11

Algoritmia discriminatoria en la selección de riesgos asegurados

ABEL B. VEIGA COPO
Profesor Ordinario de Derecho Mercantil
Universidad Pontificia Comillas

SUMARIO: 1. DISTORSIONES DISCRIMINATORIAS. 2. DISCRIMINACIÓN Y SEGUROS DE PERSONAS. 3. DISCRIMINACIÓN Y ALGORITMIA. 4. EL DATO Y LA DECISIÓN RACIONALIZADA POR EL PRISMA TECNOLÓGICO. 5. UN DESIDERÁTUM REAL Y POSIBLE: LA TRANSPARENCIA ALGORÍTMICA. MÁS ALLÁ DE LA ETICIDAD.

1. DISTORSIONES DISCRIMINATORIAS

La genética intrínseca del contrato de seguro parte de una realidad incontestada, de una parte, la enorme asimetría informativa, de otra, la propia incompletitud del contrato mismo. Y sí, son estos dos elementos y realidades los genuinos rubicones de un contrato sumamente interpretado, litigioso y litigado, dinámico y vivo como pocos y donde más allá de la erosión de la bilateralidad necesaria de un contrato como éste, basado en condicionados poco o nada negociados y en los que la capacidad de negociación se reduce a mínimos y solo a una aceptación en bloque de condiciones y cláusulas o su alternativa de elegir y aceptar los de otro oferente, la vulnerabilidad cuál estado, queda de manifiesto. El como han reaccionado los propios operadores del mercado, así como, el legislador y distintas normativas con mayor o menor acierto, yendo o no de raíz al nervio mismo del problema, ha marcado, marca y marcará el derrotero por el que transita tanto en una versión analógica tradicional como otra disruptiva tecnológica o incluso inteligente, el contrato de seguro.

Uno de los debates más apasionantes a los que estamos asistiendo en los últimos años viene de la mano, sin duda, de la interconexión estrecha y

condicionante, entre el desarrollo tecnológico y su incidencia, de un lado, en el seguro, pero de otro, y no menos fundamental, de los nuevos riesgos que esa tecnología es capaz de crear y, por tanto, ante la necesidad de dotar de coberturas asegurativas[1]. Sutil o sublimemente la posibilidad de sesgar en el universo de la algoritmia tan o más ignoto para el consumidor de seguros que el parnaso mismo de la aleatoriedad, abre la puerta hacia la discriminación y la enorme riqueza tipológica de la misma, amén de explicativa causalmente, está más entreabierta que nunca.

Mas, ¿por qué sigue existiendo opacidad y máxime una absoluta ausencia de transparencia en todo lo que es y debe ser la lucha contra la discriminación en el seguro o el facilitamiento de conductas y prácticas leoninas o abusivas que excluyen de raíz ciertos riesgos, normalmente los más onerosos o los más estadísticamente asociados a parámetros de siniestralidad más grave? En España hay alrededor de tres millones y medio de personas con discapacidad. Desde discapacidades osteoarticulares, enfermedades crónicas, a discapacidad intelectuales.

Además, la cronificación de ciertas enfermedades, o el haber padecido un cáncer, un ictus, ser diabético, hipertenso, etc., son situaciones que agravan la dificultad de un seguro o de plenas coberturas, cuando no exclusiones si bien no directas sí indirectas o con límites cuantitativos o prestacionales de cobertura.

La informática, la computerización masiva, el tratamiento de datos, la nano y la biotecnología, la predictibilidad, los nuevos tratamientos médicos, la diagnosis, la cirugía, todo está cambiando, pero también convulsionando técnicas, productos, servicios y prestaciones profesionales. El conocimiento, el dato y megadato sobre todos estos extremos que marcan la vida de la persona, sus hábitos, costumbres, conductas, acciones y omisiones son hoy conocidas, detectables, analizadas, sistematizadas, procesadas y, por tanto, tenidas en cuenta de cara a la asegurabilidad de los riesgos, si tarificación y la preconfiguración última de lo que es siniestrable o no en el seguro.

Sin duda esta nueva era o etapa disruptiva y a la vez ingente en información —no accesible a todos en idénticas circunstancias y condiciones— incidirá en el seguro, en su oferta, en sus prestaciones, en sus costes y en sus coberturas cada vez más eficientes, pero también más selectivas y por tanto, antiselectivas. Ya lo está haciendo, y lo hace tanto desde la configuración de nuevas ofertas de productos que se centran en estos riesgos exclusivamente,

1. Nos introducíamos por esta senda en nuestro pequeño ensayo VEIGA COPO, *Hacia una reconfiguración del contrato de seguro*, Cizur Menor, 2018.

como en la alteración de presupuestos y coberturas de nuevos riesgos en contratos digamos, clásicos, como el seguro contra robo[2].

Los avances tecnológicos a los que la sociedad está asistiendo, el impulso en la gestión y tratamiento tanto de análisis como de los riesgos y sus técnicas, están, inequívocamente, condicionando el propio desarrollo del seguro, tanto en sus aspectos cualitativos como cuantitativos, pero también en su propia dimensión jurídico-económica. Una dimensión donde la discriminación no es un mero convidado de piedra.

Un espacio además donde colude y colide con la pérdida de oportunidad de estar asegurado o el estarlo en miméticas condiciones u oportunidades de un digamos patrón medio de consumidor de seguros y, por ende, de trasladar un riesgo o riesgos a cambio de un precio o prima o premio y con ello la traslación de una función aseguradora de quién a cambio de bases estadísticas, actuariales, hoy algorítmicas sobre todo, lo asume en una mutualidad estandarizada de base que, propende, en último extremo hacia una catódica homogeneidad de riesgos que limita indirectamente la siniestralidad o por mejor decir, la probabilidad misma de siniestros. La discriminación recorre como antes se señaló no solo la genética sino la realidad misma del seguro al sesgar o impedir que todo potencial asegurado pueda contratar un producto en las mismas condiciones legales y jurídicas que cualquier otro potencial asegurado si no reúne ciertos caracteres o circunstancias que limitan ese acceso.

Más allá de referirnos ahora mismo a la irrupción que todo ese desarrollo informático, tecnológico, computacional, tratamiento masivo de datos puede generar *per se* como riesgos cibernéticos y amenazas a la integridad de toda esa información y su vulnerabilidad económico competencial, es ese mismo desarrollo tecnológico el que está revolucionando no pocos sectores de seguros[3].

Aunque también influyendo, cuestionando y, si se nos permite, erosionando cuasi principios sagrados del seguro como era el *alea* o aleatoriedad del contrato, carácter ya de por sí puesto en tela de juicio en la doctrina francesa donde cada vez más irrumpe una reafirmación de la conmutativi-

2. Así, por ejemplo, véase el artículo de VOGLET, «Assurance vol et nouvelles technologies: nouveaux enjeux», *L'assurance vol. Aspects juridiques et pénaux*, (CALLEWAERT, et al.), Limal, 2018, pp. 137 y ss.

3. Como bien afirma SOBRINO, «Seguro de drones», La Ley (Argentina), 16 de marzo de 2018: «Los modernos avances de la tecnología van generando nuevos desafíos para el Derecho, al aparecer distintas responsabilidades legales y —como contrapartida— obliga al mercado de seguros a buscar novedosas coberturas».

dad del seguro en vez de aleatoriedad. ¿Hasta qué punto la predictibilidad, el big data, los biomarcadores, los sensores, la genética y un largo etcétera rompen ese alea y dotan, en suma, de certidumbre al riesgo asegurable?

Hoy como ayer, el interrogante sigue incólume, ¿por qué discriminamos?, ¿qué *ratio*, que pretensión sustenta el no dar a todos un mismo trato o una idéntica oportunidad?, ¿es admisible en el seguro una discriminación entre iguales o solo la secuenciamos entre desiguales? ¿Por qué no mutalizar entre una base de cientos de miles de asegurados los riesgos de aquéllos que pueden ser objeto en la práctica de discriminación y exclusión del seguro?

Pero más allá del dato, del historial médico, de la raza, de la etnia, de la capacidad crediticia o solvente, no cabe duda de que el eje de la discriminación no solamente se reconduce a este estadio o interim pre-perfectivo del contrato y el cuestionario, cuanto a través de la exclusión en las cláusulas delimitadoras del riesgo. La ley prohíbe discriminar a personas con discapacidad, con VIH y otras circunstancias de salud, pero ¿acaso no sigue habiendo o existiendo casos de exclusión en la práctica? Una persona obesa o con sobrepeso y que paga una mayor prima ¿es un supuesto de discriminación? Y si el padecer ciertas enfermedades, máxime si las mismas son calificadas como raras y que abordaremos *infra*, es objeto de denegación o exclusión de coberturas por las aseguradoras ¿es una discriminación encubierta o directa?

Es verdad que, desde un plano abstracto y genérico la LCS en sus disposicionandos adicionales cuarto y quinto prohíbe la denegación de acceso a la contratación o el hecho de arbitrar e imponer condicionados más onerosos a un asegurado por razón de discapacidad o por padecer VIH o en su caso, otras condiciones de salud. Pero en la práctica, ¿cómo se percibe en realidad el riesgo de vida y de salud que sufre un niño con parálisis cerebral o con fibrosis pulmonar? ¿va a ser asegurado, o las dificultades y condiciones de asegurabilidad serán tan complejas y eclépticas que en verdad no tendrá una natural y homogénea cobertura del seguro?[4]

4. En el artículo de FERLUGA, «Los indeseables del seguro», El País, 10 de marzo de 2021, (https://elpais.com/economia/2021/03/09/mis_finanzas/1615308327_522071.html#:~:text=%E2%80%9CEn%20t%C3%A9rminos%20generales%2C%20no%20existe,acceso%20a%20la%20contrataci%C3%B3n%2C%20el) pone en palabras de un intermediario: «Sería proporcional que la aseguradora declarara previamente que no asegura personas que han superado un cáncer durante los primeros cinco años hasta contar con marcadores limpios, por ejemplo, pero no lo es excluirles sin remedio, que es lo que pasa ahora».

Ahora bien, hipotética o eventualmente es dable aseverar en el contrato de seguro la existencia de una igualdad equitativa de oportunidades, y si así fuere, ¿qué rol entonces han de jugar la aleatoriedad y la discriminación?[5] O planteado de otro modo, toda diferencia y por ende, toda potencial y real discriminación ¿es justa? O *a sensu contrario*, ¿cómo justificamos la discriminación que no necesariamente ha de conducir siempre y en todo caso a desigualdad real? Sí en cambio es discriminativa la que se basa o toma como idea nuclear la igualdad, pero no lo es la que parte de la desigualdad. Mas, este esquema ¿es trasladable a la discriminación y sesgo que se produce en la antiselección de riesgos en el seguro?

¿Se discrimina entre iguales o es lícita e, incluso moral, entre desiguales?, ¿todos somos efectivamente aversos al riesgo o lo somos en intensidades diferentes? Acaso en un contrato como éste en el que la asimetría informativa es ingente, ¿no se discrimina con el lenguaje o con la interpretación del contrato?, el lenguaje ambiguo, oscuro, como la reticencia y la omisión abonan el terreno de la discriminación y, con ello, de la duda de lo asegurable que erosiona la credibilidad de un contrato incompleto *per se* desde su mismo origen; ¿cómo encaja la aleatoriedad con el riesgo discriminado o sesgado? O cómo se lleva a la práctica finalmente esa discriminación contractual ¿subjetiva, objetiva, actuarialmente, a través del cálculo de probabilidades, o ya hoy, en medio del gran oleaje que también jurídicamente surge, que es la algoritmia. Acaso ¿la tecnología no sesga como antes lo hicieron otros instrumentos?

No olvidemos que no pocas garantías aseguradas en una póliza están o pueden estar limitadas por las propias disposiciones del contrato de seguro, pensemos en supuestos por ejemplo de coberturas en una póliza de responsabilidad civil o en una de accidentes y en las que existen ciertas limitaciones hacia los terceros lesionados. ¿Realmente estamos ante una discriminación o una simple concreción de los derechos del asegurado?[6]

5. Ya RAWLS, *La justicia como equidad: una reformulación*, Barcelona, 2002, p. 73 es consciente y así lo interioriza en su discurso construccional que el origen social y económico de las personas actúa como motor determinante de las expectativas vitales y los planes de acción y actuación de la persona a lo largo de su vida. Por ello, el profesor británico propone desde la igualdad de oportunidades que se trate en la medida de lo posible de mitigar las desigualdades que la fortuna arbitrariamente ha otorgado a cada individuo.
6. Vid., la reciente sentencia de Casación Francesa, 3.ª Civ., de 16 de septiembre 2021, n.º 20-15518, con la nota de CERVEU-COLLIARD, «La garantie de l´assureur envers les tiers lésés peut être limitée par les dispositions du contrat d´assurance», Gazette du Palais, 22 mars 2022, n.º 10, pp. 58 y ss.

¿Es indispensable y necesaria la discriminación en el contrato de seguro? Y de serlo, la pregunta es obligada, a saber, ¿en qué plano es admisible, solo en un plano puramente técnico o estadístico? ¿también en lo jurídico y lo social?, ¿cuándo está justificada y causalizada en la contratación de un seguro de vida, de salud, de decesos, colectivo de personas la discriminación? ¿quid con un deseable compliance normativo en este punto en el ámbito asegurador?

Pero ¿y la discriminación efectiva que puede llevarse a cabo en función de cómo esté redactado un cuestionario de salud ex artículo 10 LCS, donde incluso se pueden eliminar ciertas preguntas o sesgar intencional y tendenciosamente el sentido de las mismas o el sentido mismo de las respuestas posibles que quedan indefectiblemente condicionadas hacia un extremo?[7]

La discriminación es el trato desigual entre iguales. No entre desiguales si bien hay que identificar los parámetros de esa desigualdad para no sesgar la selección. Término, concepto, vocablo que transcurre y recorre por las fibras de este contrato incluso en su fase y momento pre-perfectiva y la ata, además, en la propia de la gestión del siniestro.

Desde el diseño mismo del producto del seguro la discriminación, —advierta lector que no adjetivamos ésta si positiva o negativa—, está presente. Pues discriminar es elegir, es optar, es limitar, es cuestionar en último y único extremo lo que es y como es asegurable para pasar a estar, en fin, asegurado.

Se elige, se sesga, se precondiciona a través de hechos y factores, circunstancias y situaciones que van desde lo humano a lo técnico, la edad y la enfermedad, al sexo o la piel, lo económico y solvente hasta lo profesional, lo tecnológico, etc., en un continuum que preconfigura y forma parte de la práctica aseguradora. O dicho de otro modo, se quiere que esté presente. Ahora bien, ¿es lógico, es razonable, es justo que se discriminen riesgos y asegurados en la práctica asegurativa? ¿cuál es en todo caso la finalidad última de esta acción?

