seguros a través de las entidades aseguradoras	542
3. Los mediadores de seguro. Ámbito general	547
4. Los mediadores de seguros complementarios	550
5. El uso de sitios web u otras técnicas de comunicación por parte de los mediadores	551
5.1. <i>Los criterios que los mediadores emplean para la selección y comparación de productos de las distintas aseguradoras</i>	552
5.2. <i>Las entidades aseguradoras sobre las que se ofrecen productos y la relación contractual con el distribuidor</i>	553
5.3. <i>Si la relación con las entidades aseguradoras es o no remunerada y la naturaleza de la remuneración</i>	553
5.4. <i>Si el precio del seguro que figura al final del proceso está o no garantizado</i>	553
5.5. <i>La frecuencia con la que la información de los distribuidores es actualizada</i>	553
6. La mediación en el seguro	555
7. Los agentes de seguros	559
8. Los corredores de seguros	564
9. Operador banca-seguros	573
10. La gestión de las cantidades pertenecientes a primas y siniestros .	576
11. Distribuciones basadas en asesoramientos, en datos, en perfiles .	579

III

EL ASEGURAMIENTO DE LOS ROBOTS. HACIA UN SEGURO OBLIGATORIO DE RESPONSABILIDAD CIVIL POR LOS DAÑOS QUE CAUSE LA INTELIGENCIA ARTIFICIAL	605
1. Urge un concepto de robot, pero ¿es asegurado o tomador en un hipotético seguro de responsabilidad civil?	624
2. Hacia una responsabilidad civil polémica	633

Página

IV

SEGUROS Y RIESGOS CIBERNÉTICOS	647
1. Los propios riesgos tecnológicos. El entramado cibernético ...	647
2. La catástrofe cibernética y el ecosistema del ciberseguro	667
3. Uso del dato y adopción de decisiones racionales	684
4. La cobertura tradicional de un riesgo sin embargo disruptor. Viejos anclajes para riesgos diferenciables	691
 BIBLIOGRAFÍA	 719

Como de otra parte el olvido de ciertos datos, significativamente, por ejemplo, el haber sufrido en el pasado algunas dolencias y que, hoy, en las exigencias de los mercados financieros pueden conllevar a situaciones discriminatorias o abusivas absolutamente, piénsese, así, en el hecho de haber sufrido cáncer y su constancia en ficheros o datos de cara a la concesión de préstamos o de seguros vinculados o no a servicios financieros¹⁷⁰.

Sin duda el rumbo que la inteligencia artificial y el *big data* han tomado es claro, lo difícil es hoy anticipar, la dirección exacta y la mudanza de cambios contractuales, conductas, gestiones, prestaciones de servicios, etc., terminará adoptando¹⁷¹.

Otro ejemplo provino de los Estados Unidos, donde en noviembre de 2015, la asociación de reguladores estatales de seguros emitió su recomendación a todos sus miembros de prohibir la optimización de precios en una variedad de circunstancias. La asociación también recomendó que los reguladores estatales consideren la introducción de reglas que les darían acceso digital a los modelos de calificación de las aseguradoras. En lugar de que las aseguradoras estadounidenses presenten informes de calificación en cantidades cada vez más masivas de papel, los reguladores obtendrían la información de calificación requerida directamente desde los sistemas de las aseguradoras. Es un desarrollo que vale la pena ver.

[...] ¿Podría un enfoque similar transformar la posición ética de las aseguradoras? Si, como en el Reino Unido, se requiere que las aseguradoras demuestren integridad tanto a nivel individual como individual, ¿podría evaluarse su capacidad para hacerlo mediante un uso similar del análisis de voz impulsado por IA? ¿Se podría exigir a todos los altos ejecutivos que hablen sobre integridad y ética durante el tiempo suficiente para que el *software* evalúe si realmente lo dicen en serio, si realmente lo entienden o si realmente están haciendo algo al respecto?

Estos son tiempos emocionantes para los seguros. La suscripción, los siniestros y el marketing se están transformando, pero para tener éxito de verdad, los seguros también deben transformar la confianza que el público tiene en ellos. Hay una oportunidad real aquí, pero debe abordarse, no dejarse al azar».

169. Del derecho al anonimato o a la identidad numérica negativa nos habla, sobre todo, LATIL, *Le droit du numérique. Une approche par les risques*, 2.^a ed., Paris, 2024, p. 93, cuando señala: «La face négative de l'identité numérique consiste à pouvoir choisir la manière de se présenter à autrui. Comme cela a déjà souvent été souligné, l'informatique (hier) et le numérique (aujourd'hui) font naître un risque de dévoilement d'informations confidentielles ou personnelles».
170. Señala BEHRENDT, «Vergessenwerden im digitale Zeitalter», *BVDI*, 2020, pp. 1448 y ss., cómo el «derecho al olvido» plantea multitud de cuestiones, cuya clarificación por parte de los estudiosos del derecho se encuentra todavía en sus inicios. En su trabajo, el autor desarrolla la doctrina del «derecho al olvido» en (fundamentalmente) conformidad con la jurisprudencia de los tribunales superiores y arroja luz sobre el complejo de cuestiones que rodean la decisión de equilibrio, las opciones de acción y las obligaciones de los motores de búsqueda y los proveedores de contenidos. La determinación precisa del grado razonable y necesario de difusión que exige la teoría de las normas solo puede retirarse por razones epistémicas. Las decisiones suponen el reconocimiento fundamental de una obligación de distribuir digitalmente la información, incluso contra la voluntad del intermediario.
171. No más significativo puede ser el epígrafe y el título que al mismo da el magistral trabajo de JUNQUEIRA, *Tratamento de dados pessoais e discriminação algorítmica nos seguros*, São Paulo, 2020, cuando en p. 198 bajo el título «Inteligência artificial e tomada de decisão por algoritmos: o seguro em direção a uma autoestrada ou a um penhasco?», acepción que toma de la conferencia internacional *Computers, privacy and data protection* (CPDP

La clave o, una de las cuestiones esenciales, es delimitar cómo Insurtech puede no solo dinamizar la gestión y creación de productos asegurativos, cuanto ser paralelamente una vía para explicar cómo podría funcionar o introducir parámetros de actuación de más eficacia para las aseguradoras, las empresas y los consumidores.

Otra cuestión bien distinta es saber y perimetrar si las Insurtech que sí han o están procurando una mayor eficiencia al mundo asegurador y también a las aseguradoras, portan en cambio eficiencia a la seguridad de las organizaciones¹⁷².

En cierto sentido, la tecnología y la irrupción de empresas sumamente tecnologizadas ofrece una capacidad única en este momento de vehicular el tránsito de la eficiencia y beneficios en la información que han de tener y conocer los consumidores¹⁷³.

2017): Is *Big data* steering insurance towards a Cliff or a superhighway? <https://cpdp-conferences.net/cdpd2017.pdf>.

172. Sumamente críticos en este punto y cuestionando precisamente esta eficiencia fuera del mundo asegurador estrictamente, TALESH/CUNNINGHAM, «The technologization of insurance», *op. cit.*, p. 39, cómo a pesar del aumento de la cantidad de información a la que tienen acceso los compradores y vendedores en el contexto de los ciberseguros, la base de datos de *Big data* a la que hemos accedido y examinado revela que los datos son limitados y no siempre precisos o fiables. Para empezar, la calidad y las fuentes de las que se compila la información son limitadas y pintan una incompleta posición en lo atinente a la ciberseguridad de cualquier grupo en particular y del riesgo asociado. Esto se debe en gran medida a que la base de datos se basa en datos disponibles públicamente para crear conjuntos de grupos homólogos. Por lo tanto, hay eventos que la base de datos no registra. En otras palabras, el hecho de que la base de datos solo incluya unos pocos eventos cibernéticos en un grupo paritario específico no significa necesariamente que ese grupo paritario sea menos propenso a ciberataques. Más bien, podría significar que los ciberataques experimentados por las empresas de ese grupo no son generalmente públicos o no llegan a ser de dominio público a través de informes o demandas, o que los que compilan la base de datos simplemente no encontraron algunos de los incidentes. Debido a que el ciberseguro carece de una línea obligatoria estandarizada y/o centralizada de informes, ninguna fuente de información es completa, y fuentes dispares contienen diferentes tipos y cantidades de datos. Además, esta información puede ser especialmente selectiva y poco representativa de datos de pérdidas cibernéticas a la hora de fijar los precios de los seguros, excluyendo a propósito los incidentes de sus asegurados de las bases de datos de los registros públicos. El variado tipo y calidad de los datos utilizados por los proveedores de datos relacionados con los seguros es un problema importante. Muchas aseguradoras no comparten sus datos con los proveedores de *Big data* por miedo a perder una ventaja competitiva en el mercado.

173. Así, HAGAN, «*Big data*, Big Questions—Insurers and Advanced Data Analytics», FINTECH L. REP. NL 2, 2018, n.º 1, pp. 21 y ss., donde describe las diferentes y diversas interacciones entre el seguro y la tecnología. Así las cosas, Insurtech que abarca toda la cadena de valor del Seguro así como todas sus líneas de negocio y las *startups* están «reaching customers through new distribution mediums—addressing shifts in the way people communicate, access information and make decisions—while not disturbing traditional channels». Insurtech, NAT'L ASS'N INS. COMM'RS, https://content.naic.org/cipr_topics/topic_insurtech.htm <https://perma.cc/SRD3-ZA6X> (last updated Feb. 19, 2020).

Información y datos que eviten sesgos discriminatorios¹⁷⁴; pero que abran un pretil a nuevos modelos de seguros sobre una filosofía disruptora, la que se asienta bajo la suscripción o perfección continua o «en tiempo real» de cara a una óptima y proporcional gestión del riesgo y la fijación de precios basada en el riesgo que recompensa a las organizaciones por la mejora de la ciberseguridad por ejemplo¹⁷⁵.

Como bien se ha señalado, la toma de decisiones algorítmica presupone que los algoritmos se aplican a un mundo estático. Pero la toma de decisiones automatizada es un proceso dinámico. Los algoritmos intentan estimar alguna cualidad difícil de medir de un sujeto utilizando indicadores, y los sujetos a su vez cambian su comportamiento para engañar al sistema y obtener un mejor trato para sí mismos (o, en algunos casos, para protestar contra el sistema). Estos cambios de comportamiento pueden entonces impulsar al algoritmo a hacer correcciones. Los movimientos y contramovimientos crean una danza que tiene gran importancia para la imparcialidad y la eficiencia de un proceso de toma de decisiones¹⁷⁶.

En efecto, ¿es todo digital cuando hablamos de análisis de datos o es otra cosa?, ¿acaso no nos damos cuenta de que estamos asistiendo a un cambio abismal de modelos de negocio que influyen e impactan sin duda también en el espectro asegurador? Se reconduce voluntaria y omniscientemente todo a inteligencia artificial, pero probablemente no somos capaces de vislumbrar un concepto único, claro y sencillo, a la vez que omnicomprendivo.

Piénsese simplemente en lo que están suponiendo ahora mismo las plataformas de comercio electrónico que están ofreciendo y vendiendo productos de seguro con una divergencia total con la mediación o los cánones de distribución hasta ahora conocidos¹⁷⁷. O los canales paralelos que irrumpen a la hora de realizar ventas cruzadas y que, hasta cierto punto, desvirtúan los canales clásicos tanto del operador como de la lógica de la venta en sí mismo, ajena a la intención primaria de adquirir un seguro.

174. Sobre el valor de la transparencia de la técnica, *vid.*, in extenso, LATIL, *Le droit du numérique. Une approche par les risques*, 2.^a ed., pp., 69 y ss., quien nos recuerda en p. 70 cómo: «L'encadrement de l'utilisation des informations personnelles par les pouvoirs publics vise pour cela à accroître la confiance en l'État de droit».

175. Véase in extenso, TALESCH/CUNNINGHAM, *op. cit.*, p. 11 y ss.

176. Cfr., BAMBAUER/ZARSKY, «The Algorithm Game», *Notre Dame Law Review*, 2018, vol. 94, n.º 1, pp. 1 y ss., hablan precisamente de la discriminación en el juego algorítmico aduciendo p. 7: «In contrast to pooling, discrimination schemes do not treat all subjects the same. Discrimination schemes attempt to allocate resources based on the expected costs or value of the individuals. The goal for discrimination schemes is to allocate a resource based on an abstract and fundamentally unknowable quality of the subjects relating to their skill, risk, need, merit, or some other quality that is deemed appropriate to the relevant setting. We will call this quality the key characteristic.»

177. Obligada referencia a DÍAZ LLAVONA, «Plataformas», *op. cit.*, p. 88, quien nos advierte de estas plataformas: «se ven obligadas a adoptar las fórmulas clásicas de la distribución, pero lo hacen a efectos meramente formales, sin cumplimiento de los requisitos propios de cada figura, con los riesgos que esto comporta».

Lo mismo sucede cuando hablamos de identidad digital en contraposición tal vez a identidad personal cuando no son miméticas, por no decir, identificación. Incluso, identificación biométrica que en lo que respecta por ejemplo a la selección o antiselección de un riesgo asegurable, es esencial.

Los últimos años han visto como un nuevo y compuesto supraconcepto modernista, el de metaverso, da un paso más en esa gran envolvente que lo digital, lo tecnológico y lo cuántico amenaza —sentido figurado en su significado— por revolucionar definitivamente el seguro y el mercado financiero cuando no, por abrir espacios digitales de interacción a través de realidad aumentada donde interactuar social y económicamente¹⁷⁸. Término hoy en declive o desuso, no distando de ser una era burbuja interesada pero especulativa del que apenas se habla en 2025.

Mas ante este cliente digital disruptor y por generalizar, la digitalización del seguro y de la técnica asegurativa se ha introducido con intensidades disímiles en función de la diversidad de su universo de clientes, entre lo tradicional a lo más rupturista y digitalizado¹⁷⁹.

178. Campo este último donde los interrogantes no solo en el mercado de seguro sino sobre todo en los financieros empiezan a agudizarse, por ejemplo, ¿puede el metaverso convertirse en un canal de distribución y venta de productos asegurados?, ¿son susceptibles de aseguramiento todos y cada uno de los activos digitales que están irrumpiendo en esta vasta iconografía digital financiera? ¿será *blockchain* o cualquier otro registro suficiente para dar soporte y cabida a una ciberrealidad desbordante en estos momentos? En el artículo «El metaverso abre una puerta de infinitas posibilidades para las pymes» de 2 de diciembre de 2021, en CESCE, <https://www.cesce.es/es/w/asesores-de-pymes/metaverso-pymes>, se afirma: «En un entorno digital único pero inabarcable, el uso complementario de la realidad virtual con la realidad aumentada permitirá disfrutar de experiencias digitales completas, en las que se lograrán emociones más allá de lo conocido gracias a las nuevas tecnologías, pero en donde la economía digital jugará un rol fundamental. Por medio de ambientes virtuales pero que serán igual de interactivos que los reales, los usuarios podrán, por ejemplo, probarse una prenda de ropa o ver el tráiler de una película y, si así lo desean, adquirir el producto o el servicio y disfrutarlo. Algo que, en mayor o menor medida, ya facilitan muchos videojuegos *online* pero que abarcará por completo los cinco sentidos humanos a través del metaverso».

Por medio de entornos tridimensionales y en continua evolución, las posibilidades para las empresas son infinitas, casi como si de un nuevo mundo por construir se tratara, o, incluso, superiores. Esto es así porque no existe, en principio, ninguna limitación física ni económica, lo que significa, para una pyme con la tecnología adecuada, poder posicionarse en el mercado y competir desde cero con otras entidades de mayor tamaño y más consolidadas en la realidad «tradicional».

Todavía queda mucho por conocer en relación con la interacción real con la realidad virtual o de qué manera se podrán realizar transacciones económicas seguras en el metaverso, aunque es evidente que las monedas digitales jugarán un rol importante, lo que significará, a buen seguro, el impulso en el desarrollo de una legislación global que proteja principalmente a los compradores. «En todo caso, ya existen informes de distintas consultoras analizando las posibilidades para las empresas de participar en el metaverso en sectores como la salud, las finanzas o el ocio».