7. Nuevamente FERLUGA, «Los indeseables del seguro», cit., señala: «Eliminar preguntas que son relevantes para la valoración de un riesgo es una barbaridad, porque se estaría obligando a las aseguradoras a contar con cálculos incorrectos», opina, por el contrario, Emilio Fiances. Este actuario de seguros considera que la discriminación es indispensable, pero solo desde un punto de vista puramente técnico y matemático. «La discriminación en tanto que marginación social es a todas luces inaceptable. Pero en estadística, no es más que la clasificación de datos, personas o cosas en función de características comunes y no tiene nada de malo», enfatiza Fiances, para quien esta herramienta sirve para segmentar los riesgos y ponerles precio en consecuencia, y para que estos se mutualicen por grupos homogéneos».

¿Por qué se discrimina?, ¿por qué se trata desigualmente incluso a quiénes de suyo por enfermedades, historiales médicos, predisposiciones genéticas, raza, etnia, discapacidad, etc., son desiguales, pero no ante el seguro? Discriminación y exclusión son términos homónimos conceptualmente en esta práctica de elipsis intencionada. Mas ¿cuándo lo desigual es injusto, indeseable, ilícito o cuando menos, requiere un reproche moral y conductual ante prácticas que pueden ser abusivas y vaciar de contenido y función al contrato mismo de seguro?

Lo común viene salpicado de fragmentación o segmentación, la homogeneidad no siempre es absoluta, o debe serlo. Pero los modelos de análisis y preselección de riesgos es obvio que se configuran y crean en base a estadísticas y frecuencias que han de contener al menos para su estudio sesgos discriminatorios. Ahora bien, esos sesgos pueden ser positivos, negativos, neutros o, decidida y finalísticamente, abusivos al excluir *per se* la asegurabilidad misma. Homogeneidad y mutualidad pueden ser una respuesta frente a la discriminación selectiva pero a la vez indiscriminada, pues mutualizar las bases personales del riesgo asegurado es diluir y dispersar esa frecuencia e intensidad de riesgos en algunos asegurados entre la multitud de pólizas.

Buenos y malos riesgos, selección *versus* antiselección, está y ha estado siempre presente en el seguro y en la técnica de seguros, pero también en la propia configuración y redacción del contenido de las cláusulas. Y tanto en seguros contra daños como en seguros de personas. El condicionado sigue siendo la verdadera piedra de toque discursiva y litigiosa de este contrato. Cuando no, la misma confusión, deliberada y ambigua, pero que año tras año está presente, entre cláusulas delimitadoras del riesgo y limitativas de derechos. Acaso, ¿no se discrimina o puede hacerse al excluir de cobertura o garantía asegurativa algunos riesgos cuya intensidad o frecuencia puede ser más alta o más onerosa en función de algunas circunstancias personales y subjetivas, temporales y objetivas, cuando no, económicas de los potenciales asegurados?

Combinados los hechos discriminantes de un lado, con las cláusulas de exclusión y limitaciones por otro, la ecuación es perfecta, o diríamos cuasiperfecta si no traemos a la misma otras variables, entre las que están la desnaturalización misma del contrato y el derecho a la igualdad.

Referirnos a discriminación significa indagar en la causa, en el porqué y el para qué y su finalidad última o teleológica. Amén de si con ello se vacía o no la función social del seguro[8]. Si se discrimina es porque hay una intencionalidad

8. In extenso. sobre esta función, véase nuestra monografía, VEIGA, *Función social del contrato de seguro*, Madrid, 2022.

manifiesta y finalística en llevarla a cabo. No importa el cauce o la forma. Hoy como ayer, el contrato de seguro se ha edificado a través de selecciones, de exclusiones, de sesgos, al margen del por qué y de la vía o instrumento en que se lleva a cabo. Hablar de digitalización, de revolución tecnológica y seguro implica de suyo secuenciar, con nitidez, el fondo y trasfondo del debate[9]. Máxime teniendo en cuenta que estamos ante un campo ignoto hasta hace unos años y donde lo tradicional asegurativo no casa y la estadística actuarial no existe[10].

Mas un campo donde la discriminación puede ser más amplia, sutil y sin embargo, sublime y poco detectable. Dedicaremos un capítulo a la discriminación algorítimica a la hora de esta selección de los «buenos y malos riesgos» o dicho de otro modo de lo que se quieren en fin, asegurar o no, aunque por el camino desnaturalicemos y vaciemos de función al seguro.

2. DISCRIMINACIÓN Y SEGUROS DE PERSONAS

Los contratos de seguros sobre la persona tienen como denominador común la cobertura de riesgos que atañen tanto a la existencia misma de la persona humana, como a su integridad corporal o a su salud[11]. Es la perso-

9. Como bien señala MADRID PARRA, «Smart contracts-Fintech: reflexiones para el debate jurídico», Revista Aranzadi de Derecho y Nuevas Tecnologías, 2020, n.º 52, (recurso electrónico), p. 1 «se descubre todo un "ecosistema" informativo que va desde quien vende las bondades de la tecnología Blockchain y de las criptomonedas hasta quien presta servicios financieros a través de apps instaladas en un móvil ofreciendo asesoramiento jurídico en relación con las criptodivisas y los Smart contracts».
10. Claros y categóricos en la doctrina norteamericana se dice: «La tecnología y los datos han transformado la oferta de seguros en el contexto cibernético porque, a diferencia de la mayoría de los ámbitos tradicionales de los seguros, las aseguradoras cibernéticas carecen de carecen de un historial de pérdidas y de datos actuariales en los que basarse a la hora de evaluar el riesgo. Como el ciberseguro es tan nuevo e incierto, y los riesgos cibernéticos y los ataques de los ciber atacantes cambian constantemente, las aseguradoras cibernéticas codician los datos de los proveedores de datos. Las aseguradoras cibernéticas están recurriendo a los macrodatos, la IA y el análisis para ayudar en los procesos de suscripción y gestión de riesgos y siniestros y, como resultado, están redefiniendo el negocio de los seguros». Cfr. CUNNINGHAM/TALESH, «The tecnologization of insurance: an empirical analysis of big data and artificial intelligence´s impact on cybersecurity and privacy», cit., p. 7.
11. Como bien señalan PICARD/BESSON, *Les assurances terrestres en droit français, Le contrat d'assurance*, cit., p. 609, al resaltar el carácter no indemnitario de los mismos, como los seguros de personas son seguros que tienen por objeto a la persona asegurada, «comportent des prestations» con independencia del daño que pueda resultar de la realización del riesgo cubierto. Véase también la definición amén de los caracteres jurídicos y técnicos de los seguros de personas que nos brindan LAMBERT-FAIVRE/LEVENEUR, *Droit des assurances*, 13.ª ed., Paris, 2011, pp. 739 y ss., autores que ade-

na, es su salud, son sus necesidades asistenciales o prestacionales, las que configuran inequívocamente el tronco nervial de estos seguros[12]. Y es aquí en la persona, en el ser humano, en su historial médico, en su patrimonio genético hereditario, en su piel, en sus enfermedades, en sus conductas, hábitos, costumbres, etc., donde los sesgos y las diferencias, los marcadores y parámetros de vida, actividad y salud pueden ser objeto de discriminación. El cómo se lleva a cabo la misma, así como las bases últimas en que ésta antiselecciona el riesgo y decide qué y hasta cuándo se cubre con límites no siempre iguales entre unos y otros asegurados o potenciales asegurados, abre el abanico discursivo crítico de esta monografía.

Estamos ante seguros de sumas, no de indemnización, sin que ello impida que algunas modalidades, híbridas, convivan auténticas parcelas, incluso seguros, como el de enfermedad o de reembolso de gastos médicos, en los

más nos ofrecen en la p. 751 unas causas sobre los porqués de la fuerte progresión de los seguros de personas en los últimos años, marcados sobre todo por la crisis de los mercados financieros y la especial atracción de estos seguros que combinan la previsión con el ahorro. Sobre las dificultades de brindarnos una noción clara de los seguros de personas se pronuncia NICOLAS, *Droit des contrats d'assurances*, Paris, 2012, pp. 443 y ss., especialmente bajo el epígrafe de las dificultades de comprehensión que implica la fórmula «seguro de personas». Una amplia retrospectiva histórica en la literatura del seguro nos la ofrece DONATI, *Trattato del diritto delle assicurazioni private*, III, cit., pp. 559 y ss. Señalaban DE GREGORIO/FANELLI, *Le assicurazioni*, 3.ª ed., Milano-Roma, 1969, p. 146 que mientras en los seguros de daños el ordenamiento jurídico tutela la necesidad de obtener un resarcimiento de un daño económico, en cuanto que este efectivamente se verifique y dentro de los restrictivos límites del daño realmente verificado, en el aseguramiento de vida se predispone un instrumento jurídico acto para satisfacer una cualquiera exigencia económica que se prevé pueda presentarse al verificarse la muerte o la sobrevivencia de una persona, sin que la existencia efectiva y la naturaleza de esta exigencia tengan algún relieve jurídico.
12. La historia del seguro, ineludiblemente va ligada también a la historia de los seguros de vida o los primeros aseguramientos. Como expusimos en el primer volumen del primer tomo de este Tratado, si fueron los seguros de incendios y marítimos los primeros seguros que conocieron la práctica, no anduvo muy a la zaga, si bien el debate como sabemos se centró en el interés o no en la vida humana y la apuesta, el seguro de vida, si bien éste arranca siglos después. Una buena retrospectiva histórica nos la ofrecen FISCHER/SWISHER/STEMPEL, *Principles of insurance law*, 3.ª ed., New York, 2006, pp. 1 y ss., sobre todo en el capítulo primero donde se analizan los fundamentos y la historia del seguro. También, imprescindible la aportación más antigua de VANCE, *Handbook of the law of insurance*, St. Paul, 1904, pp. 2 y ss. En EE. UU. la primera forma de seguros de vida surge hacia mitad del siglo XVIII, concretamente en 1759 en la iglesia prebisteriana de Filadelfia y de Nueva York que crearon la Corporation for relief and por and distressed widows of prebyterian ministers, dirigida a proporcionar un sustento económico a la familia en caso de muerte del ministro presbiteriano. Otras iglesias mimetizarían estos seguros. Vid. ALBORN/MURPFHY, *Anglo-american life insurance. 1800-1914*, London-New York, 2013.

que la finalidad resarcitoria también está presente, o incluso sea ésta la única finalidad del seguro, toda vez que, con ocasión de la persona, de la salud, de la enfermedad, surge un débito en su haber[13]. Y aquí también puede haber una discriminación de entrada de asegurados en función de su salud, de su estado físico o del país en el que viven, etc. Como es sabido la práctica asegurativa ofrece seguros con sumas ínfimas, llamados desde antaño, *seguros populares* y donde las pruebas médicas, los cuestionarios, son sumamente flexibles. Seguros extendidos y de mínimos que, hasta cierto punto, abrían la puerta a todo tipo de asegurados dentro de unos límites o marcadores y en los que, de entrada, la discriminación o rechazo del asegurado conforme a ciertas circunstancias no se producía.

Pero es también la prestación, el servicio profesional el que toma el pulso a algunos de estos seguros, significativamente los de asistencia sanitaria y los de dependencia, incluso el de decesos o exequiales. Y aquí sí se producen discriminaciones en donde la salud, y su historial familiar genético, los hábitos, la raza o etnia, pueden denotar precisamente esa discriminación y no selección. No por ello dejan de cobijarse bajo el paraguas de los seguros de personas, si bien, en puridad, deberíamos resituarlos en esa categoría propia y con perfiles definidos como serían los seguros de prestación de servicios o de asistencia, genuino *tertium genus* que debería, una vez por todos, romper la dualidad seguros contra daños *versus* seguros de personas.

Pero ello no significa que, a pesar de esta disparidad en la concepción, mas sobre todo, en la etiología misma de estos seguros, tengamos una regulación armónica, completa y satisfactoria de los seguros de personas. Al contrario. Así lo testimonia y asevera —todavía hoy en 2022— un genérico y bajo el evocativo capítulo de, disposiciones comunes, el artículo 80 de la norma de seguro en un claro afán tanto sistematizador como, en último caso, delimitador del alcance y, por tanto, de diferenciación, de los seguros de personas respecto de otros contratos de seguro[14]. Regulación que no es

13. Comienza su monografía VILRET, *Droit de l'assurance-vie luxembourgeoise*, Windhof, 2017, aseverando p. 7: «Le contrat d'assurance-vie est un outil complexe à facettes multiples. À ses origines, il avait une vocation de prévoyance et seul le risque vie était couvert par l'entreprise d'assurance; puis il est devenu un instrument d'épargne. De nos jours, il a également pour fonction d'être un instrument de crédit puisqu'il est fréquemment utilice dans la pratique des affaires comme mode de garantie pour un crédit accordé. Ce genre particulier de contrat relève d'un droit spécial et dans une certaine mesure des règles générales du droit des obligations».
14. Recuerda SÁNCHEZ CALERO, «Art. 80. Concepto», *Ley de Contrato de Seguro*, 4.ª ed., pp. 2029 y ss., p. 2030 como la delimitación de la noción de seguro de personas es importante tanto para señalar sus elementos diferenciadores con otras modalidades

completa, tampoco fue ésta la pretensión del legislador de 1980 y que ha de beber, por tanto, de los primeros artículos 1 a 25 de la LCS[15].

Ahora bien, la pregunta inicial y no por ello menos esencial, refiere a la propia entidad de esta regulación o disposiciones comunes, habida cuenta que el interrogante primigenio se centra en saber si todas estas normas o reglas comunes, pese a ese evocativo título, realmente son aplicable a las distintas categorías de seguros de personas. Y a renglón seguido si en base a este pequeño marco regulatorio, y a excepción de las taxativas y categóricas pero en todo caso genéricas disposiciones adicionales cuarta y quinta que tratan de limitar y vetar la discriminación, ¿es suficiente el marco eximio y constricto de regulación en estos seguros de personas para en verdad cauterizar las prácticas discriminatorias abusivas? En cierto modo, no cerremos o condenamos absolutamente la técnica antialeatoria y en cuyo seno se abriga la técnica discriminatoria.

Discriminar riesgos es seleccionar los mismos y ello es lícito hacerlo en función de parámetros claros, concisos, seguros y sobre todo, siempre con un límite de mínimos, a saber, no desnaturalizar el contenido mínimo de coberturas y prestaciones que un seguro, *per se*, en su función de garantía y en el fondo también en su función social ha y debe cumplir. El peligro es cuando esa discriminación veda absolutamente el acceso a la función asegurativa rechazando de entrada por las «vulnerabilidades» y circunstancias que para una aseguradora supone una onerosidad pese a la desvirtuación absoluta y banal del propio seguro.