179. No en vano ha afirmado SINHA, «Insurance industry eyes *blockchain* as top firms begin tests», *Cointelegraph*, 24 de diciembre de 2019, <https://cointelegraph.com/news/insurance-industry-eyes-blockchain-as-top-firms-begin-tests>: «Blockchain technology is not a silver bullet, but rather a powerful new tool to drive data integrity, interoperability

A ello, únase, como el análisis avanzado de datos en tiempo real está creando toda una pléyade de nuevos productos casi de forma instantánea y ajustados *ad hoc* a las necesidades cambiantes o no de nuevos perfiles de consumidores y usuarios que interactúan a través de dispositivos electrónicos y redes sociales.

La atención o asesoramiento asistido tal y como hasta el presente lo hemos conocido en el mundo del seguro está cediendo frente a determinados tipos de clientes o potenciales asegurados especialmente conocedores de la tecnología y proclives a interactuar de otro modo, especialmente enfocado a sus necesidades, su conocimiento digital y el autoservicio. El enorme reto es buscar la hoja de ruta hacia ese estado digital donde el seguro se omnicanalice y siga siendo útil y accesible en otros formatos y con otros ropajes, pero sin perder la esencia y entidad intrínseca que el mismo cumple o ha de cumplir en el momento de enorme transformación digital que está ya presente.

Pero referenciar un discurso o un ensayo a lo tecnológico ha de hacerse desde un marco y, a la vez, una visión sumamente amplia y dinámica, además de transversal. Son múltiples las facetas, las aristas, las dimensiones a analizar y a abarcar. Incluso en un anclaje filosófico. Aunque empleemos indistintamente y como si fueren conceptos homónimos expresiones como tecnológico, digitalización, *big data*, inteligencia artificial, computación en la nube, etc., distan de ser, tanto por sus significados y significantes, miméticos¹⁸⁰.

Y en nuestro caso saber cómo impactan en el seguro. Pues esa interacción e intersección a la vez entre seguro y tecnología, entre *big data* e inteligencia artificial no admite ni puede admitir una vuelta atrás o regresión en el mercado del seguro¹⁸¹. Antes al contrario.

and traceability». Es decir: «La tecnología Blockchain no es una bala de plata, sino una herramienta nueva y poderosa para impulsar la integridad, la interoperabilidad y la trazabilidad de los datos. Con el aumento de los centros de almacenamiento de datos y la disminución de la confianza entre pacientes, hospitales y socios de la cadena de suministro, *blockchain* puede tener un impacto real en la industria del cuidado de la salud».

180. Advierte JUNQUEIRA, *Tratamento de dados pessoais*, *op. cit.*, p. 201, de la necesidad de diferenciar entre la vasta gama de elementos que componen la inteligencia artificial, entre algoritmos de análisis de datos —que realizan entrecruzamientos de datos estructurados en busca de patrones o correlaciones—, y algoritmos que componen sistema capaces de aprender «sozinhos» por aprendizaje de máquinas. Así, el *machine learning* es capaz de analizar, hacer correlaciones y buscar patrones a partir de datos no estructurados: fotos, vídeos, textos, datos adquiridos por smartphones y sensores.
181. Así, TALESH/CUNNINGHAM, «The technologization of insurance», *op. cit.*, p. 54, de modo rotundo adveran «Aunque la intersección de los seguros y la tecnología es problemática, nada de lo anterior sugiere que las aseguradoras cibernéticas no puedan desempeñar un papel significativo en la mejora de la postura de ciberseguridad de sus asegurados y, en última instancia, de la sociedad en su conjunto. Grandes datos, la IA y las nuevas tecnologías están revolucionando la prestación y la práctica de los seguros, y no hay vuelta atrás. A pesar de los desafíos sugerimos en esta parte que las insurtech pueden, en teoría, ser parte de la solución y pueden ayudar a aumentar la

En el riesgo, en la tarificación final de ese riesgo y coste del seguro, pero también en la función «social» que el seguro cumple o hasta el presente, de un modo u otro, ha venido cumpliendo¹⁸². Y no solo en la contratación¹⁸³. O en un modelo de negocio caduco y que necesariamente ha de *aggiornarse* ante ese avance disruptivo y en lo que no todo es, en puridad, inteligencia artificial. Hoy se comercializan y adquieren seguros donde antes simplemente era impensable, por ejemplo, en webs de entidades con un objeto disímil al del seguro y en apariencia sin afección ni vinculación de ningún tipo al mundo asegurador¹⁸⁴.

Sin lugar a duda, el reto inmediato de los próximos años será el saber adaptar el aterrizaje real de las empresas de Insurtech al mundo del seguro y al nuevo modelo de negocio que las mismas traen consigo y escrutar el verdadero valor añadido ínsito a esta irrupción y modelo. Un marco donde deslindar y aclarar el marco regulatorio y las reglas de juego jurídico-económicas es y será axial. Las empresas tecnológicas de seguro, son actores que desarrollan una actividad en un entorno regulatorio caduco y configurado bajo otros patrones, analógicos si se nos permite y que han de ser igualmente *aggiornados*.

No cabe duda de que el dato, que el empleo de algoritmos es un cauce de enorme potencialidad de cara a objetivar decisiones, baremar aspectos y conductas con impacto en un producto de seguro, en la siniestralidad, en el comportamiento, pero también en el diseño y la creatividad de productos, su oferta, etc. Mas ¿qué es un algoritmo y cómo impacta el mismo en el mundo del seguro?¹⁸⁵

Piénsese además en los datos que se utilizan en una identificación biométrica, en cómo se realizan las mediciones, las características físicas, el comportamiento de cada persona y sobre todo aquello que nos hace diferentes a otra persona. Téngase presente como la legislación comunitaria respecto

ciberseguridad de las organizaciones y la capacidad de las aseguradoras para desempeñar un papel regulador positivo».

182. Sobre la función social del seguro, véase nuestro ensayo, VEIGA, *Función social, jurídica y económica del seguro*, Madrid, 2022, especialmente capítulo segundo.

183. Clarividente sin duda el artículo de SNYDER, «A.I., Big data and the threat of proxy discrimination: a revolution in the U.S. insurance industry», 15 de abril de 2019, <https://www.jimsnyderlaw.com/blog/2019/4/15/ai-big-data-and-the-threat-of-proxy-discrimination-a-revolution-in-the-us-insurance-industry>.

184. Constata DÍAZ LLAVONA, *op. cit.*, p. 88, cómo el acceso a grandes carteras de clientes se convierte en un atractivo indudable para la generación de negocio, por lo que si antes este era el fuerte de las entidades bancarias cuando iniciaron su relación con la actividad de distribución de seguros, el atractivo ahora de la venta cruzada es mucho mayor, pues hablamos aquí de acceso a millones de clientes que ya son del sitio web de que se trate en virtud de relaciones jurídicas o comerciales distintas en mercados mucho más amplios.

185. Sobre el origen y significando de algoritmo y su intersección con el derecho, imprescindible el trabajo de HUERGO LORA, «Una aproximación a los algoritmos desde el derecho administrativo», *La regulación de los algoritmos* [HUERGO (Dir.)], Cizur Menor, 2020, pp. 23 y ss., sobre todo, pp. 26 a 30.

a la inteligencia artificial concibe el dato biométrico como datos personales resultantes de un tratamiento técnico especializado relacionado con las características físicas, fisiológicas o de comportamiento de una persona física, de tal modo que permiten o confirman la identificación única de esa persona física, como imágenes faciales o datos dactiloscópicos¹⁸⁶.

Un interrogante necesario a la vez que todo parece reducirse al dato como elemento principal y principal de una nueva era, la era del dato frente a la anterior actuaría intramuros el seguro. Interrogante que hemos de cerrar en una elipsis necesaria como veremos al hablar de la eticidad y auditación del algoritmo que no es otro que plantear cómo el poder algorítmico ha de rendir cuentas¹⁸⁷. Otra cuestión será delimitar si la transparencia o no de un algoritmo es la mejor de las opciones o simplemente una opción limitada a la hora de la verdad¹⁸⁸.

186. Hace ya más de una década, HEIMHALT/REHMANN, «Gesundheits- und Patienteninformation en via Apps», *MPR*, 2014, Heft 6, pp. 197 y ss., y más recientemente responde a este interrogante de cuando un *software* es un dispositivo médico, KLÜMPER, «Aus gegebenem Anlass: Wann ist eine *Software* ein Medizinprodukt?», *MPR*, 2024, Heft 6, pp. 240 y ss.

187. Este es uno de los ejes del trabajo de YEUNG/LODGE, *Algorithmic regulation. An introduction*, Oxford, 2019, y en el que los autores parten del hecho de que el poder y la sofisticación de los «grandes datos» y el análisis predictivo continúan expandiéndose, también lo han hecho las políticas y la preocupación pública sobre el uso de algoritmos en la vida contemporánea. Esto no es de extrañar dada nuestra creciente dependencia de los algoritmos en nuestra experiencia cotidiana, que afecta a sectores políticos que van desde la sanidad, el transporte, las finanzas, el comercio minorista, la fabricación, la educación, el empleo hasta la prestación de servicios públicos y el funcionamiento del sistema de justicia penal. Esto ha generado preocupaciones sobre la necesidad y la importancia de hacer que el poder algorítmico rinda cuentas, pero no está nada claro que los mecanismos legales y de supervisión existentes estén a la altura.

188. Sitúa precisamente el foco de la transparencia en su limitación CHANDER, «The racist algorithm?», *Michigan Law Review*, 2017, vol. 115, pp. 1023 y ss., p. 1040, cuando afirma cómo la transparencia de los propios algoritmos puede resultar una solución limitada. Afirmación que sustenta en cinco ideas, a saber:

En primer lugar, la transparencia invita a las manipulaciones por parte de quienes juegan con esos algoritmos. Google responde a quienes piden transparencia algorítmica que, aunque su algoritmo de clasificación de páginas se describe con todo detalle: «Si la gente que intenta jugar con los rankings de búsqueda conociera cada detalle de cómo clasificamos los sitios, sería más fácil para ellos discriminar aquellos resultados con páginas que no son relevantes y que resultan frustrantes para los usuarios, como la pornografía y el *malware*». Por otra parte, Cynthia Dwork y Deirdre Mulligan sostienen que «exponer los conjuntos de datos y los algoritmos del análisis de *Big data* puede mejorar la comprensión de los algoritmos, pero dada la complejidad independiente (a veces intencionada) de los algoritmos, no es razonable esperar que la transparencia por sí sola elimine el sesgo».

En segundo lugar, exigir la publicación del propio algoritmo puede poner en peligro los secretos comerciales.

Tercero, las personas pueden saber lo que hace el algoritmo y, sin embargo, no tener la opción de participar en él.

Cuarto, el algoritmo puede ser demasiado complicado para que muchos otros lo entiendan, o incluso si es comprensible, demasiado exigente, en términos de tiempo, para comprenderlo completamente.

El reto de la transformación digital con el uso de la automatización y la inteligencia artificial, los desafíos de la ciberseguridad¹⁸⁹, la robótica y su impacto en las actividades profesionales y decisionales, son y han sido, mas también serán, un foco de atención principal para el mundo del seguro en todos y cualesquier de sus campos de actuación y proyección¹⁹⁰. Pero también para el derecho, máxime, rescribiendo conceptos y basamentos, como el de, por ejemplo, otorgar o no personalidad jurídica a los agentes inteligentes, como los robots. El riesgo, evitara caer en una *slippery slope* o pendiente resbaladiza¹⁹¹. Qué duda cabe que ese desafío primigenio se centra

En quinto lugar, debido a que la discriminación puede surgir a través de los datos de entrenamiento u operacionales y no del propio algoritmo, revelar el algoritmo facialmente neutral puede ayudar a defender ese algoritmo de las acusaciones de discriminación.

Por último, en la era de los algoritmos que se mejoran a sí mismos, los diseñadores humanos de los algoritmos pueden no entender del todo su propia creación: incluso los ingenieros de Google pueden no entender ya lo que hacen algunos de sus algoritmos.

189. Vid., entre otros el trabajo «Cyber-Security: Praxishinweise aus Versicherungssicht», *WPg Die Wirtschaftsprüfung*, 2022, Heft 21, pp. 1233 y ss.

190. No más gráfico pueden ser las aseveraciones de ZARIFIS/MILNE/HOLLAND, «Evaluating the impact of AI on insurance: the four emerging AI- and data-driven business models», 2019, https://www.researchgate.net/publication/336575076_Evaluating_the_impact_of_AI_on_insurance_The_four_emerging_AI_and_data-driven_business_models, donde analizan cómo las crecientes capacidades de la inteligencia artificial (IA) están cambiando la forma en que las organizaciones operan e interactúan con los usuarios tanto interna como externamente. El sector de los seguros está utilizando actualmente la IA de varias maneras, pero su potencial para interrumpir los seguros no está claro. Esta investigación evalúa la implementación de la automatización dirigida por IA en 20 compañías de seguros. Los hallazgos indican que surgen cuatro modelos de negocios (BM): en el primer modelo, la aseguradora toma una parte más pequeña de la cadena de valor, lo que permite que otros con IA y datos superiores tomen una parte más grande. En el segundo modelo, la aseguradora mantiene el mismo modelo y cadena de valor pero utiliza IA para mejorar la efectividad. En el tercer modelo, la aseguradora adapta su modelo para utilizar completamente la IA y buscar nuevas fuentes de datos y clientes. Vid., además, HALL, «How artificial intelligence is changing the insurance industry for the future», 19 de marzo de 2020, <https://inmediatesg.medium.com/how-artificial-intelligence-is-changing-the-insurance-industry-for-the-future-20af0ba6e8d1>. Reconoce el autor cómo la IA no es un sistema perfecto, tiene fallas.

191. Nos advierte SCHIRMER, «Artificial Intelligence and legal personality: introducing “Teilrechtsfähigkeit”: a partial legal status made in Germany», *Regulating artificial intelligence* [WISCHMEYER/ RADEMACHER/ (Eds.)], Cham, 2020, pp. 123 y ss., p. 132, cómo: «Conceder personalidad jurídica a los agentes inteligentes probablemente acabaría en lo que yo llamo la “trampa de la humanización”: el estatus de persona jurídica indica una importante actualización normativa. La ley no solo trasladaría al centro de atención un hecho antes marginal, sino que también se dirigiría a los agentes inteligentes como actores independientes. Los agentes inteligentes se situarían al mismo nivel que otros sujetos jurídicos, acercándose mucho al representante más destacado: el ser humano. Y una vez que una entidad llega a este punto, la trampa se cierra. Se hace más difícil justificar por qué esta persona no debería disfrutar de los mismos derechos y privilegios que tienen las personas físicas. La experiencia en el tratamiento de las entidades corporativas es un buen ejemplo (y una advertencia): Muchos juristas alemanes afirman que las personas jurídicas son titulares del derecho general a la personalidad porque, como personas, deberían disfrutar de los mismos derechos que las demás personas. Asimismo, en Estados Unidos, una interpretación formalista de

en la creación misma del contrato, del producto de seguro, del condicionado, y la tutela al consumidor asegurado¹⁹².

No son pocos los dilemas a los que nos enfrentamos y que estamos obligados a resolver, pero también a regular¹⁹³. Entramos, ya lo hemos hecho en el análisis del riesgo, la prima y la gestión del siniestro, en el campo de la regulación algorítmica¹⁹⁴.

la palabra “persona” en la decimocuarta enmienda supuso la concesión a las corporaciones del derecho a la libertad de expresión. Esto ha tenido amplias consecuencias para el sistema legal y la sociedad en su conjunto. En otras palabras, al igual que con las entidades legales, sería difícil justificar por qué los agentes inteligentes, aunque sean reconocidos como personas bajo la ley, no deberían tener ciertos derechos como la protección de los trabajadores o incluso derechos constitucionales. Para ser claros, no estoy diciendo que los agentes inteligentes no deban disfrutar de estos derechos en absoluto. Solo creo que es importante determinar su capacidad de ser titulares de derechos para cada derecho en concreto. Sin embargo, al otorgar personalidad jurídica a los agentes inteligentes, el debate podría terminar antes de empezar».