3. DISCRIMINACIÓN Y ALGORITMIA

La revolución tecnológica se manifiesta en las herramientas, aplicaciones, internet de las cosas, la nube, el algoritmo, el big data, el machine learning, etc., sobre las que se asienta el vertiginoso y dinámico avance que revolu-

o clases de contratos de seguro como para poder distinguirlo de otras categorías contractuales que no son contratos de seguro en sentido estricto, en cuanto no pueden encuadrarse en el concepto de este contrato que ofrece el artículo 1.
15. Señala BINON, *Droit des assurances de personnes. Aspects civils, techniques et sociaux*, 2.ª ed., Bruxelles, 2016, p. 13 el gran péndulo que la legislación belga ha dado desde la inicial regulación de 11 de junio de 1874 en la que los seguros de personas fueron prácticamente ignorados a la hoy hipereglamentada normativa que existe en aras a la tutela del consumidor. Así señala en p. 23 como este derecho de seguros de personas, al igual que sucede con los de daños, ha devenido principalmente en un derecho con un fuerte tenor imperativo y de inspiración consumista. Y en el que la hiper reglamentación es algo menor que en otros ramos, dejando un amplio margen en materia de pago de la prima, o en el ámbito de duración del contrato.

ciona intrínseca y extrínsecamente el seguro en todas y cualesquiera de sus dimensiones[16]. Con ella lo hace la antiselección del riesgo asegurable, los parámetros que permiten edificar buenos y malos riesgos asegurables. O de mínimos asegurables y aceptados por quién compra y vende la asunción de riesgos y la gestión del siniestro dentro de tales parámetros.

Y todo ello sin perder de vista una realidad inmediata, a saber, no cabe esperar que la automatización reemplace todos los aspectos o dimensiones de la industria del seguro a corto plazo. Pero sí va a vertebrar la contratación, sus formas, la configuración intrínseca del producto con una acercamiento y realidad a la información y su procesación inaudita hasta el presente. Convivirá lo clásico o tradicional como lo más disruptivos, lo analógico con lo digital y, en su momento, lo cuántico[17].

Lo tradicional que partía de una radiografía sumamente estática del riesgo asegurado durante el período de seguro, a otra más dinámica donde el riesgo muta, pero también lo hace continuamente el riesgo asegurado y con ello, la prima[18]. Mas, cómo juristas, ¿qué rol y qué protección tendrá el

16. Aciertan TALESH/CUNNINGHAM, cit., p. 10 cuando concluye tras el análisis empírico con más de sesenta aseguradoras sumamente tecnologizadas, como «... los big data, la IA y las tecnologías emergentes no son todas iguales. Los científicos de datos y los programadores tienen múltiples oportunidades para dar forma a su desarrollo. Nuestra investigación empírica revela que las tecnologías emergentes no son neutrales, sino que se configuran y construyen de forma sutil por los individuos y las organizaciones que las desarrollan. Por tanto, la cuestión no es si los datos y la tecnología son buenos o malos o eficaces o ineficaces sino en qué condiciones estas tecnologías conducen a resultados socialmente deseables o indeseables. Nuestras ideas proceden del mundo empresarial y revelan la movilización de la tecnologización de los seguros, que conduce a resultados no neutrales que favorecen al sector de los seguros, pero que no necesariamente hacen que las empresas y los y, por tanto, a la sociedad) contraten más ciberseguros».
17. Vid., BLOSFIELD, «Imagining how tecnology might transform risks and insurance by 2030», 7 de noviembre de 2019, (https://www.insurancejournal.com/news/national/2019/11/07/547850.htm).
18. No les falta razón a TALESH/CUNNINGHAM, «The technologization of insurance», cit., p. 55 cuando enfatizan el eje esencial de una Insurtech respecto al paradigma común o tradicional del seguro y el punto de interacción ante el riesgo cibernético frente a las aseguradoras convencionales, así, afirman: «según el modelo tradicional, una vez que el asegurado acepta un contrato de seguro, la cobertura del asegurado queda bloqueada durante un año, independientemente de que el riesgo cambia». Pero las empresas insurtech totalmente integradas realizan en cambio una suscripción continua y «una gestión de riesgos más implicada y activa y un seguimiento de la variabilidad real del riesgo».
Mientras que la mayoría de las aseguradoras cibernéticas convencionales ofrecen servicios previos a la infracción que los asegurados sólo utilizan el 10% de las veces, las compañías de insurtech totalmente integradas incorporan funciones de seguridad de

consumidor y los datos ligados a su íntima privacidad así como su esfera real decisional en todo este proceso? [19]

Así, la clave de bóveda es, sin duda, la tecnología, su desarrollo exponencial y vertiginoso y, quizá, más que una sola, la combinación de distintas tecnologías que se están e irán sucediendo sin solución de continuidad desde hace años y a un futuro donde el presente se llama disrupción, avances, cuantificación, etc.[20]. Ahora bien, ¿quid si esa tecnología se emplea para discriminar y antiseleccionar vaciando la esencia, función y garantía que ha y debe cumplir en todo y cualquier caso el seguro? ¿Existe en verdad un uso imparcial de la tecnología en el seguro?

La tecnologización de los seguros no solo implica big data, análisis predictivo y herramientas forenses y de seguridad avanzadas. No cabe duda asimismo como en un futuro inmediato los proveedores de seguridad de la información que utilizan la IA para ayudar a las aseguradoras en la creación de modelos predictivos para mejorar la eficiencia en el proceso de contratación jugarán cada vez un rol más importante[21].

supervisión previa a la violación en el propio seguro y aumentan significativamente la adopción por parte de los asegurados. Si identifican que una amenaza es inminente, alertan a la compañía y trabajan con ella para evitar la amenaza. Estas aseguradoras ofrecen la transferencia y la gestión del riesgo simultáneamente.
19. Absolutamente acertado, HELVESTON, «Consumer Protection in the Age of Big Data», Wash. U. L. Rev., 2016, vol. 93, pp. 859 y ss., p. 866 y enfocado a la tutela del consumidor, cuando señala: «El análisis predictivo se refiere casi exclusivamente a las predicciones que resultan de sofisticados análisis tecnológicos de grandes conjuntos de datos. En contextos comerciales, el análisis predictivo se ha definido como los esfuerzos de las empresas para dar sentido al Big Data y obtener información que les proporcione ventajas competitivas sobre sus pares». No podemos olvidar como los macrodatos también plantean problemas de privacidad. Los datos pueden obtenerse y cosecharse sin el conocimiento o el consentimiento de las personas cuya información se recopila. Aunque los macrodatos no suelen utilizarse para identificar a personas concretas, no hay garantía de que la identidad personal se elimine de los datos. Los datos pueden utilizarse para eludir las leyes antidiscriminatorias dirigiendo el marketing online a determinados datos demográficos de los asegurados, como la raza, el sexo, la edad, etc. Si se prohíbe a las aseguradoras este tipo de información directamente, no se les debería permitir recopilarlos o utilizarlos en la clasificación de riesgos, y se deben hacer esfuerzos para detectar y prevenir la discriminación algorítmica. Cfr., TALESH/CUNNINGHAM, «The technologization of insurance», cit., p. 20.
20. Sobre esta combinación, véase ya hace más de un lustro, NAYLOR, *Insurance transformed: technological disruption*, Cham, 2017, pp. 1 y ss.
21. Claros en este punto TALESH/CUNNINGHAM, cit., p. 36 cuando reproducen la investigación empírica y señalan: «And so, what we did is we started collecting all that data, as well as looking at things like dark web data, and building out machine-learning algorithms and natural language processing algorithms to actually sort

Esta confluencia impacta en el seguro de un modo tal como en su momento hicieron conceptos como la mutualidad y la estadística para revolucionar el contrato, la gestión y la distribución en tanto valor global en su conjunto. Mas la pregunta que hemos de hacernos, obligada por lo demás, es saber cuál es el verdadero impacto de esto que llamamos tecnológico unas veces, digital otro[22]. Una tecnología digital que, incluso, va a transformar la regulación, pero paralelamente y sin solución de continuidad, reinventar estrategias, productos y servicios de seguro[23]. Pero eso

through all this stuff at scale. And so now, instead of only having your population of companies that you've either underwritten and actually written the policy or have come and shopped with you, you can now compare people to the universe and use that to really try to fine-tune your strategy. So, underwriters can get company-specific information-sets of risk factors, technical things like vulnerabilities to behavioral things like employee sentiment, for example. And then we'll build out frequency and severity models and provide analytics on all this stuff so that underwriters could understand if I write a particular layer of coverage, based on (these) models, what are the dollars and probabilities associated to losses?».

22. No más gráfica puede ser 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), cuando afirma: «El valor de la innovación es mejorar la sociedad y fomentar el desarrollo humano. La innovación debe tener el propósito de aumentar la igualdad de oportunidades y la inclusión. La innovación debe acercarnos y no separarnos más».
23. El pasado 7 de febrero de 2022, EIOPA, en su informe «*Report on Best Practices on licensing requirements, peer-to-peer insurance and the principle of proportionality in an InsurTech context*», resume las consideraciones de la ESA (Autoridades Europeas de Supervisión) en respuesta a la invitación de la Comisión Europea para brindar recomendaciones sobre temas relacionados con el mundo de las finanzas digitales. El informe proporciona algunas recomendaciones intersectoriales y específicas de seguros para garantizar que el marco regulatorio y de supervisión de la UE se adapte a la era digital. Con referencia al mercado de seguros, EIOPA, en cooperación con las otras ESA, señala respecto al negocio asegurador a la luz de la digitalización como el artículo 18, apartado 1, letra a), de la Directiva Solvencia II establece que el objeto social de las empresas de seguros debe limitarse a «la actividad de seguros y las operaciones derivadas directamente de ella, con exclusión de cualquier otra actividad comercial». En la práctica, sin embargo, puede no ser tan fácil identificar cuáles de las actividades que no están estrictamente relacionadas con los seguros pueden ser realizadas por una compañía de seguros. Este no es un tema nuevo, pero parece surgir con especial frecuencia con el desarrollo de la digitalización y las InsurTech, lo que a su vez está asociado con un cambio de un modelo basado en la protección/cobertura de riesgos a uno más basado en la prevención/asesoramiento (como se ve, por ejemplo, en el mercado de riesgo cibernético). EIOPA reconoce que el citado artículo, al referirse también a las operaciones que «derivan directamente».
Este podría ser el caso, por ejemplo, de actividades puramente de desarrollo de software/API de TI realizadas directamente por la empresa, pero ofrecidas a otras aseguradoras o intermediarios (EIOPA da el ejemplo del intermediario que desarrolla

no implica, por otra parte, reconocer precisamente que el mundo o ámbito del seguro sea el más innovador[24].

Otra cuestión es si será capaz, o no, de acompañar todo ello, de una cierta cultura ética donde la opacidad o por su parte, las situaciones de vulnerabilidad digital hacia ciertos sectores sobre todo de consumo signifiquen vacíos, exclusiones o discriminación a través de esa interacción entre el dato y la inteligencia artificial[25].

su propia herramienta de comparación para uso interno, pero luego lo ofrece a otros intermediarios como un servicio de marca blanca).
Una posible solución podría ser que las actividades (digitales) directamente relacionadas con las actividades de seguros y los riesgos asegurados, como las dirigidas a los servicios de prevención o gestión de riesgos ofrecidos a los clientes (aplicaciones de salud, servicios de rehabilitación, coaching) se consideren actividades de seguros o auxiliares.

24. Señala OSTROWSKA, «Regulation of InsurTech: is the principle of proportionality an answer?», Risks, 19 de octubre de 2021: «No obstante, el sector de los seguros no se considera el más innovador y aún persiste la impresión de un enfoque anticuado y conservador por parte de las empresas de seguros. Las empresas de tecnología notaron el potencial sin explotar para innovar y comenzaron a desarrollar soluciones que mejorarían los servicios de seguros. Partiendo de apoyar a las aseguradoras tradicionales en el desarrollo de su negocio, las denominadas startups "InsurTech" iniciaron la revolución tecnológica en el mercado asegurador y se están convirtiendo en auténticos competidores de los servicios de seguros tradicionales. El término también describe a las empresas tecnológicas emergentes en el sector de los seguros, que aprovechan las nuevas tecnologías para brindar cobertura a una base de clientes con más conocimientos digitales».
25. En este sentido, advierte MINTY, «Ethics, data and insurance: 4 developments worth watching», 2017, (https://nft.nu/en/ethics-data-and-insurance-4-developments-worth-watching), como: «Un peligro para las aseguradoras es que a menudo se concentran mucho en su propia transformación y no toman en cuenta otras transformaciones que suceden a su alrededor». Los académicos han estado rastreando los cambios en la forma en que la sociedad piensa en los datos y han estado trabajando en un nuevo marco para la ética de los datos para reflejar esto. Al mismo tiempo, los reguladores de los servicios financieros también han estado sopesando opciones para su propia transformación.
Una primera ilustración de esto sucedió hace algunos años, cuando las preocupaciones en el Parlamento del Reino Unido sobre el perjuicio causado por el mercado de crédito a corto plazo dieron como resultado un nuevo pensamiento por parte del regulador. La Autoridad de Conducta Financiera adquirió datos de precios y productos de firmas de «préstamos de día de pago» que juntas representaban alrededor del 80% de ese mercado. Estos mil millones de puntos de datos se analizaron y modelaron para producir un conjunto de regulaciones de precios y productos que empujaron al mercado de manera bastante dramática hacia un camino más ético.
Lo que destacó este ejercicio fue que así como las aseguradoras pueden modelar los comportamientos de los consumidores para fijar el precio de sus productos y liquidar

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 adoptando[26].

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 consumidores[27]. Información y datos que eviten sesgos dis-

sus reclamaciones, el regulador podría extraer los datos del mercado de seguros y modelarlo de acuerdo con sus propias necesidades y objetivos. Se llama regulación panóptica y podría representar el camino futuro de la supervisión de seguros.
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».

26. 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 Paolo, 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 2017): Is Big Data steering insurance towards a Cliff or a superhighway? (https://cpdpconferences.net/cpdp2017.pdf).

27. Así, HAGAN, «Big Data, Big Questions-Insurers and Advanced Data Analytics», FINTECH L. REP. NL 2, 2018, n.° 1, pp. 21 y ss., donde describe las diferentes y diversas interactuaciones 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.

criminatorios, 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 ejemplo[28].

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 omnicomprensivo. 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 respecto por ejemplo a la selección o antiselección de un riesgo asegurable, es esencial.