192. Imprescindible la consulta al trabajo de hace un quinquenio de GREIS, *Auswirkungen der Digitalisierung auf Abschluss und Gestaltung privater Versicherungsverträge*, Berlin, 2020, sobre todo a partir del capítulo 3 pp. 155 y ss., donde se analiza con sumo rigor la problemática del objeto del contrato a raíz del diseño de productos digitales.

193. Interrelacionándolo con los algoritmos y los procedimientos y productos sanitarios y el software, afirma JABRI, «Artificial Intelligence and Healthcare: products and procedures», *Regulating artificial intelligence* [WISCHMEYER/ RADEMACHER/ (Eds.)], Cham, 2020, pp. 308 y ss., p. 309: «La creciente importancia de los programas informáticos en los dispositivos médicos va unida a un aumento de la complejidad. El desarrollo evoluciona desde el conocimiento basado en la experiencia del médico individual hasta la intervención basada en la evidencia utilizando la mejor evidencia científica externa disponible en la actualidad. Por lo tanto, **el creciente uso de software, especialmente la inteligencia artificial, conduce a una mayor necesidad de regulación: los algoritmos apoyan automáticamente las decisiones que antes estaban reservadas a los seres humanos y pueden influir significativamente en una decisión humana autodeterminada**. El aumento de la complejidad a menudo resulta de la falta de previsibilidad de la salida de los algoritmos de aprendizaje. Los algoritmos de aprendizaje se enfrentan a una gran variedad de estímulos ambientales y, en consecuencia, cambian su base de decisión y su estructura. Esto da lugar a una expansión continua del poder analítico y de la capacidad de aprendizaje y, por tanto, complica la eficacia de los controles preventivos de los algoritmos de aprendizaje. La protección integral de los ciudadanos frente a los riesgos y peligros que pueden derivarse del uso de productos técnico-médicos ha sido siempre una tarea tradicional del Estado, que posee también una dimensión constitucional. En consecuencia, el Estado se enfrenta ahora a la importante cuestión de cumplir su mandato de protección legal a pesar de la creciente complejidad del tema de la regulación».

194. Así, en un *paper* de la Facultad de Derecho del King's College de Londres de 23 de mayo de 2017, señala YEUNG, «Algorithmic regulation: a critical interrogation», 2017, *Paper n.º 2017-27*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972505, cómo: «Las innovaciones en las tecnologías de comunicación digital en red, incluido el auge de los “Big data”, la computación ubicua y los sistemas de almacenamiento en la nube, pueden estar dando lugar a un nuevo sistema de ordenamiento social conocido como regulación algorítmica. La regulación algorítmica se refiere a los sistemas de toma de decisiones que regulan un dominio de actividad con el fin de gestionar el riesgo o alterar el comportamiento a través de la generación computacional continua de conocimiento mediante la recopilación sistemática de datos (en tiempo real de forma continua) emitidos directamente desde numerosos componentes dinámicos pertenecientes al entorno

Una regulación que ha de vincularse con la cuantificación, la clasificación y evaluación que se produce, primero con la recopilación de información, segundo, con el establecimiento de normas y, finalmente a través de la intervención con la modificación de la conducta¹⁹⁵. Sin obviar el enorme problema de la eticidad y la responsabilidad algorítmica¹⁹⁶.

Pero también con los peligros o alertas inmanentes a esta misma revolución tecnológica, máxime en todo el riesgo que entraña y que puede sufrir y realizarse incluso desde lo cibernético o criptográfico¹⁹⁷. O, pensemos,

regulado con el fin de identificar y, si es necesario, refinar automáticamente (o refinar rápidamente) las operaciones del sistema para lograr una meta preespecificada. Proporciona un análisis descriptivo de la regulación algorítmica, clasificando estos sistemas de toma de decisiones como reactivos o preventivos, y ofrece una taxonomía que identifica 8 formas diferentes de regulación algorítmica en función de su configuración en cada una de las tres etapas del proceso cibernético: en particular, a nivel de establecimiento de estándares (estándares conductuales adaptativos versus fijos); recopilación y seguimiento de información (datos históricos vs. predicciones basadas en datos inferidos) ya nivel de sanción y cambio de comportamiento (ejecución automática vs sistemas de recomendación). Mapea los contornos de varios debates emergentes en torno a la regulación algorítmica, basándose en conocimientos de estudios de gobernanza regulatoria, críticas legales».

195. Sobre este reetiquetado de las funciones y a medio camino entre la regulación algorítmica y la gobernanza del algoritmo, nos remitimos al trabajo que cierra la trilogía de Yeung, así, *vid.*, ULBRICHT/YEUNG, «Algorithmic regulation: a maturing concept for investigating regulation of and through algorithms», *Regulation & Governance*, Agosto, 2021, https://www.researchgate.net/publication/354186345_Algorithmic_regulation_A_maturing_concept_for_investigating_regulation_of_and_through_algorithms.
196. Sobre la eficiencia y reducción de costes y aumento de agilidad que supone la IA sobre todo en su comparación con las decisiones tomadas por humanos, JUNQUEIRA, *Tratamento de dados pessoais e discriminação algorítmica nos seguros*, *op. cit.*, p. 202 y 203.
197. Así, y aunque se abordará *infra* más específicamente, el riesgo cibernético, en palabras de MALEK/SCHÜTZ, «Cybersversicherung: Rechtlinie und praktische Herausforderungen», *r+s*, 2019, Heft 8, pp. 421 y ss., p. 422, el evento asegurado es el daño patrimonial que haya sido establecido de manera verificable por primera vez y que haya sido causado por una *violación de la seguridad de la información*, Sección A1-2.2 AVB Cyber. Así lo entiende la AVB Cyber: «un menoscabo de la disponibilidad, integridad o confidencialidad de los datos electrónicos de las Naciones Unidas o de los sistemas de procesamiento de información utilizados por las Naciones Unidas en el ejercicio de sus actividades comerciales o profesionales».

Por tanto, la cobertura del seguro se basa en los denominados valores fundamentales de TI u objetivos de protección (confidencialidad, disponibilidad e integridad), que se utilizan en tecnologías de la información para garantizar un nivel mínimo de seguridad. El alcance de la cobertura del seguro depende, entre otras cosas, de la comprensión del concepto de *sistema de procesamiento de información*. Esto determina qué equipo (técnico) del asegurado está asegurado y es decisivo, por ejemplo, para determinar si: Por ejemplo, las máquinas de producción o los robots de fabricación o los dispositivos IoT («dispositivos inteligentes») también están incluidos en el alcance de cobertura. La AVB Cyber no define explícitamente qué se entiende por sistema de procesamiento de información. Hasta donde se puede ver, no es un término técnico en tecnología de la información. Sin embargo, la regulación del apartado A1-10 AVB Cyber habla a favor de una comprensión amplia del término. Como ejemplos de sistemas de procesamiento de información se mencionan servidores, sucursales de producción o ventas y almacenes. En base a ello, y teniendo en cuenta la finalidad perseguida por AVB Cyber (y

por ejemplo, ¿qué sucede o sucedería si alguien utilizase el aprendizaje automático y algoritmos secretos para la recopilación de datos públicos o privados de los clientes asegurados o todavía potenciales solicitantes de un seguro? ¿*Quid* con el peligro de un *proxy discrimination* o por representación? Hablamos en este punto en el uso de datos y de información fácilmente neutra obtenido por otras fuentes «por representación»¹⁹⁸.

La cantidad promedio de transacción de *ransomware* en 2021 ha alcanzado cotas inimaginables siquiera un lustro o un par de años antes, como el reto del mercado global de seguros cibernéticos que solo en 2025 se aspira a superar los veinte mil millones de dólares, sobre todo ante el auge y demanda de seguros cibernéticos en el sector sanitario-médico, los servicios profesionales, la industria financiera, las entidades administrativas, etc.¹⁹⁹.

reconocible para el asegurado) de asegurar la infraestructura técnica (TI) utilizada para las actividades operativas, probablemente se trate de todo sistema de tecnología de la información y la comunicación o de todo sistema conectado a él. El término *sistemas de procesamiento de información* debería por tanto abarcar todos los sistemas que realmente pueden verse afectados por un ciberataque. Los ejemplos anteriores quedarían cubiertos por esta perspectiva.

Además, la violación de la seguridad de la información debe haber sido provocada por uno de los eventos asegurados enumerados en los apartados A1-2.4 AVB Cyber (final):

- «ataque a los sistemas electrónicos de procesamiento de datos o información de las Naciones Unidas», que debe incluir al menos todas las acciones llevadas a cabo por terceros (externos) específicamente contra los sistemas de TI de las Naciones Unidas,
- «acceso no autorizado a los datos electrónicos de la VN», como espiar, alterar o eliminar secretos comerciales o datos personales,
- «interferencia con los sistemas de procesamiento de información de las Naciones Unidas», que probablemente incluye acciones tanto intencionales como negligentes por parte de empleados de las Naciones Unidas,
- «un acto u omisión que dé lugar a una violación de las normas de protección de datos de la ONU», es decir, ataques externos o una «violación de datos» causada internamente por empleados de la ONU, como resultado de lo cual la protección de los datos personales ya no está garantizada, o
- «programas maliciosos que afectan los sistemas electrónicos de procesamiento de datos o información de las Naciones Unidas».

Al igual que el AVB Cyber, un gran número de otros términos y condiciones también están vinculados fundamentalmente a la ocurrencia de un evento causal específico, específicamente nombrado, si bien utilizando una terminología diferente. Esto crea un requisito de cobertura adicional y limita la gama de escenarios que deben cubrirse.»

198. En este punto, de nuevo SNYDER, «A.I., *Big data* and the threat of proxy discrimination: a revolution in the U.S. insurance industry», *op. cit.*, y en donde el autor hace referencia a todos esos datos que tienen no tanto un componente racial o de clasificación por sexo, cuanto el uso de códigos postales, promedios de calificaciones, información de compra con tarjeta de crédito, análisis de reconocimiento facial, etc., de cara a identificar a aquellos clientes objetivo a quienes las compañías no desean asegurar, o solo asegurarán con un pago de prima más alto.

199. Un bosquejo a modo de radiografía económica en HILL/MITCHELL, «Cyber security: 2022's top trends», 20 de enero de 2022, https://www.lexology.com/library/detail.aspx?g=0c36868a-d38b-46a1-b01b-d20d669614f8&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+General+section&utm_

Desde la creación y la ingeniería productiva de seguros y modalidades, pasando por su distribución y comercialización, al impacto que supone el conocimiento del riesgo en todas sus dimensiones, intensidades y frecuencias que abarcan, sin duda, la gestión del siniestro²⁰⁰. Pero también lo será en todos aquellos sectores comunicantes y a la vez interdependientes con el seguro, como es por ejemplo el ámbito salud o sanitario, donde se habla precisamente de la digitalización sanitaria o sanidad digital²⁰¹.

campaign=Lexology+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2022-01-24&utm_term=, donde aseveran: «Si bien los ataques a víctimas de alto perfil como Colonial Pipeline, JBS y Kaseya han atraído la atención del público, la resiliencia cibernética debería ser un imperativo para todas las organizaciones; El 39% de todas las empresas del Reino Unido informaron una violación de datos o un ataque cibernético en 2020/21. El fuerte aumento de los ataques de *ransomware*, acelerado sin duda por los modelos de trabajo híbridos, está impulsando un aumento en los precios de los seguros cibernéticos».

200. El reto sin duda es, y pasa, porque ese uso de análisis, de inteligencia artificial y mejora en los procesos de gestión del siniestro alcance a todo tipo de siniestros, no solo los de menor intensidad. Como afirma HEMSTED, «Insurers will explore the use of claims automation in serious and catastrophic casualty claims», 10 de diciembre de 2021, https://www.lexology.com/library/detail.aspx?g=3bec75cf-40df-4bf4-80bc-b294fbc34a6f&utm_source=, a medida que crece la experiencia en el uso de tecnologías de manejo de siniestros y estas tecnologías se vuelven más sofisticadas, las aseguradoras buscarán cada vez más utilizar procesos de automatización de siniestros en siniestros más graves y catastróficos, así como siniestros complejos fuera del espacio de siniestros. Estos cambios no solo beneficiarán a las aseguradoras, sino que también brindarán una mejor experiencia de reclamos para los asegurados. El uso de análisis, inteligencia artificial y mejora de procesos en reclamos más complejos elimina no solo los costos administrativos, sino que, lo que es más importante, brindará a los manejadores tiempo adicional para concentrarse en la progresión y liquidación de reclamos.
201. En este punto, afirma PES, «L'assicurazione contro il rischio di non autosufficienza nel sistema delle assicurazioni della salute», *Ass.*, 2021, n.º 4, pp. 595 y ss., p. 628: «Si premette che con l'espressione "digitalizzazione sanitaria" si allude sia alla c.d. sanità digitale (*eHealth*), consistente nell'uso degli strumenti di informazione e di comunicazione tecnologica in ambito medico —quali, tra tutti, la telemedicina, il telemonitoraggio, il teleconsulto, le cartelle cliniche e i fascicoli sanitari elettronici—, sia al contiguo fenomeno dello sfruttamento dei *Big data* sanitari, ossia all'utilizzo dell'immensa mole di dati inerenti ai profili sanitari, ricavabili dal *web* o da altre fonti, tra cui, appunto, gli stessi dispositivi di *eHealth*. L'innovazione tecnologica del settore medico, attualmente oggetto di grande attenzione e di ingenti investimenti delle istituzioni italiane e sovranazionali, assume in questa sede particolare interesse poiché le nuove tecnologie son sempre più di frequente applicate nell'ambito dei contratti assicurativi della salute, e, dunque, anche dell'assicurazione contro il rischio di non autosufficienza, svelando, come intuibile, indubbie potenzialità nella tutela del soggetto in condizione di vulnerabilità. In termini generali, è con l'espressione "*Digital Health Insurance*" che si fa riferimento al graduale diffondersi, nel mercato assicurativo italiano, di polizze della salute che prevedono, in via accessoria rispetto alla prestazione principale dell'assicuratore, l'erogazione di una serie eterogenea di prestazioni connotate dal ricorso a strumenti di matrice digitale. Seppur in misura minore rispetto alle altre coperture sanitarie, anche con riguardo all'assicurazione contro il rischio di non autosufficienza si registra ormai un processo di graduale digitalizzazione, invero fortemente auspicato e destinato a permeare l'intero settore *LTC*».

No cabe duda que, es el ámbito curativo y terapéutico, donde más fuerza ha cobrado la inteligencia artificial al hablar de medicina, pero lo que no significa que no haya impactado en otros marcos o ámbitos sanitarios²⁰².

Frente a riesgos tradicionales irrumpen con intensidad nuevos riesgos o riesgos latentes que la digitalización del seguro permitirá, a través de su transformación aplicativa, acercarse más certeramente al riesgo, al impacto, la frecuencia del mismo, como sucede con el cambio climático o los riesgos asociados al mismos y donde la predictibilidad en esta nueva era de los datos frente a la anterior era actuarial ha dado un giro copernicano²⁰³.

Precisamente cuando otros riesgos y su siniestralidad están cayendo o lo harán cada vez más gracias al empleo de mecanismos inteligentes y dispositivos que precisamente hacen que la probabilidad siniestral caiga, como sucede por ejemplo con la conducción inteligente y automatizada²⁰⁴. Pero el hecho de que las cosas sigan o no este derrotero no empece constatar cómo InsurTech ha traído problemas específicos desde un punto de vista, también, regulatorio. Las tecnologías traen riesgos, ignotos en buena medida para las pautas de evaluación y mensurabilidad de los esquemas aún antiguos de no pocas prácticas y experiencias o marcos asegurativos.