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 en lo discriminatorio, 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

org/cipr_topics/topic_insurtech.htm [https://perma.cc/SRD3- ZA6X) (last updated Feb. 19, 2020).

28. Véase *in extenso*, TALESH/CUNNINGHAM, cit., p. 11 y ss.

indistintamente y como si fueren conceptos homónimos expresiones como igualdad, discriminación, asegurabilidad, intensidades, frecuencias, mutabilidades, variabilidad de riesgos, y hoy cómo no en la era de lo tecnológico, vocablos como digitalización, *big data*, inteligencia artificial, computación en la nube, etc., distan de ser, tanto por sus significados y significantes, miméticos[29]. Y en nuestro caso saber cómo impactan en el seguro. Pues esa interacción e intersección entre lo «caduco» y lo «rupturista», sigue discriminando, algo que no va a cambiar ni opacarse o realizar una vuelta atrás o regresión en el mercado del seguro[30]. Antes al contrario.

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 cumpliendo[31]. Y no solo en la contratación[32]. O en un modelo de negocio caduco y que necesariamente ha de aggiornarse ante nuevos avances disruptivos y en lo que no todo es, en puridad, inteligencia artificial.

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,

29. Advierte JUNQUEIRA, *Tratamento de dados pessoais*, 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 sistemas 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.
30. Así, TALESH/CUNNINGHAM, «The technologization of insurance», 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 ciberseguridad de las organizaciones y la capacidad de las aseguradoras para desempeñar un papel regulador positivo».
31. Sobre la función social del seguro, véase nuestro ensayo, VEIGA, *Función social, jurídica y económica del seguro*, Madrid, 2022, especialmente capítulo segundo.
32. 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).

su oferta, etc. Mas ¿qué es un algoritmo y cómo impacta el mismo en el mundo del seguro?[33]

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 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 dactiloscópicos.

Un interrogante necesario a la vez que todo parece reducirse al dato como elemento principial de una nueva era, la era del dato frente a la anterior actuaria 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 algorítimo ha de rendir cuentas[34]. 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 verdad[35].

33. 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.
34. 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.
35. 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 como 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

El reto de la transformación digital con el uso de la automatización y la inteligencia artificial, los desafíos de la ciberseguridad, 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 proyección[36]. Pero también para el derecho, máxime, rescribiendo conceptos y basamentos,

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.

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».

36. 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 como 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 como la IA no es un sistema perfecto, tiene fallas.

como el de, por ejemplo, otorgar o no personalidad jurídica a los agentes inteligentes, como los robots. El riesgo, evitará caer en una *slippery slope* o pendiente resbaladiza[37].

No son pocos los dilemas a los que nos enfrentamos y que estamos obligados a resolver, pero también a regular[38]. Entramos, ya lo hemos hecho en el

37. 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 como: «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 sólo 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 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. Sólo 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».

38. 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

análisis del riesgo, la prima y la gestión del siniestro, en el campo de la regulación algorítmica[39]. 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 conducta[40]. Sin obviar el enorme problema de la eticidad y la responsabilidad algorítmica[41].

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».

39. Así, en un papel 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), como: «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 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».

40. Sobre este re-etiquetado 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 concepto 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).

41. 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, *Tratamiento de dados pessoais e discriminação algorítmica nos* seguros, cit., p. 202 y 203.

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 criptográfico. O, pensemos, 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 con una clara finalidad selectiva o discriminatoria de perfiles o patrones de aseguramiento? ¿Quid con el peligro de una *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»[42].

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 siniestro[43]. 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 digital[44].

42. En este punto, de nuevo SNYDER, «A.I., Big data and the threat of proxy discrimination: a revolution in the U.S. insurance industry», 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.

43. El reto sin duda es, y pasa, por que 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.

44. En este punto, afirma PES, «L´assicurazione contro il rischio de 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

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 predectibilidad en esta nueva era de los datos frente a la anterior era actuarial ha dado un giro copernicano[45]. 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 automatizada[46].

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 experimentado y si lo hacen o sirvieren, ¿verdaderamente estas normas son neutras?[47]

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

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 sovrannazionali, 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».

45. 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».
46. Como bien aduce MUÑOZ PAREDES, «Seguros usage-based», 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.
47. Vid., sobre este reto sobre la necesidad de una regulación tenológicamente 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.

de un producto o proveen un asistente virtual[48]. 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 cara[49]. 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 prestaciones[50].

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 auditada[51]. No olvidemos que la inteligencia artificial se basa, ante todo,

48. 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 éste como una herramienta que cambia la forma de contratar el seguro y haciéndolo más cercano y atractivo para el perfil de clientes jóvenes.
49. Sobre estos asistentes véase la propia web de Zurich, (https://www.zurich.es/notas-prensa/zurich-lanza-azul-asistente-virtual-asegura-por-la-cara).
50. 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 pre-perfectiva como constante el seguro. Incide precisamente a los buscadores de atención en línea de proveedores de atención médica, así como también los topes 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=).
51. 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), como una toma de decisions más precisa, eficiente, justa y coherente es sin duda una gran ventaja. A diferencia de la toma de decisions 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 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

en la estadística[52]. Y que existen sesgos, se introducen, pero también prejuicio en los sistemas computacionales[53]. Pero ese uso, ese basarse «en» puede y ha

los datos que se introducen en estos algoritmos. Los datos históricos en justicia criminal, el reclutamiento 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, reforzandos estereortipos y, quizás, crear otros nuevos».

52. 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 sólo puede evaluar el futuro teniendo en cuenta el pasado. Las consideraciones normativas, en cambio, se rigen por lo contra fáctico. 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, «Discriminación 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.

53. Repárese cuando menos en el provocativo pero elocuente título del artículo de CHANDER, «The racist algorithm?», Michigan L. Rev., 2017, vol. 115, pp. 1023 y ss.,

de ser imparcial[54]. Mas no podemos llamarnos a equívocos, las posibilidades de **manipulación discriminatoria** son innegables al tiempo que innumerables[55].

Y aún 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[56]., por los que, hasta el presente, ha discurrido el quehacer asegurativo, desde una base o planta más tradicional, a otra, absolutamente disruptiva[57]. 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 programado[58].

donde pone de manifiesto en p. 1025 como corporaciones como Facebook posee una patente sobre un proceso por el que puede denegar un préstamo a un usuario en función de quiénes sean sus redes de contacto o amigos. O el caso de IBM que pretende ofrecer un algoritmo que distingue a los refugiados de los terroristas —«the sheep from the wolves»—. O el hecho de que los agentes y policía usan algoritmos de «policía predictiva» —predictive policing— de cara a identificar a «hot people» quiénes a priori serían más propensas a cometer delitos.

54. 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».

55. 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-ofmachine-learning-a-provocation/ (https://perma.cc/XSS9-2D58), p. 82 cuando señala como los algoritmos de búsqueda de Google y los algoritmos de presentación de Facebook, determinan la información que vemos.

56. 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 intersante artículo de KOSS, «Leveraging Predictive Policing Algorithms to Restore Fourth Amendment Protections in High-Crime Areas in a Post-Wardlow 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.

57. Así señala MUÑOZ PAREDES, «Seguros usage-based», 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.

58. Correctamente señala LAZCOZ, cit., p. 284 «... se trata de complejos modelos algorítmicos que, frente a la programación clásica, tienen la capacidad de «aprender» en

Desde una era genuinamente actuarial a otra ingente y todavía no abarcable ni conceptual ni categóricamente en toda su intensidad, como es la era de los datos o la ciencia de los datos masivos. Así, por ejemplo, ¿acaso la selección del riesgo, *recte*, antiselección y discriminación, discurrirá por idénticos cauces como ha sido hasta el presente o supondrá, que lo está haciendo ya incipientemente, un cambio de paradigma? Y esta vez sí, empleamos en todo su significante esta expresión, cambio de paradigma, al que estamos asistiendo lenta pero inexorablemente en este intersector necesario entre tecnología y derecho y para el caso, en el derecho de seguros.

El acceso a datos, el conocimiento más intrínseco del riesgo, la capacidad cuántica de su procesamiento y análisis revoluciona sin duda la selección del riesgo y con ello, la causa del contrato mismo y la asegurabilidad de unos u otros riesgos donde la predectibilidad tradicional y parcial, deja paso a otro que se aproxima más a la certeza[59]. El cómo se haga, el cómo se obtengan, analicen, procesen y valoren esos datos de cara a medir y decidir el índice y grado de asegurabilidad puede, en suma, ser discriminatorio. Como lo es el acceso mismo a los datos, al análisis y la valoración en su resultado último.

Así las cosas, conscientes de esta realidad y, en aras a evitar estos errores, se han desarrollado las tecnologías de la «equidad de la inteligencia artificial» que no es sino un vehículo que permite adaptar a ésta a las restricciones matemáticas de la equidad[60]. ¿Por qué no blasonar un uso imparcial de la

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».

59. Vid., EIOPA, «Big data analytics in motor and health insurance: a thematic review», Luxembourg, 2019, pp. 35 y ss., en las que a EIOPA se le presentan por una aseguradora de automóviles más de 350 factores de riesgo en base a un modelo de predicción, pero en base al uso de informaciones tanto intrínsecas como extrínsecas y en las que se usa el análisis big data. Disponible este estudio-informe en (https://register.eiopa.europa.eu/Publications/EIOPA_BigDataAnalytics_ThematicReview_April2019.pdf). Un informe que nos recuerda en su p. 8: «The data used by insurance firms in the different stages of the insurance value chain may include personal data (e.g medical history) as well as non-personal data (e.g. hazard data), and it can be structured (e.g. survey, IoT data) or unstructured (e.g. pictures or e-mails). It can be obtained from internal sources (e.g. provided directly by the consumer to the firm) as well as from external sources (e.g. public databases or private data vendors)».

60. Clave sobre la equidad de la inteligencia artificial frente a sesgos y errores sistemáticos, VON ZAHN/FEUERRIEGEL/HUEHL, «The cost of fairness in AI: evidence from E-commerce», 7 de septiembre 2021, (https://link.springer.com/article/10.1007/s12599-021-00716-w). Y añaden: «La IA puede conducir a resultados dispares para las personas según ciertos datos sociodemográficos (género, raza u otros atributos considerados sensibles). En este caso, la IA puede conducir a la discriminación (Barocas y Selbst 2016). La evidencia empírica ha confirmado resultados dispares en una variedad de casos de uso de IA. En la calificación crediticia, se ha descubierto que AI niega solicitudes de préstamo de mujeres y minorías raciales a una tasa desproporcionadamente alta (Hardt et al. 2016). En el sistema de justicia penal, la IA se utiliza cada vez más para predecir el riesgo de reincidencia, pero ha clasificado falsamente a los acusados negros como «en riesgo» con más frecuencia que a los acusados que no son negros (Angwin et al. 2016). En el comercio electrónico, la IA se utiliza para personalizar las interacciones del sitio web y, sin embargo, se ha descubierto que los sistemas de IA muestran significativamente menos anuncios de trabajos bien remunerados para mujeres que para hombres (Datta et al. 2015; Lambrecht y Tucker 2019). Esto podría limitar el acceso de las mujeres a los recursos o dificultar los avances económicos.
Para superar los problemas de equidad en la IA, la literatura anterior ha desarrollado algoritmos para la llamada «equidad de la IA» (cf. Feuerriegel et al. 2020; Haas 2019). La equidad de la IA hace posible construir inferencias que satisfagan las definiciones matemáticas de equidad y que no conduzcan a resultados dispares para ciertas personas (Dwork et al. 2012; Hardt et al. 2016). Intuitivamente, podría parecer suficiente simplemente omitir los atributos confidenciales. Sin embargo, otros atributos pueden servir como proxy y, como resultado, la fuente de injusticia puede persistir (Barocas y Selbst 2016). Esto se ilustra mejor mediante un ejemplo. El salario puede servir como indicador indirecto del género. Por lo tanto, incluso si se elimina el género, la IA puede aprovechar uno de los proxies y, por lo tanto, conducir a resultados que discriminan por género. La equidad de la IA proporciona un remedio, que está diseñado para que se cumplan ciertas restricciones matemáticas en aras de la equidad.

inteligencia artificial que logre en suma neutras predicciones subyacentes y decisiones objetivas en base a los datos analizados?, ¿cómo se han de diseñar los algoritmos?[61]

61. Así, BORDEN/LEE/ROSS/HAILEMARIAM, *Minority report the ethics and impacts of algorithms*, 2019, (https://www.mcca.com/wp-content/uploads/2019/04/Minority-Report-The-Ethics-and-Impacts-of-Algorithms.pdf) señalan en p. 541 se interrogan: «¿Cómo pueden diseñarse los algoritmos para la sostenibilidad (de los mercados laborales, de las ciudades, etc.) y la equidad? Por ejemplo, para crear un mercado laboral, deben tenerse en cuenta las preocupaciones de todos los de ese mercado laboral, es decir, deben tenerse en cuenta las preocupaciones de todos los actores de ese mercado. Estos actores pueden ser los trabajadores, los empresarios, los propietarios de plataformas y los clientes. ¿Cómo deben ponderarse estas preocupaciones?
¿Cómo debería incorporarse la rendición de cuentas en estos sistemas para garantizar que los actores puedan recurrir cuando los algoritmos sean insostenibles o injustos?
¿Cómo pueden diseñarse las tecnologías a través de las cuales los algoritmos se diseñan para permitir la creación de sentido? ¿Cómo puede el diseño permitir a los usuarios comprender y actuar sobre la base de su comprensión de manera productiva, incluso cuando la complejidad total del algoritmo es total? ¿Cómo pueden diseñarse las tecnologías de forma que sean beneficiosas para los trabajadores y para todo el sistema?».

No en vano, en aras de evitar sesgos discriminatorios, se propone reformular la equidad algorítmica como una optimización restringida[62]. Mas otra cuestión bien distinta es que existan o se utilicen algoritmos que resulten de una discriminación por representación[63]. Y el objetivo es claro, evitar la asegurabilidad de ciertos clientes o sobre primar el coste del seguro en función de datos que, si bien no son, o tienen un contexto racial o de sexos, sí indican ciertas cualidades, circunstancias y hábitos del asegurado o potencial asegurado de cara a su exclusión final del seguro[64].

62. Este es el foco de estudio del trabajo de CORBETT-DAVIES/PIERSON, et. al., «Algorithmic decision making and the cost of fairness», 4 de agosto de 2017, (https://dl.acm.org/doi/10.1145/3097983.3098095), donde analizan un aspecto del sistema jurídico. A saber, los algoritmos se utilizan de forma habitual para decidir si los acusados en espera de juicio son demasiado peligrosos para ser devueltos a la comunidad. En algunos casos, los acusados de raza negra tienen muchas más probabilidades que los blancos de ser clasificados incorrectamente como de alto riesgo. Para mitigar estas disparidades, se han propuesto recientemente varias técnicas para lograr la equidad algorítmica. Aquí reformulamos la equidad algorítmica como una optimización restringida: el objetivo es maximizar la seguridad pública mientras se satisfacen las restricciones formales de equidad diseñadas para reducir las disparidades raciales. Demostramos que, para varias definiciones anteriores de equidad, los algoritmos óptimos resultantes requieren detener a los acusados por encima de los umbrales de riesgo específicos de la raza. Además, mostramos que el algoritmo óptimo sin restricciones requiere aplicar un único umbral uniforme a todos los acusados. El algoritmo sin restricciones maximiza así la seguridad pública, al tiempo que satisface una importante concepción de la igualdad: que todos los individuos sean sometidos a la misma norma, independientemente de su raza. Dado que los algoritmos óptimos restringidos y no restringidos suelen ser diferentes, existe una tensión entre la mejora de la seguridad pública y la satisfacción de las nociones predominantes de equidad algorítmica. Examinando los datos del condado de Broward (Florida), demostramos que esta disyuntiva puede ser grande en la práctica. Nos centramos en los algoritmos para la toma de decisiones sobre la libertad condicional, pero los principios que discutimos se aplican a otros dominios, y también a los responsables humanos que llevan a cabo reglas de decisión estructuradas.

63. No le falta razón a CHANDER, «The racist algorithm?», cit., p. 1025 cuando afirma: «Si sabemos que los resultados de un algoritmo son sistemáticamente discriminatorios, entonces sabemos lo suficiente como para tratar de rediseñar el algoritmo o desconfiar de sus resultados. La distinción es similar a la diferencia probatoria entre demostrar un trato dispar y demostrar un impacto dispar. Mi afirmación central es la siguiente: si creemos que los hechos del mundo real, en los que se entrenan y operan los algoritmos, están profundamente impregnados de discriminación injusta, entonces nuestra receta para el problema de los algoritmos racistas o sexistas es la acción afirmativa algorítmica. Por tanto, el problema no es la caja negra, que a menudo es más neutra que el que sustituye, sino el mundo real en el que opera. Debemos diseñar nuestros algoritmos para un mundo impregnado del legado de las discriminaciones del pasado y de la realidad de las discriminaciones del presente».

64. En este punto, es obligada la remisión a PRINCE/SCHWARCZ, «Proxy discrimination in the age of artificial intelligence and big data», Iowa Law Review, 2020, vol. 105, pp. 1257 y ss., quiénes ponen en valor el hecho de como esta gran revolución de datos plantea numerosos desafíos complejos para los regímenes contra la discriminación, como por ejemplo aquellos algoritmos diseñados incorrectamente o los datos erróneos pueden dañar de manera desproporcionada a subconjuntos discretos de población. Lo que no impide a censo contrario que incluso algoritmos correctamente diseñados o programados y con datos precisos puedan sin embargo reforzar patrones discriminatorios pasados.

Nunca como hasta el presente, se puede o ha podido, controlar el riesgo verdadero de un modo constante y actualizable a lo largo de la vida de ejecución de un contrato de seguro[65]. Riesgos que mutan, que se agravan o por el contrario relativizan su impacto e intensidad y con ello el coste último del seguro. Al tiempo que la propia tecnología es capaz *per se* de crear nuevos riesgos, silenciosos, pero con un efecto catastrófico ingente en daños como puede ser, de idéntica magnitud, el riesgo climático o una pandemia[66]. Sin obviar, como hoy, las empresas más tecnologizadas son capaces de controlar y monitorear como nadie el comportamiento del consumidor de seguros a

65. Afirman TALESH/CUNNIGHAM, «The technologization of insurance», cit., p. 21 que, aunque las insurtech son dinámicas y las correlaciones que descubren pueden utilizarse para cobrar de las aseguradoras, algunas de estas correlaciones están impulsadas por factores sobre los que el consumidor tiene poco control, lo que da lugar a un trato preferente por parte de la aseguradora. Es decir, los individuos con mayores factores de riesgo que normalmente se equilibran como parte del grupo de riesgo pueden perder su subsidio y terminar pagando primas más altas.
Las primas aumentan cuantos más factores de riesgo tenga un individuo, y con el uso de insurtech, la suscripción se realiza sobre la base de categorías de riesgo más pequeñas o segmentadas de grupos de riesgo.

66. No va desencaminada CASTRIOTTA, «A semantic framework for analyzing "silent cyber", Conn. Ins. L. J., 2021, vol. 27. n.º 2, pp. 68 y ss., p. 71 cuando afirma: «Podemos considerar la cuestión del "ciberespacio silencioso" de forma similar. El sector de los seguros ha desarrollado y mantenido un prolífico cuerpo de arquitectura contractual (pólizas) que ha creado un legado de productos de transferencia de riesgos significativos para los clientes. Entre esos productos está la relativamente emergente póliza de seguro cibernético diseñada específicamente para cubrir ciertos aspectos del llamado «riesgo cibernético». En su conjunto, el sector de los seguros ha pagado históricamente las pérdidas asociadas a sus productos de seguros y ha seguido siendo rentable. Como ocurre ocasionalmente en la comunidad arquitectónica, el sector de los seguros se encuentra con la apreciación emergente del alcance catastrófico de determinadas amenazas. En los últimos años, una de esas preocupaciones es el amplio alcance del riesgo cibernético y, con él, los temores sobre si el sector de los seguros será capaz de resistir un evento como un ataque de malware a la red eléctrica de Estados Unidos. Este temor se ve agravado por el reconocimiento de que la exposición cibernética "silenciosa" se extienda más allá del ámbito de las carteras de seguros cibernéticos mono línea y amenace la sostenibilidad de las líneas tradicionales de cobertura de seguros. En concreto, el sector está preocupado por los riesgos que no ha tenido en cuenta, y que no han sido adecuadamente valorados, por las pérdidas cibernéticas (de desgaste o de otro tipo)».

tiempo real, tanto en un escenario precontractual como constante el seguro lo que impacta tanto en el riesgo como en la tarificación del mismo[67].

El big data, el control o fiscalización de hábitos, costumbres, salud, comidas, conducciones, etc., la aplicación de dispositivos electrónicos que monitorean a través de relojes inteligentes, descargas de apps, o cualesquiera otros dispositivos, permiten esa sincronía perfecta entre riesgo y prima y romper con la asimetría riesgo declarado *versus* riesgo real.

Medir este impacto de la inteligencia artificial y el big data en un mayor «control» del riesgo del asegurado y sus hábitos saludables o fiscalización a través de wearables, ya es una realidad amén de posibilidad, otra cuestión es si generalizará y desde cuándo por todas las aseguradoras o en función de unos u otros productos[68]. No podemos soslayar que, el algoritmo, ha de entenderse e interpretarse en el contexto y entorno en el que mismo actúa[69]. Mas todo ello no impide ver con anteojeras y cuestionar, si cabe, impactos o restricciones negativas que, en último caso dimanan o pueden

67. Así las cosas, lo indubitado es que las insurtech pueden aumentar el control de las aseguradoras sobre el comportamiento de los asegurados. Con la cantidad de datos que las aseguradoras pueden aprovechar o incluso, pueden movilizar a los asegurados y obligar a los titulares de las pólizas a adoptar comportamientos que reduzcan el riesgo o a enfrentarse a tarifas más altas que inhiban la capacidad de mantener el seguro.
Muchas de las preocupaciones se derivan de no poder ver cómo la IA y los modelos predictivos, crean una enorme «caja negra» para los responsables políticos, los defensores de los consumidores y las partes interesadas. No tener un proceso transparente para entender cómo funcionan la tecnología y los macrodatos que estas tecnologías y modelos afectan sin duda a tener en último extremo un impacto dispar en las clases protegidas. Vif., TALESH/CUNNINGHAM, «The Technologization of insurance», cit., p. 23.

68. Las razones del éxito actual del algoritmo complejo se deben en palabras de LAZCOZ, cit., p. 284 en la capacidad para manejar ese número inabordable de variables que casa de forma idónea con la llamada «revolución del big data», que ha sido posible gracias a los desarrollos técnicos que permiten almacenar y procesar cantidades masivas de datos —también en la nube— de forma mucho más barata y rápida. Lo que además coincide con los avances en el campo del aprendizaje automático en sí, con particular incidencia en el aprendizaje profundo o *deep learning*.

69. En este sentido, capital el trabajo de RAHWAN/OBRADOVICH/CEBRIAN/BONGARD, «Machine behaviour», Nature, 2019, vol. 568, n.º 7753, p. 477. Las máquinas impulsadas por inteligencia artificial median cada vez más en nuestras interacciones sociales, culturales, económicas y políticas. Comprender el comportamiento de los sistemas de inteligencia artificial es esencial para nuestra capacidad de controlar sus acciones, aprovechar sus beneficios y minimizar sus daños. Los autores estudian el comportamiento de las máquinas que incorpore y amplíe la disciplina de la informática e incluya conocimientos de todas las ciencias.

dimanar de estas tecnologías. Desde la tutela del consumidor, la erosión en la bilateralidad negociada de los contratos, la imposición de ciertas coberturas versus exclusiones a cuestiones discriminatorias o anticompetitivas en último caso[70].

¿Qué recorrido tendrán los seguros *pay as you live*?, o planteado de otro modo, ¿cómo se ajustan las primas o coste del seguro al verdadero riesgo constante que día a día o por franjas temporales impacta en el asegurado?[71]

70. No es por tanto descabellado plantearse, por ejemplo, como a pesar de los resultados positivos que pueden aportar las insurtech, su uso también puede tener consecuencias negativas. Así, analizando y cuestionando este campo, señalan TALESH/CUNNIGHAM, cit., p. 19 y 20 como para empezar, hay preocupaciones con la calidad y la fiabilidad de los big data. Aunque los big data pueden ser útiles para encontrar correlaciones, pueden existir errores en los propios datos, especialmente si proceden de fuentes poco fiables que pueden sufrir cortes y otras pérdidas, a la hora de recopilar toda esa base de datos. De hecho, los macrodatos pueden estar plagados de errores debidos al sesgo de selección, inexactitud o juicio subjetivo, incluso cuando la información en sí es precisa. Incluso si los datos están limpios e imparciales, los algoritmos podrían encontrar erróneamente correlaciones con significación estadística que no tienen una conexión significativa entre las variables.

71. Destacan las pólizas que Hancock ofrece a través de sus programas «vitality program». Vid. el trabajo de MUÑOZ PAREDES, M.ª L., «¿Son ventajosos los seguros con monitorización del asegurado o sus bienes?», 1 de junio de 2021, (https://almacendederecho.org/son-ventajosos-los-seguros-con-monitorizacion-del-asegurado-o-de-sus-bienes), donde alude a este tipo de seguros «Pay as you drive», «Pay as you live» y que comercializan ya en España diversas aseguradoras con limitaciones o bien temporales, o bien de hábitos saludables, o bien a través de descuentos, franjas kilométricas, etc. Y ejemplifica el supuesto norteamericano: «En USA, *John Hancock*, aseguradora de vida con más de 150 años de antigüedad, introdujo en 2015 las pólizas de vida asociadas a hábitos saludables, a través del que denomina «*Vitality Program*», que tiene dos versiones, la básica («*Vitality Go*»), que se anuncia como gratuita, y la «premium» («*Vitality Plus*»), que requiere una aportación de dos dólares mensuales. Si se contrata el seguro de vida (temporal o entera), asociado a uno de estos programas, el asegurado obtiene descuentos en la prima, además de rebajas en compras en establecimientos comerciales asociados y otros regalos. Estos beneficios son mayores en el programa «premium» que en el básico y, a su vez, cuantos más puntos gane el asegurado, más descuentos y regalos obtendrá. Los puntos pueden ganarse mediante el cumplimiento de tareas físicas y también si se sigue una alimentación saludable, a cuyo efecto también proporcionan al asegurado descuentos en establecimientos por compra de comida saludable, buscando así la generación de un círculo virtuoso (pues los descuentos en comida saludable son mayores cuantos más puntos se obtengan precisamente por comer saludable). Para ganar los puntos, el asegurado puede registrar sus actividades a través de *wearables*, como el *Apple Watch*, que le vende la aseguradora con descuento, en una aplicación de móvil específica o bien *online* en la *web* de la aseguradora. No es obligatorio unirse a estos programas, pero quien contrate un seguro de salud sin asociarse a ellos no tendrá acceso a estas ventajas económicas. Por otro lado, *Hancock*

No todo ajuste de prima viene en función de un hábito o una conducta, un comportamiento continuado en el tiempo, también a través de otros mecanismos comerciales o prácticas asociadas al seguro pero que en nada entroncan con éste. Como son o pueden ser en función de ciertas conductas saludables, descuentos promocionales, o entregas de bonos canjeables en empresas donde se fomente precisamente ese comportamiento[72]. Pero en este supuesto y ante estas prácticas comerciales que en cierto modo premian la conducta del potencial asegurado ¿estamos ante una discriminación positiva que incentiva conductas que impactan a futuro en el riesgo y el siniestro?, ¿y al hacerlo, no se está despreciando o marginalizando a otro tipo de consumidores de seguros que, por las razones que fueren no acomete tales conductas?

Máxime partiendo del presupuesto cierto que, al basarse fundamentalmente en datos y generar coberturas o productos de seguros anclado, sobre todo en predicciones que esos mismos datos arrojan, toda vez que son analizadas desde el algoritmo, están llamados a reconfigurar —quizás revolucionar— el propio contrato de seguro y sobre todo, su gestión y su siniestralidad. El seguro se basa ante todo y, sobre todo, en datos, tanto los que suministra el potencial asegurado, como la siniestralidad y antiselección de riesgos[73].

El control del riesgo puede, en seguros de auto, vida, hogar, etc., llegar a ser total y con ello el conocimiento del riesgo constante, en todo momento, con lo que el problema es, de un lado, la ajustabilidad y razonabilidad

dice expresamente que no se compromete a mantener los descuentos durante toda la vida y que podrá variarlos».

72. Existen así, portales de seguros de vida y salud que recompensan el ejercicio físico del asegurado o cliente. Se miden a través de una pulsera la actividad física, ya sean pasos, calorías, distancia o la calidad del sueño y a través de una app, (PuntoSeguro Fit) se superan x retos mensuales que, logrados, se obtienen tarjetas regalo de Amazon, suscripciones a Netflix o Spotify, escapadas de fin de semana, etc., vid., (https://www.puntoseguro.com/blog/puntoseguro-fit-la-app-de-seguros-de-vida-que-te-recompensa-por-estar-sano/). La participación en el resto se basa en, primero, contratar un seguro de vida o de salud en PuntoSeguro, segundo, descargar la app en google play o en apple health y, finalmente, superar el reto propuesto cada mes.