El problema eminente es de encaje. Esto es, sirvan las normas actuales y aún vigentes para encajar la revolución digital que también están expe-

202. Así, afirma con razón MOLNÁR-GÁBOR, «Artificial Intelligence in Healthcare: doctors, patients and liabilities», *Regulating artificial intelligence* [WISCHMEYER/ RADEMÄCHER/ (Eds.)], Cham, 2020, pp. 337 y ss., p. 339: «La inteligencia artificial (IA) ya se utiliza de muchas maneras en la medicina actual, y su ámbito de aplicación abarca varios campos tanto de la investigación médica como de la asistencia sanitaria, entre ellos el descubrimiento de fármacos, el cribado, la cirugía, la gestión de enfermedades crónicas y la organización general de la asistencia sanitaria. Sin embargo, su campo de aplicación más frecuente y probado en la actualidad se encuentra en el centro de la asistencia sanitaria curativa: la detección de enfermedades, especialmente a través de imágenes médicas. La evaluación de las imágenes de rayos X, TAC, TRM o microscopía de escaneo láser confocal creadas con la ayuda de la IA se centra en la detección de anomalías y la segmentación mediante la delimitación de áreas espaciales biológica y médicamente distinguibles (como la diferenciación entre tejido enfermo y sano) y la posterior clasificación por tipo de enfermedad. La IA ya ha logrado un éxito considerable en todos estos procesos de trabajo y a menudo supera la calidad de los hallazgos diagnósticos de los médicos y el personal de radiología».

203. Categórico LAZCOZ MORATINOS, «Análisis jurídico de la toma de decisiones algorítmica en la asistencia sanitaria», *La regulación de los algoritmos* [HUERGO (Dir.)], Cizur Menor, 2020, pp. 283 y ss., concluye en p. 285: «La medicina y el cuidado de la salud son algunos de esos escenarios donde la ubicuidad algorítmica ha cobrado especial protagonismo».

204. Como bien aduce MUÑOZ PAREDES, «Seguros *usage-based*», *op. cit.*, p. 2, la introducción del *Big data* en el seguro con la consiguiente digitalización del contrato ha propiciado que haya una mayor relación con la compañía al tiempo que ha hecho que se introduzcan modalidades contractuales más adaptadas a las necesidades de cada cliente y, en este clima, que se popularicen fórmulas de aseguramiento que se basan precisamente en que la aseguradora controla el riesgo durante el curso del contrato a través del uso de dispositivos telemáticos.

rimentado y si lo hacen o sirvieran, ¿verdaderamente estas normas son neutras?²⁰⁵

No son pocas las aseguradoras que ya a través de *chatbots* interactúan con sus clientes o que escanean la cara del usuario para perfilar la oferta de un producto o proveen un asistente virtual²⁰⁶. Asistentes que son capaces de combinar tecnologías como la biometría o la inteligencia artificial para revolucionar el enfoque de los seguros de vida.

El sistema convierte la contratación en un proceso interactivo en el que, en lugar de que el usuario rellene formularios, es capaz de inferir los datos básicos y hábitos de vida del cliente con solo analizar su cara²⁰⁷. A ello, hay o habría que unir una mejor información, más eficiente y, sobre todo, más utilizable —*usable information*— que permita al consumidor de seguros un conocimiento más real de los productos y las prestaciones²⁰⁸.

Una de las cuestiones clave, es y será, perimetrar y conocer, cómo usarán las entidades aseguradoras y el sector en general, pero también reguladores y supervisores económicos, la inteligencia artificial. Y si la misma será o no capaz de ser auditada²⁰⁹. No olvidemos que la inteligencia artificial

205. *Vid.*, sobre este reto sobre la necesidad de una regulación tecnológicamente neutra, de TERESZKIEWICZ, «Digitalisation of insurance contract law: preliminary thoughts with special regard to insurer's duty to advise», *InsurTech: a legal and regulatory view* [MARANO/KYRIAKI (Eds.)], 2020, Berlín, pp. 127 y ss.

206. Nos habla de *Azul*, el asistente virtual de Zurich, la profesora MUÑOZ PAREDES, M.^a L., «“Big data” y contrato de seguro: los datos generados por los asegurados y su utilización por los aseguradores», *La regulación de los algoritmos* [HUERGO (Dir.)], Cizur Menor, 2020, pp. 129 y ss., p. 131, viendo además a este como una herramienta que cambia la forma de contratar el seguro y haciéndolo más cercano y atractivo para el perfil de clientes jóvenes.

207. Sobre estos asistentes véase la propia web de Zurich, <https://www.zurich.es/notas-prensa/zurich-lanza-azul-asistente-virtual-asegura-por-la-cara>.

208. Empleamos la expresión información utilizable en el caso de buscadores de cuadros médicos y prestaciones sanitarias que ha reglamentado la autoridad sanitaria holandesa («NZa») y donde se exige a las aseguradoras de salud que informen adecuadamente a los consumidores, ya sea en fase preperfectiva como constante el seguro. Incide precisamente a los buscadores de atención en línea de proveedores de atención médica, así como también los toques de rotación. *Vid.*, in extenso, SCHRIJVERSHOF/PLETTENBURG/PEETERS, «New NZa regulations on the provision of information by health insurers: a missed opportunity or a conscious choice?», 18 de enero de 2022, https://www.lexology.com/library/detail.aspx?g=e33f9335-acf6-47e8-9923-710eeb2d3e26&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+General+section&utm_campaign=Lexology+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2022-01-26&utm_term=.

209. Afirma WATCHER, «The other half of the truth: staying human in an algorithmic world», 2019, <https://www.oecd-forum.org/posts/49761-the-other-half-of-the-truth-staying-human-in-an-algorithmic-world>, cómo una toma de decisiones más precisa, eficiente, justa y coherente es sin duda una gran ventaja. A diferencia de la toma de decisiones humana, las contrapartes algorítmicas no se cansan, no están de mal humor o no pueden ser sobornada. La IA es objetiva en sus decisiones y tratará por igual a las personas. La IA puede ayudarnos a tomar decisiones justas eliminando el elemento humano falible de la ecuación. Pero esto es solo la mitad de la verdad. Hace tiempo

se basa, ante todo, en la estadística²¹⁰. Y que existen sesgos, se introducen, pero también prejuicio en los sistemas computacionales²¹¹. Pero ese uso, ese

que somos conscientes de que la toma de decisiones sesgada y discriminatoria es uno de los mayores desafíos de la IA. «Los algoritmos aprenden de los datos históricos y, por lo tanto, también aprenden de nuestro pasado. La injusticia y las desigualdades de nuestro mundo se reflejan en los datos que se introducen en estos algoritmos. Los datos históricos en justicia criminal, el reclutamientos y los servicios financieros reflejan el pasado y, a veces, las amalas decisiones que hemos tomado colectivamente. Esto significa que la IA puede replicar nuestros sesgos, preconceptos, reforzando estereotipos y, quizás, crear otros nuevos».