73. Destaca MUÑOZ PAREDES, M.ª L., ««Big data» y contrato de seguro: los datos generados por los asegurados y su utilización por los aseguradores», *cit.*, pp. 129 y ss., los tres momentos vitales en los que los datos pasan a un primer plano, a saber, cuando las aseguradoras diseñan sus pólizas y se apoyan en los siniestros pasados de cara a determinar la probabilidad de que el futuro ese siniestro vuelva a ocurrir, cuando recaban datos del cliente, datos personales para concretar el riesgo y, por último cuando se produce un siniestro y vuelven a recoger datos sobre las circunstancias y consecuencias del mismo.

de los márgenes reales del coste del seguro al efectivo riesgo asumido por la aseguradora y, segundo, una potencial propensión a formas nuevas de discriminación.

Productos más transparentes, menos arbitrarios y, ajustados en esa ecuación riesgo *versus* prima a una realidad perfecta[74]. Los datos son, con frecuencia, imperfectos en algunas de las manifestaciones o dimensiones en que se presentan, por lo que es posible que el algoritmo herede ese sesgo o prejuicios de los que tomaron decisiones con anterioridad[75]. Desde un punto de vista estrictamente jurídico, pero no técnico ni económico, no somos aún conscientes los juristas del impacto que el big data tiene en todas las dimensiones del derecho contractual y la resolución de conflictos[76].

Otra cuestión será medir, además, la expansión del poder computacional de las nuevas tecnologías. Como también la enorme complejización que existe y trasciende en la realidad algorítmica[77]. Así como a los riesgos

74. Incide magistralmente en la reducción de la discrecionalidad que la inteligencia artificial puede conseguir HUERGO LORA, «Inteligencia artificial y regulación económica», *Inteligencia artificial y seguro de personas*, [VEIGA (Dir.)], Cizur Menor, 2022, (en prensa), sobre todo sabiendo como está, en la medida que algunas decisiones siendo discrecionales, pasarían a fundamentarse en datos, es decir, en predicciones basadas en datos y obtenidas a partir del análisis algorítmico de los mismos.

75. Afirman TALESH/CUNNIGHAM, «The technologization of insurance», cit., p. 21 como el aspecto de la personalización de la suscripción suscita muchas preocupaciones. La IA y los big data aumentan el riesgo de discriminación involuntaria, pero «racional» por delegación. Aunque las insurtech son dinámicas y las correlaciones que descubren pueden utilizarse para cobrar de las aseguradoras, algunas de estas correlaciones están impulsadas por factores sobre los que el consumidor tiene poco control, lo que da lugar a un trato preferente por parte de la aseguradora. Es decir, los individuos con mayores factores de riesgo que normalmente se equilibran como parte del grupo de riesgo pueden perder su subsidio y terminar pagando primas más altas. Las primas aumentan cuantos más factores de riesgo tenga un individuo, y con el uso de insurtech, la suscripción se realiza sobre la base de categorías de riesgo más pequeñas o segmentadas de grupos de riesgo.

76. Capital el trabajo de BAROCAS/SELBST, «Big Data´s Disparate Impact», Calif. L. Rev., 2016, n.º 104, pp. 671 y ss.

77. No en vano PASQUALE, *The black box society: the secret algorithms that control money and information*, Cambridge, 2015, p. 6 sostiene al referirse a los algoritmos hipercomplejos: «Real secrecy establishes a barrier between hidden control and unauthorized access to it. We use real secrecy daily when we look our doors or protect our e-mail with passwords. Legal secrecy obliges those privies to certain information to keep it secret; a bank employee is obliged both by statutory authority and by terms of employment not to reveal customer´s blances to his buddies. Obfuscation involves deliberate attempts at concealment when secrecy has been compromised. For example, a firm might respond to a request for information by delivering 30 million pages of

que son intrínsecos a esta revolución tecnológica y que han crecido exponencialmente en los últimos años y con un potencial de daño catastrófico difícilmente evaluable *ex ante*[78]. Un crecimiento que además, perfila el cariz del riesgo cibernético y el alcance real del daño cubierto y que afecta tanto a intereses propios tutelados en la póliza como a terceros que, por una acción u omisión del asegurado puede acarrear un daño[79]. La ciber póliza, lo

documents, forcing its investigator to waste time looking for a needle in a haystack. And the end result of both types of secrecy, and obfuscation, is opacity, my blanket term for remediable incomprehensibility».

78. Una buena retrospectiva de cómo se aseguraba a comienzos de la década de los noventa y qué riesgos asociados a lo cibernético que no pasaba de asegurar gastos en daños a la organización y la propiedad intelectual, a una posterior evolución hacia la cobertura de la interrupción de negocios, la extorsión cibernética, así como los costes de restauración del sistema, para asegurar hoy, sobre todo, en palabras de CASTRIOTTA, cit., p. 75: «Las ofertas cibernéticas actuales se dividen generalmente en tres partes conceptuales de cobertura: (1) coberturas de responsabilidad civil; (2) coberturas de primera parte; y (3) coberturas de interrupción del negocio (que son técnicamente coberturas de primera parte, pero de carácter específico de "elemento temporal"). Cada una de ellas responde a una variedad de incidentes cibernéticos
Los seguros a terceros responden a una variedad de incidentes cibernéticos, que van desde los ataques a la propia red, a los fallos del sistema y otras interrupciones, hasta los ataques al sistema de un proveedor de red. Las coberturas de terceros suelen ofrecerse de la siguiente manera: responsabilidad de privacidad y seguridad, responsabilidad de los medios de comunicación, cobertura reglamentaria, y cobertura del sector de las tarjetas de pago (o "PCI"). Según los tipos de productos y servicios ofrecidos por un posible asegurado, también puede ofrecerse un seguro adicional para cubrir la negligencia en relación con la tecnología desarrollada o integrada por el asegurado para un tercero. La cobertura a terceros incluye la respuesta a incidentes (incluidos los costes del centro de llamadas, la supervisión del crédito y costes de mitigación relacionados), extorsión cibernética y costes de restauración.
La parte de interrupción del negocio suele incluir la cobertura de los costes de interrupción del negocio debido a un evento cibernético, ya sea que el evento sea perpetrado sobre el propio titular de la póliza o una empresa de la que depende el asegurado. Esto suele incluir los costes de reputación asociados a un evento cibernético. En los últimos años, otra categoría de cobertura de primera parte se ha vuelto cada vez más común en las pólizas cibernéticas, cuyo propósito es reembolsar al asegurado por pérdidas financieras de naturaleza cuasi-criminal, como por ejemplo cuando un asegurado es víctima de la ingeniería social o de la manipulación de facturas».

79. Las coberturas son un buen lugar para encontrar una comprensión cabal de lo que la industria considera como pérdida cibernética cubierta o potencialmente cubierta. Por ejemplo, las coberturas de responsabilidad civil responden naturalmente a los costes legales y a los daños (sentencias, multas y sanciones, o acuerdos) que surgen de un evento cibernético. Las coberturas de primera parte nos indican con detalle las ciber pérdidas que puede sufrir una empresa. Por ejemplo, un acuerdo de seguro de respuesta a incidentes nos habla de los costes incurridos en servicios que se necesitan para responder cuando hay un incidente de seguridad o privacidad. Entre ellos se

cibernético, no cubre, empero el daño personal, así como tampoco cualquier tipo de daño material. normalmente se excluyen las lesiones corporales y los daños materiales.

De este modo, el tercero víctima no obtiene en estos seguros cibernéticos, que no están anclados sobre todo, en la filosofía y operatividad de los seguros de responsabilidad civil, un resarcimientos por daños corporales o lesiones, serán otras pólizas, con otras coberturas, típicas del seguro tradicional, como es una póliza general de responsabilidad civil general empresarial o profesional y donde en función del específico riesgo delimitado en la cobertura se trazará esa cobertura o no y hasta qué límite[80].

El riesgo viene porque esa inteligencia, o en realidad, el uso de la inteligencia artificial pueda sesgarse con datos y resultados discriminatorios, y caer en una caja negra algorítmica, carente de eticidad, con predicciones que conducen a la antiselección directa de malos riesgos asegurables, y donde la protección de datos y la regulación antidiscriminatoria lejos de interpretarse conjuntamente y desde una visión íntegra, caminen en polos o hacia polos

encuentran los asesores en materia de infracciones, los asesores en materia de privacidad, los servicios de supervisión del crédito de los clientes, los servicios forenses, etc. Los acuerdos de extorsión y restauración proporcionan cobertura para los pagos de ransomware realizados a los ciberdelincuentes y los costes de una empresa de ciberseguridad para restaurar los datos (y en algunos casos, el hardware). Y por último, las coberturas de interrupción del negocio nos dicen que las empresas pueden sufrir pérdidas de ingresos e incluso pérdidas contractuales u otras oportunidades de negocio debido a un evento cibernético. Cfr. CASTRIOTTA, cit., p. 76.

80. Ya hace una década afirmaba CLARKE, «Cyber liability: where to find cyber coverage», Insurance Journal, 28 de enero de 2013, (https://www.insurancejournal.com/magazines/mag-coverstory/2013/01/28/278213.htm), como algunos productos de seguros cibernéticos se combinan con pólizas de seguro de otro tipo, por ejemplo, seguro de responsabilidad por errores y omisiones de tecnología (EO). Y, hay alguna protección de seguro «cibernético» importante disponible en las pólizas de seguro que podrían no ser reconocidas inmediatamente como que brindan dicha cobertura. Un artículo donde el autor describía el proceso involucrado en la selección de una cobertura de seguro cibernético eficaz. Nos recuerda además como inicialmente estas pólizas eran costosas y contenían un lenguaje excluyente para situaciones tales como «falla en la instalación rápida de un parche de software», y el alcance de la cobertura se limitaba principalmente a alegaciones de seguridad y privacidad relacionadas con la electrónica. Los aseguradores expresaron su preocupación por la posibilidad de una agregación mundial de plantación de virus, piratería o problemas de red electrónica. Pero la cobertura evolucionó con la entrada de nuevas aseguradoras al mercado y con los esfuerzos para mejorar la cobertura. Pronto, estuvo disponible una amplia cobertura de primera parte (interrupción en el flujo de ingresos en línea) y el alcance de la cobertura de responsabilidad civil se amplió para brindar cobertura en una base de «toda la empresa».

divergentes y sin equidad alguna algorítmica[81]. Otra cuestión será abordar si el derecho antidiscriminatorio actuará frente a esos sesgos implícitos, aunque también frente a la inteligencia artificial[82].

O *a sensu contrario*, acaso no puede despojarse de cualquier significado, sobre todo legal, a conceptos o categorizaciones como la raza, la etnia, el género, la orientación sexual o la discapacidad, máxime si tenemos en cuenta que, en un principio de no discriminación, tales cualidades o circunstancias no deberían regir?[83] Sin embargo en el seguro, han primado hasta ahora de cara al sesgo y perfil del asegurado semejantes identidades o

81. Sobre esta dualidad normativa y necesidad de interpretar íntegramente el algoritmo en la protección de datos y la regulación antidiscriminatoria, en aras de la equidad digital y algorítmica, vid., el importante estudio de HACKER, «Teaching fairness to artificial intelligence: existing and novel strategies against algorithmic discrimination under EU law», Common Mark Law Rev., 2018, n.º 55, pp. 1143-1186. Para el autor, son evidentes las pruebas empíricas de que las aplicaciones de inteligencia artificial amenazan con discriminar a los grupos legalmente protegidos. Y el fallo está en que la legislación antidiscriminatoria de la UE no se adapta a la toma de decisiones algorítmica. Las víctimas, enfatiza en este trabajo el autor no podrán probar su caso sin acceso a los datos y los modelos algorítmicos. Casar protección de datos con la ley contra la discriminación es un gran reto, donde la equidad algorítmica está presente. El autor pone el foco de atención en la literatura informática sobre equidad algorítmica, en aras a integrar y sobre todo analizar conjuntamente la ley contra la discriminación con la protección de datos en aras a cumplir la equidad en la era digital. Para ello Hacker, muestra como los conceptos de la ley contra la discriminación pueden combinarse con auditorias algorítmicas y con evaluaciones de impacto de protección de datos en un esfuerzo por desbloquear la caja negra algorítmica.

82. Así afirma TISCHBIREK, «Artificial intelligence and discrimination: discriminating against discriminatory systems», *cit.*, p. 114: «La doctrina clásica de las discriminaciones directas y abiertas rara vez se aplicará a la IA discriminatoria: no es seguro que la IA muestre algo (funcionalmente) equivalente a la intención. Los programadores y/o usuarios de la IA no suelen actuar con malicia en los casos de IA discriminatoria, como hemos visto. Establecer la causalidad es, en su mayor parte, imposible. Sin embargo, tanto la causalidad imputada a través de los regímenes de carga de la prueba reforzada como el concepto de discriminación indirecta prometen ser, una vez más, herramientas eficaces. Si las estadísticas mostraran, por ejemplo, que el algoritmo de una compañía de seguros computa —en promedio— tarifas más altas para las mujeres que para los hombres, esto podría reconocerse, en primer lugar, como prueba circunstancial en el sentido del artículo 8 de la Directiva 2000/43/CE del Consejo. En segundo lugar, satisfaría el primer criterio del test de impacto dispar del TJUE. En consecuencia, corresponde a los usuarios de los mecanismos de decisión de la IA —en nuestro caso, la compañía de seguros— demostrar las pruebas exculpatorias y la justificación».

83. Sobre este punto, vid., BAER, «Chancen und Grenzen positive Mabnahmen nach § 5 AGG», Vortrag zum 6- Geburtstag des ADNB im TBB 2009, (https://www.rewi.hu-berlin.de/de/lf/ls/bae/w/files/ls_aktuelles/09_adnb_baer.pdf) pp. 1 y ss.

cualidades[84]. Otra cuestión, es canalizar y arbitrar las herramientas idóneas que permitan convertir datos no estructurados en inteligencia procesable[85].

No podemos los juristas obviar que la toma de decisiones algorítmica también puede conculcar el derecho a la no discriminación[86]. Sea tanto a

84. Sobre este combate ante la discriminación en el seguro, y desde un punto de vista ante todo tarifario, imprescindible el trabajo de DANIS-FATÔME, «La lutte contre la discrimination en droit des assurances», *La lutte contre les discriminations a l'epreuve de son effectivite: les obstacles à la reconnaissance juridique des discriminations*, [GRÜNDLER/THOUVENIN (Dirs.)], Paris, 2016, pp. 387 y ss.

85. Al respecto ya escribía en 2016, TUCKER, «Refugee or Terrorist? IBM Thinks Its Software Has the Answer», Def. One (Jan. 27, 2016), http://www.defenseone.com/technology/2016/01/refugee-or-terroristibm-thinks-its-software-has-answer/125484/ (https://perma.cc/S27J-KR6S), donde señala: «Las herramientas para convertir datos no estructurados en inteligencia procesable están mejorando, y eso podría alterar el cálculo de riesgo-recompensa en el centro del debate sobre la recopilación de datos. Tome el i2 Enterprise Insight Analysis de IBM, o i2 EIA. IBM compró i2 EIA en 2011 y agregó algunas de las capacidades informáticas cognitivas patentadas de la compañía, la más famosa de las cuales es Watson, la IA que venció al campeón de Jeopardy, Ken Jennings. IBM cree que la herramienta podría ayudar a los gobiernos a separar a los refugiados reales de los impostores, desenredar células terroristas o incluso predecir ataques con bombas. En octubre pasado, mientras muchos países europeos se esforzaban por hacer espacio para los refugiados sirios, otras naciones cerraban las puertas, diciendo que los atacantes de ISIS podrían intentar mezclarse entre la multitud. «Nuestro equipo mundial, algunas personas en Europa, estaban recibiendo comentarios de que había algunas preocupaciones de que dentro de estas poblaciones solicitantes de asilo que habían estado hambrientas y abatidas, había hombres en edad de pelear que salían de botes que se veían terriblemente saludables. ¿Fue eso un motivo de preocupación con respecto a ISIS y, de ser así, podría ser útil este tipo de solución?». dijo Andrew Borene, ejecutivo de iniciativas estratégicas de IBM.
IBM esperaba demostrar que el i2 EIA podía separar a las ovejas de los lobos: es decir, las masas de solicitantes de asilo inofensivos de los pocos que podrían estar conectados con el yihadismo o que simplemente mentían sobre sus identidades». Y más adelante ejemplifica: «Otro escenario que el grupo de Borene proyectó como parte de la manifestación involucró una bomba hipotética en una estación de tren, detonada por un mensaje de texto SMS. Utilizando metadatos telefónicos y SMS inventados pero realistas para un área urbana típica, un analista abrió un mapa, dibujó un círculo alrededor del área y, utilizando el momento exacto de la detonación, descubrió el número de teléfono que había enviado el texto. La búsqueda de ese número trajo inmediatamente más números de teléfono, direcciones de personas potencialmente conectadas, números de seguro social, todo relacionado con el número original».

86. No obstante, las nociones de raza, discapacidad, género, etc. se justifican como categorías sociológicas. Como tales, proporcionan al derecho antidiscriminatorio el vocabulario indispensable para describir las estructuras discriminatorias en primer lugar. Esto no es indiscutible, sobre todo en los estudiosos del derecho antidiscriminatorio europeos que en los estadounidenses. Es inevitable que, por el mero hecho de utilizar estos conceptos, el propio derecho antidiscriminatorio amenace con ahondar en una

través de la discriminación indirecta como la directa[87]. O ser, por tanto, un aliado en ese antiselección de riesgos que, *de facto*, bordea la línea entre las coberturas normales del riesgo y las desnaturalizaciones absolutas del riesgo asegurado y, por tanto, de la póliza[88].

forma de pensar divisoria en las mismas líneas que en realidad desea combatir. Cfr., TISCHBIREK, «Artificial intelligence and discrimination: discriminating against discriminatory systems», *cit.*, p. 115. Que añade en p. 116: «Por este dilema, Francia, sobre todo, se ha comprometido con una política de «ceguera racial». Esta política ha incluido recientemente una enmienda constitucional para eliminar el término «raza» del artículo 1 de la Constitución de la Quinta República, que anteriormente proclamaba «la igualdad de todos los ciudadanos ante la ley, sin distinción de origen, raza o religión». También en Alemania, el uso de la raza como término jurídico es muy discutido. La alternativa, sin embargo, es la amenaza de que el derecho antidiscriminatorio no tenga voz. Esto conlleva consecuencias también para los casos de IA discriminatoria. Si un demandante quisiera demostrar que un algoritmo actuarial perjudica a las personas de color a la hora de calcular las tarifas de los seguros, el propio requisito previo de su demanda es el reconocimiento legal del concepto (sociológico) de raza. Si la ley carece de los conceptos para señalar las discriminaciones, el principio de no discriminación no puede aplicarse efectivamente».

87. Vid., ZUIDERVEEN, «Strengthening legal protection against discrimination by algorithms and artificial intelligence», The International Journal of Human Rights, 2020, n.º 24, vol. 10, pp. 1 y ss.. La toma de decisiones algorítmica y otros tipos de inteligencia artificial (IA) se pueden utilizar para predecir quién cometerá un delito, quién será un buen empleado, quién no pagará un préstamo, etc. Sin embargo, la toma de decisiones algorítmica también puede amenazar los derechos humanos, como el derecho a la no discriminación. El documento evalúa la protección legal actual en Europa contra las decisiones algorítmicas discriminatorias. La ley de no discriminación, en particular a través del concepto de discriminación indirecta, prohíbe muchos tipos de discriminación algorítmica. La ley de protección de datos también podría ayudar a defender a las personas contra la discriminación. La aplicación adecuada de la ley de no discriminación y la ley de protección de datos podría ayudar a proteger a las personas. Sin embargo, el documento muestra que ambos instrumentos legales tienen severas debilidades cuando se aplican a la inteligencia artificial. El documento sugiere cómo se puede mejorar la aplicación de las normas actuales. El documento también explora si se necesitan reglas adicionales. El documento aboga por reglas específicas del sector, en lugar de generales, y describe un enfoque para regular la toma de decisiones algorítmica.

88. Advierten sobre la discriminación indirecta, PRINCE/SCHWARZ, cit., p. 1259 como sorprendentemente, sin embargo, una de las amenazas más importantes para los regímenes antidiscriminatorios que plantean los macrodatos y la IA está en gran parte inexplorada o mal entendida en la literatura legal existente. Este es el riesgo de que las IA modernas den como resultado una «discriminación por representación». La discriminación por representación es un subconjunto particularmente pernicioso de impacto dispar. Como todas las formas de impacto dispar, implica una práctica aparentemente neutral que daña desproporcionadamente a los miembros de una clase protegida. Pero una práctica que produce un impacto dispar solo equivale a discriminación indirecta

La clave de bóveda en este momento pasa, ineludiblemente en conocer el perímetro que en la clasificación de los riesgos hará la entidad aseguradora o la empresa o servicio *insurtech* de cara a sus propias estrategias de prevención y discriminación selectiva o antiselección[89].

El dato, el metadato, pero sobre todo, la posibilidad real de conocer y compartir, analizar y sistematizar millones de datos a un tiempo óptimo y aprender

cuando se cumple una segunda condición. En particular, la discriminación indirecta requiere que la utilidad para el discriminador de una práctica aparentemente neutra se derive, al menos en parte, del hecho mismo de que produce un impacto dispar. Esta condición puede cumplirse cuando el discriminador tiene la intención de impactar de manera dispar a un grupo protegido o cuando una característica legalmente prohibida predice los objetivos del discriminador en formas que no pueden ser capturadas más directamente por datos no sospechosos.
Esta distinción entre el impacto desigual generalizado y el fenómeno más específico de la discriminación de terceros se ilustra bien al postular una aseguradora de vida que utiliza una IA para fijar el precio de sus pólizas. Supongamos que el modelo generado por la IA de la aseguradora cobra más por la cobertura a los solicitantes que son miembros de un grupo de Facebook enfocado en aumentar la disponibilidad para los afroamericanos de las pruebas genéticas para las variantes de *BRCA*, que son altamente predictivas de ciertos tipos de cáncer. En estas circunstancias, es casi seguro que el asegurador estaría discriminando por poder para la información genética. En primer lugar, el modelo de precios de la IA presumiblemente afectaría de manera dispar a las personas con una predisposición genética al cáncer de mama y de ovario, ya que es relativamente probable que los miembros del grupo de Facebook tengan una conexión familiar con estos cánceres relacionados con *BRCA*. En segundo lugar, este vínculo entre la pertenencia al grupo de Facebook y la historia genética difícilmente sería fortuito. Por el contrario, presumiblemente sería la razón por la que la IA se aferró a la membresía en el grupo de Facebook al establecer las primas de los solicitantes. Enmarcando el punto en términos econométricos, los datos sobre la membresía de los solicitantes en el grupo de Facebook probablemente dejarían de ser predictivos de reclamos en un modelo que controlara las predisposiciones genéticas de los solicitantes al cáncer. Por el contrario, la aseguradora en este ejemplo probablemente no discriminaría por representación con respecto a la raza del titular de la póliza, incluso si los afroamericanos fueran perjudicados de manera desproporcionada por las acciones de la aseguradora. Sin duda, es plausible suponer que las acciones de la aseguradora afectaron de manera dispar a los afroamericanos dada la naturaleza específica de raza del grupo de Facebook. Aun así, el poder predictivo de la pertenencia de los solicitantes al grupo probablemente no tendría nada que ver con la correlación entre dicha pertenencia y la raza de los solicitantes. En cambio, el impacto dispar que sienten los afroamericanos sería meramente fortuito. Una vez más, enmarcando este punto en términos econométricos, la membresía de los solicitantes en el grupo de Facebook sería igualmente predictiva de futuras reclamaciones de seguros, incluso en un modelo que controlara la raza de los solicitantes.

89. Esencial en este apartado el trabajo de JUNQUEIRA, *Tratamento de dados pessoais e discriminaçâo algorítmica nos seguros*, São Paulo, 2020, pp. 274 y ss.

de ese conocimiento y la utilización de algoritmos es la clave de bóveda que actúa como motor y palanca de múltiples vectores asociados a esta inercia y que están evolucionando vertiginosamente[90]. Y, de un modo inconsciente para el consumidor, quién sufre las consecuencias de una brecha digital que hasta el presente, no ha distinguido la insuficiente capacidad y cognoscibilidad de consumidores *in potentia* que son vulnerables al conocimiento tecnológico y a operar digitalmente, la práctica desarrolla que esa ingente cantidad de datos acaba perfilando patrones y tipologías de posibles asegurados que, junto al riesgo y su capacidad económica, crearán productos potencialmente sesgados para unos u otros tipos de clientes[91].

90. Pasquale utiliza dos sorprendentes metáforas platónicas para ilustrar sus preocupaciones. En primer lugar, considera que la industria de los datos lleva un anillo de invisibilidad: «Las personas que están dentro de la caja negra están protegidos como si llevaran un anillo de Gyges, que otorga a sus portadores la invisibilidad, pero que, como nos advierte Platón en La República, es también una invitación abierta al mal comportamiento» (p. 190). En segundo lugar, Pasquale plantea que el resto de nosotros, la gente común, como prisioneros en la alegoría de la caverna de Platón, obligados a mirar a una pared pétrea «con sombras parpadeantes proyectadas por un fuego a sus espaldas» (p. 190) Pasquale concluye: (Los prisioneros de la caverna) no podemos comprender las acciones, y mucho menos la de los que crean las imágenes que son todo lo que conocemos de la realidad. Como los que se contentan con utilizar la tecnología de la caja negra sin AI igual que los que se contentan con utilizar la tecnología de la caja negra sin entenderla, (podemos) ver resultados hipnotizantes, pero (no) tenemos manera de protegernos de la manipulación o la explotación (p. 190). Vid., PASQUALE, «Bittersweet Mysteries of Machine Learning», cit., p. 190 y ss.

91. Así, analizando estos perfilados, sostiene MINTY, «Ethics, data and insurance», cit., «Otra consecuencia de todos esos datos que fluyen hacia las aseguradoras es la creación cada vez más automatizada de perfiles de consumidores para fines de seguros. La optimización de precios es una categoría de perfil de «capacidad de pago», pero es solo una de muchas. Se dice que una aseguradora tiene más de 1.000 factores de calificación solo para su cartera de automóviles, incluso si bebe agua del grifo o embotellada. ¡Parece que están apareciendo «correlaciones» relacionadas con el riesgo en todo tipo de lugares sorprendentes! Por lo tanto, no es de extrañar que los suscriptores hablen a menudo de que ya no saben cómo se calculan sus primas.
Sin embargo, esto viene con implicaciones éticas. A medida que la suscripción se vuelve cada vez más automatizada, a través de herramientas de inteligencia artificial como el aprendizaje automático, existe un mayor riesgo de que los consumidores experimenten resultados discriminatorios. Los aseguradores, naturalmente, protestarán diciendo que ese es un camino por el que ninguno de ellos consideraría seguir. Y algunos simplemente descartarían la posibilidad, sobre la base de que sus sistemas no están configurados de esa manera. Sin embargo, estas garantías serían prematuras si se tienen en cuenta dos factores.
En primer lugar, las aseguradoras quieren que sus algoritmos de aprendizaje automático les descubran nuevos conocimientos relacionados con el riesgo. Lo harán a través de herramientas como el agrupamiento de correlación, que analiza la relación

El acceso a la información, al dato, favorecerá una opción clara por la calidad y adaptabilidad real al riesgo de los asegurados, lo que será una gran ventaja competitiva. Mas todo ello no significa la sustitución o reemplazamiento del ser humano y la inteligencia humana frente a la artificial. Articular esta de momento complementariedad o yuxtaposición no será una cuestión ni sencilla ni menor. Ni tampoco significa erosionar o menoscabar un comportamiento ético, pues nada impide que la inteligencia artificial, aún tomando decisiones por sí misma, actúe conforme a patrones ética. Otra cuestión será cómo y por parte de quién se programarán esos patrones éticos.

Un interrogante necesario a la vez que todo parece reducirse al dato como elemento principal de una nueva era, la era del dato frente a la anterior actuaria intramuros el seguro. Interrogante que hemos de cerrar en una elipsis necesaria centrada, inequívocamente, en la eticidad y auditación del algoritmo que no es otro que plantear cómo el poder algorítimo ha de rendir cuentas[92].

Se trata de enmarcar el espacio en el que la inteligencia artificial coadyuvará y hará evolucionar decisiones, y en ello en base a predicciones, a suposiciones, a frecuencias, a correlaciones, etc., que la mente humana simplemente no puede llevar a cabo o, de hacerlo, consumiría ingentes cantidades de esfuerzo, tiempo y recursos. Piénsese en el *software* integrado en productos sanitarios[93].

entre los objetos de datos en lugar de la representación real de los objetos en sí. *De dicho análisis de conglomerados surge una pieza de «información fabricada» que el algoritmo luego aprende a asociar con ciertas identidades*. No se crea ningún campo de datos para esa información fabricada: el algoritmo simplemente la aprende».