210. No le falta razón a TISCHBIREK, «Artificial intelligence and discrimination: discriminating against discriminatory systems», *Regulating artificial intelligence* [WISCHMEYER/RADEMACHER/ (Eds.)], Cham, 2020, pp. 103 y ss., p. 107 cuando afirma: «La IA se basa en la estadística, y solo puede evaluar el futuro teniendo en cuenta el pasado. Las consideraciones normativas, en cambio, se rigen por lo contrafáctico. En consecuencia, puede resultar muy difícil traducir dichas consideraciones a un lenguaje que entienda la IA. Permítanme ilustrar esto con un último ejemplo, que nos conducirá directamente a las implicaciones jurídicas de la IA discriminatoria ... En una de las sentencias más influyentes en materia de derecho antidiscriminatorio de la última década, el TJUE, en el caso de la Association belge des Consommateurs Test-Achats, ha declarado que las tarifas de seguros que diferencian en función del sexo del cliente son discriminatorias». La sentencia del TJUE es un ejemplo clásico de cómo una prescripción normativa, por su propia naturaleza, puede tener que luchar contra los hechos (actuales) en beneficio de una realidad futura diferente, ya que, a la vista de los conocimientos estadísticos más avanzados, las compañías de seguros tienen todas las razones para calcular tarifas específicas por sexo. Estadísticamente, los hombres son mucho más propensos a causar accidentes de tráfico que implican daños importantes. Por otra parte, la esperanza de vida media de las mujeres es varios años superior a la de los hombres. Por último, las mujeres suelen tener más gastos relacionados con el embarazo. En consecuencia, cabe esperar que los seguros de coche y de vida sean más caros para los hombres que para las mujeres, mientras que las tarifas de los seguros de salud de las mujeres serán más altas que las de los hombres. En otras palabras: si las cifras son correctas —y nada indica que no lo sean—, el conocimiento estadístico insta a las compañías de seguros a utilizar el sexo como factor actuarial. Dicho conocimiento estadístico y sus consecuencias están, sin embargo, sujetos a la evaluación política y, en última instancia, a la estructuración jurídica. Se puede argumentar con fuerza que los costes del embarazo deberían repartirse por igual entre hombres y mujeres en lugar de dar lugar a tarifas de seguro de enfermedad específicas para cada sexo: la protección de la maternidad es incluso una obligación constitucional en muchos países y, posiblemente, la sucesión de generaciones preocupa a la sociedad en general. Además, como ha señalado el Abogado General en el asunto Test-Achats, el «principio de causalidad» exige sin duda una imposición de los costes por igual entre los sexos en caso de embarazo. Del mismo modo, incluso las expectativas de vida divergentes de hombres y mujeres pueden percibirse como una preocupación común, lo que implica un seguro completo. Sobre esta sentencia nos hemos ocupado ampliamente en el artículo conjunto VEIGA COPO/SÁNCHEZ GRAELLS, «Discrimination por razón de sexo y prima del contrato de seguro. Apuntes críticos a la sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 1 de marzo de 2011, en el asunto C-236/09 (Association Belge des Consommateurs Test-Achats ASBL y otros contra Conseil des Ministres)», *Revista de responsabilidad civil y seguro*, 2011, n.º 4, pp. 6 a 33; así como en VEIGA, *Tratado de contrato de seguro*, 7.ª ed., tomo II, 2021.
211. Repárese cuando menos en el provocativo pero elocuente título del artículo de CHANDLER, «The racist algorithm?», *Michigan L. Rev.*, 2017, vol. 115, pp. 1023 y ss., donde pone de manifiesto en p. 1025 cómo corporaciones como Facebook posee una patente sobre un proceso por el que puede denegar un préstamo a un usuario en función de quiénes sean

basarse «en» puede y ha de ser imparcial²¹². Mas no podemos llamarnos a equívocos, las posibilidades de manipulación discriminatoria son innegables al tiempo que innumerables²¹³.

Y aun siendo imparcial, neutro, no podemos ignorar que debemos conocer también cómo ese mismo uso y empleo de la inteligencia artificial afectará a los marcos, cánones, principios, vectores, etc.²¹⁴, por los que, hasta el presente, ha discurrido el quehacer asegurativo, desde una base o planta más tradicional, a otra, absolutamente disruptiva²¹⁵. No es que la máquina adquiera conocimiento, sino que el empleo de algoritmos complejos redimensiona y revoluciona el análisis, el aprendizaje y conocimiento de lo que resulta programado²¹⁶.

Desde una era genuinamente actuarial a otra ingente y todavía no abaricable ni conceptual ni categóricamente en toda su intensidad, como es la era de los datos o la ciencia de los datos masivos²¹⁷.

sus redes de contacto o amigos. O el caso de IBM que pretende ofrecer un algoritmo que distinga a los refugiados de los terroristas: «the sheep from the wolves». O el hecho de que los agentes de policía usan algoritmos de «policía predictiva» —*predictive policing*— de cara a identificar a «*hot people*» quiénes *a priori* serían más propensas a cometer delitos.

212. Ya señalaba en su momento REIDENBERG, «*Lex Informatica: the formulation of information policy rules through technology*», *Texas L. Rev.*, 1998, vol. 76, n.º 3, pp. 553 y ss., p. 581: «The advantages of *Lex Informatica* give it strength as a policy instrument. Technological configurations allow security wrappers to be placed firmly around information wherever it travels on the network. PolicyMaker, for example, can be used to assure that information is only used by authorized individuals for permitted uses. Technological mechanisms even allow data sources to specify information policies that impose restrictions on the manipulations of information at remote sites».
213. Así, PASQUALE, «Bittersweet Mysteries of Machine Learning (A Provocation)», *London Sch. Econ. & Pol. Sci.: Media Pol'y Project Blog* (Feb. 5, 2016), <http://blogs.lse.ac.uk/mediapolicyproject/2016/02/05/bittersweet-mysteries-of-machine-learning-a-provocation/> <https://perma.cc/XSS9-2D58>, p. 82, cuando señala cómo los algoritmos de búsqueda de Google y los algoritmos de presentación de Facebook, determinan la información que vemos.
214. También vemos la aparición de algoritmos policiales preventivos, que pueden tener el efecto de dirigirse cada vez más a los barrios minoritarios, sometiendo así a las minorías a una mayor vigilancia, y quizás mayor riesgo de uso accidental o erróneo de la fuerza policial. Así, véase el interesante artículo de KOSS, «Leveraging Predictive Policing Algorithms to Restore Fourth Amendment Protections in High-Crime Areas in a Post-Wardlaw World», *Chi.-Kent L. Rev.*, 2015, n.º 90, pp. 301 y ss., p. 321, donde se describe cómo las áreas de alta delincuencia zonas de alta criminalidad son desproporcionadamente barrios de bajos ingresos y minorías en todo Estados Unidos.
215. Así señala MUÑOZ PAREDES, «Seguros *usage-based*», *op. cit.*, p. 3, frente al seguro tradicional, el seguro *usage-based* insurance, se caracteriza porque la prima aumenta o se reduce en función del uso efectivo del bien, si son seguros de cosas, o del comportamiento del asegurado, si lo son de personas.
216. Correctamente señala LAZCOZ, *op. cit.*, p. 284 «... se trata de complejos modelos algorítmicos que, frente a la programación clásica, tienen la capacidad de “aprender” en su tarea programada, rutinaria y automatizada a partir de ejemplos que se facilitan, además, con la capacidad de manejar un número de variables inabordable por la programación clásica».
217. En su trabajo, BAMBAUER/ZARSKY, «The algorithm game», *op. cit.*, p. 9, señalan: «La segunda advertencia importante sobre los algoritmos de discriminación es que

Esta obra pretende responder a un simple interrogante, ¿es la IA la que ha de adaptarse al Derecho o es este, acaso, el que ha de adaptarse a la IA? No cabe duda que tanto los retos como a la vez desafíos que la IA depara son, simplemente, fascinantes, tensionando anclajes, principios, inmutables hasta el presente, dogmas —no pocos de ellos falsos o artificiales a su vez—, y cuestionando esencias, circunstancias y accesoriedades que el jurista ha de distinguir con su fino bisturí. Sacralizar principios o dogmas o meramente pretender explicar y cobijar cada construcción jurídica ex novo anclándolo con o sin fórceps en esas viejas preconcepciones, sería, es y será un error. Pero lo nuevo, la IA no supone un cambio de paradigma. No es eso.

Cómo ha de usarse la IA y cómo evoluciona el derecho ante la misma ha abierto un amplio debate y sobre todo tensionado y revolucionado las viejas costuras jurídicas de entender principios, contratos, reglas interpretativas, elementos esenciales de la relación jurídico desde otro plano. Seguridad y confiabilidad son el eje nervial del desarrollo y transformación digital a la que asistimos y que gravita sobre el dato, o por mejor señalar, sobre millones de datos. Este libro, ya en su tercera edición, ofrece respuestas y brinda argumentos en este debate y en este nuevo constructo jurídico en el que todo debe ser redimensionado.

ISBN: 978-84-1085-107-8