92. 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.

93. Así distingue JABRI, cit., p. 315 entre el *embedded software* y el *stand-alone software*. Así, afirma: «producto sanitario y se comercializan junto con él se denominan programas informáticos integrados. Los programas informáticos integrados no son independientes, sino que se supone que controla todo el producto únicamente desde el punto de vista técnico, sin tener una finalidad médica en sí mismo. De acuerdo con los principios anteriores, el software integrado no es un producto sanitario. En cambio, el producto

Unas predicciones que han de basarse en un uso y reutilización ética de la inteligencia artificial, la cual, supone, y sobre todo, en un campo tan sensible como es el riesgo asegurable y los grupos de asegurados tan dispares, basarse en una cierta paridad estadística, esto es, aquella que parte de un presupuesto clave, esto es, la probabilidad de resultaos debe ser la misma en todo el grupo protegido (raza, sexo, mayores, discapacidad, solvencia, etc.)[94].

4. EL DATO Y LA DECISIÓN RACIONALIZADA POR EL PRISMA TECNOLÓGICO

El dato y la combinación matemática formulada a través de algoritmos son la base para adoptar decisiones «racionalizadas» a través de correla-

sanitario, incluido el software integrado, debe considerarse como un todo, tanto en lo que respecta al procedimiento de evaluación de la conformidad como al marcado CE. En otras palabras, el software integrado no está sujeto a su propio procedimiento de evaluación de la conformidad, de acuerdo con la sección 6(2) de la MPG, sino que se considera y se comprueba adecuadamente como parte del procedimiento de evaluación de la conformidad del producto principal. Por consiguiente, sólo se concede una marca CE, que cubre el producto sanitario en su totalidad. El software que controla el sistema de suministro de energía de un producto sanitario puede citarse como ejemplo de software integrado. Por regla general, no puede distribuirse por separado y mostrarse en ningún otro producto sanitario.
Software independiente
A diferencia del software integrado, el software autónomo no se incorpora a un producto sanitario, sino que puede utilizarse y distribuirse de forma independiente. Por este motivo, el software autónomo se menciona por separado en la sección 3 de las MPG. El factor decisivo para la calificación de autónomo es que el software no esté incorporado en un producto sanitario en el momento de su comercialización o puesta a disposición. Ciertamente, el software también puede utilizarse en combinación con el hardware mediante su integración en un sistema. Sin embargo, esto no altera la calificación del software».

94. Alegan VOZ ZAHN/FEUERRIGEL/KÜHL, «The cost of fairness», cit., La equidad en la IA se formaliza matemáticamente a través de las llamadas nociones de equidad, que miden las desviaciones de un resultado que se consideraría justo (Chouldechova y Roth 2020). Sin embargo, existen diferentes nociones y es matemáticamente imposible cumplir todas las nociones de equidad al mismo tiempo (Kleinberg et al. 2016). Por lo tanto, los profesionales de SI deben elegir una noción de equidad que sea apropiada para el caso de uso dado. Para una descripción detallada de las nociones de equidad, nos referimos a Barocas et al. (2019). A continuación, proporcionamos un breve resumen de dos nociones de equidad: i. es decir, paridad estadística y probabilidades igualadas, que son particularmente relevantes para la práctica de SI. Para esto, usamos la siguiente notación: nos referimos a la etiqueta predicha como $\hat{Y}$ Y^, la etiqueta real como Y y el atributo sensible como A. *La paridad estadística* (también llamada paridad demográfica e igualdad de paridad) requiere que la etiqueta pronosticada sea independiente del atributo sensible A (Dwork et al. 2012). En otras palabras, la probabilidad de resultados debe ser la misma en todo el grupo protegido (p. ej., usuarias) y fuera de él. Formalmente, esto viene dado por $\hat{Y}$».

ciones que permiten un conocimiento y una eficacia prácticamente ignota hasta el presente del verdadero valor del riesgo (en cualquier estadio del mismo, sea precontractual, contractual como post contractual) en el seguro, así como la gestión siniestral y resarcitorio[95].

Es cierto que, rápidamente empleemos, eso sí, convenientemente, una presuposición que no se explica o que para los profanos aparentemente se da como conocida pero que en realidad se ignora. En efecto, los datos, los miles o millones de datos son tratados o analizados por sistemas de inteligencia artificial, pero la pregunta es clara, a saber, ¿qué es eso, qué significa y cómo se lleva a cabo?[96]

El dato, el acceso al dato, el control y monitorización de los mismos, así como su análisis suponen en estos momentos un giro copernicano en la gestión íntegra del seguro e incluso de la asegurabilidad del riesgo. Esa combinación con la fórmula matemática, la explotación algorítmica de los datos supone un cambio de paradigma en la gestión del riesgo, que lo hacen más eficiente, más real pese a un componente inicial predictivo, y al mismo tiempo, sumamente flexible de cara su coste[97].

Datos que en todo lo atinente al comportamiento, la conducta social y profesional, el hábito deportivo, alimenticio, de consumo, de asistencia sanitaria o farmacológica, de cómo conduce o que multas o accidentes haya podido experimentar, de cuál es su capacidad de pago o crediticia, esperanza de vida, conocimiento de antecedentes hereditarios o genéticos, edad, domicilio o zona concreta, nivel de estudios, trabajos, redes sociales, etc., preconfigurar una predicción «etiquetada» o de datos etiquetados sobre los que trazar predicciones y correlaciones claves, de cara a lanzar productos de seguro muy concretos u ofertas a determinados grupos de personas con claves o patrones conductuales o de estatus muy similares[98].

95. No le falta razón a MUÑOZ PAREDES, M.ª L., «Big data» y contrato de seguro», cit., p. 130 cuando sostiene que el paso del uso de «simples datos» a «grandes datos» no es sólo una cuestión de volumen y variedad de fuentes, pues la utilización de nuevas tecnologías asociadas y el propio tratamiento de los datos origina problemas nuevos.
96. In extenso, sobre esta conceptualización e interacción entre big data e inteligencia artificial, vid., JUNQUEIRA, *Tratamiento de dados pessoais e discriminação algorítmica*, cit., pp. 200 y ss.
97. Como bien señala HUERGO LORA, «Inteligencia artificial», cit., «las predicciones algorítmicas suponen una forma distinta de aproximarse a un problema o de tomar una decisión».
98. Sin embargo, nos advierte CHANDER, «The racist algorithm?», cit., p. 1028 como dada la persistencia de la discriminación racial y de género generalizada en siglo XXI, ¿no deberíamos esperar que los algoritmos, a menudo programados por programadores

Un campo el de la digitalización que abre un espectro completamente nuevo y radical en cuanto a prestaciones, obligaciones y su modo de implementarlas. Quid si no, por ejemplo, con la simbiosis entre seguro y digitalización sanitaria[99].

La preselección de riesgos, de diagnósticos, incluso de coberturas, piénsese en la resonancia que advierte de una pequeña adenopatía sin que se sepa a ciencia cierta si es típica o atípica, reactiva o no, pero que a través del algoritmo se empiezan a extraer predicciones y en su caso, las decisiones últimas que la aseguradora sanitaria ha de realizar asistencialmente, o en una fase anterior, rechazar o no semejante cobertura[100]. El factor objetivado

racistas y sexistas, nos manipulen para que aceptemos decisiones racistas y sexistas? ¿Es probable que los programadores manipulen los algoritmos para exacerbar la discriminación existente en la sociedad? Por una media docena de razones, creo que tal y como hace Pasquale, debo señalar, no sugiere que haya programadores programadores deshonestos o jefes malignos, pero la preocupación por la manipulación algorítmica podría interpretarse así. Bien es verdad, sin embargo, que dado que gran parte de la discriminación social es subconsciente o inconsciente, es menos probable que se codifique en los algoritmos automatizados que en los responsables humanos de la toma de decisiones a los que los algoritmos sustituyen.

99. Imprescindible el estudio de CAMEDDA, «La digitalizzazione del mercato assicurativo: il caso della Digital Health Insurance», Rivista di Diritto Bancario, 2018/2019, pp. 567 y ss., y donde elabora el nuevo marco que nace en la tipología de los seguros de la salud que integran las tradicionales coberturas sanitarias con dispositivos tecnológicos de diversa naturaleza y presenta la ventaja de permitir a los asegurados una más eficiente y rápida fruición de las prestaciones garantizadas gracias al «spostamento del fulcro dell´assistenza verso il *self care* e il domicilio».

100. Consciente de las dificultades y reto que a la vez supone la inteligencia artificial en lo sanitario añade MOLNÁR-GÁBOR, cit., p. 339: «Sin embargo, en el contexto rutinario de la atención sanitaria de vida o muerte (y con frecuencia también en la investigación médica), la obtención de beneficios y la superación de las limitaciones suelen complicarse aún más por los retos relacionados con la comprensión de la enfermedad y la salud como temas centrales en la aplicación de cualquier sistema médico, incluidos los basados en la IA.
La IA persigue el objetivo de sistematizar el rendimiento perceptivo y mental del ser humano y ponerlo a su disposición a través de medios técnicos. Dado que los conceptos de enfermedad y salud combinan características descriptivas y normativas, no son cantidades o características objetivas o totalmente generalizables, sino que se basan en juicios de valor que están vinculados al respectivo contexto personal del afectado y al contexto sociocultural de la medicina per se. En la medida en que sus conceptos reúnen elementos físicos, psicológicos, sociales y culturales, su operacionalización a la hora de aplicar la IA presenta retos específicos. Fundamentalmente, la consideración de la autoevaluación de la persona afectada por la enfermedad como necesitada de ayuda —ahora o en el futuro— basada en la comprensión del bienestar subjetivo es un importante desafío en medicina. Este reto relacionado con la operacionalización de los conceptos de enfermedad y salud de la persona afectada se ve agravado por el

ha desplazado al factor subjetivo que salvo en la emoción o emotividad, es más incierto que aquél[101].

Pensemos por ejemplo todo el avance que puede suponer y, de facto, supone ya la telemedicina y sus avances, pero aspectos tales como la monitorización de pacientes, sobre todo, los crónicos a distancias o en entornos no urbanos y más despoblados o con dificultades de acceso y distancias y movilidad, a extremos tales como la inter operatividad, o el uso de inteligencia artificial de cara a optimizar procesos y por su parte información y compartirla codificadamente entre centros sanitarios, de diagnosis, de imagen, hospitales, etc., y lo que ello supone tanto para el sistema sanitario como para el seguro y sobre todo el bienestar del paciente asegurado[102].

La utilización de tecnologías digitales en la salud y la creación de productos de seguros donde la inteligencia artificial y su uso permiten sin duda una mayor calibración del riesgo a tiempo real, con una optimización de las primas ajustadas al verdadero impacto del riesgo, pero sobre todo, significa situar al asegurado en el centro de gravedad de nuevos modelos asisten-

hecho de que los sistemas médicos basados en la IA carecen de fórmulas cruciales que suelen aplicarse para superar este reto en los contextos médicos tradicionales, como la capacidad de darse cuenta de características humanas como la compasión y la empatía o la interpretación y el empleo adecuados del «conocimiento» social y la comunicación basada en información no medible de múltiples capas que luego debe incorporarse de forma creativa a la atención médica y a la planificación correspondiente. Además, estas fórmulas también se ven influidas por factores ajenos al estrecho contexto médico, como las valoraciones políticas y sociales de los conceptos de enfermedad y salud que se mezclan en los respectivos contextos culturales, de modo que su amplia generalizabilidad está expuesta a limitaciones».

101. Categórico afirma HUERGO LORA, «Inteligencia artificial», cit., «el algoritmo elimina el factor subjetivo (es una predicción, no un "pálpito") y, además, los factores objetivos que se tienen en cuenta son factores cuya relevancia está justificada por los hechos».

102. Señalan PRINCE/SCHWARCZ, «Proxy discrimination in the age of artificial intelligence and big data», cit., p. 1264 a propósito de las prohibiciones sobre el uso de características predictivas directas son particularmente importantes en la regulación de seguros. Por ejemplo, la Ley de Protección al Paciente y Cuidado de Salud Asequible («ACA») prohíbe a las aseguradoras discriminar en función del estado de salud.
Y la Ley de No Discriminación por Información Genética («GINA») prohíbe la discriminación por parte de las aseguradoras de salud cubiertas (y los empleadores, que a menudo brindan seguros de salud) sobre la base de la información genética.
Sin embargo, las características legalmente sospechosas también predicen directamente objetivos aparentemente neutrales fuera del entorno de seguros. Por lo tanto, los empleadores tienen prohibido considerar el sexo, la raza, la edad y la discapacidad en las decisiones de contratación, aunque estos factores pueden predecir directamente objetivos neutrales, como maximizar las horas trabajadas por los empleados o las ventas totales.

ciales más eficientes, más accesibles, y con un tratamiento más próximo en el tiempo. Otra cuestión será el uso de ese big data y su protección y confidencialidad en el ámbito sanitario[103].

Bascular entre la equidad y la discriminación a través de algoritmos que pueden no ser neutros, tiende y propende al sesgo[104]. Piénsese, además,

103. Véase la sugerente aportación de CAES, «Access to and re-use of government data and the use of big data in healthcare», *Regulating new technologies in uncertain times*, [REINS (Ed.)], Tilburg, 2019, pp. 193 y ss., cuando en p. 194 asevera: «El término "big data" hace referencia a conjuntos de datos de gran volumen, variedad y velocidad, cuyo procesamiento (es decir, la recopilación, el almacenamiento y el análisis) requiere una tecnología y unos métodos específicos. En el ámbito de la sanidad, estos conjuntos de datos pueden ser una herramienta para la toma de decisiones basada en pruebas por parte de los responsables de las políticas sanitarias, las instituciones y los fondos de seguros sanitarios, los hospitales y otros centros sanitarios, los profesionales de la salud y los pacientes. Por lo tanto, los conocimientos que ofrecen los macrodatos pueden contribuir a un sistema sanitario más eficiente y cualitativo.
Hay una gran variedad de tipos de datos valiosos para la asistencia sanitaria: datos de atención primaria y secundaria, datos de reclamaciones de seguros médicos, datos genéticos, datos administrativos, datos de sensores, datos de medios sociales, datos de salud pública, etc. Además, estos datos son almacenados y controlados por diversos actores, por ejemplo, profesionales y centros sanitarios, proveedores de seguros médicos, instituciones y organismos gubernamentales o empresas privadas. Pueden encontrarse en distintas bases de datos, que pueden estar abiertas al público, pero que en la mayoría de los casos sólo son accesibles bajo estrictas condiciones».

104. En este punto, contrasta en ese eje fairness/discrimination KELLER, *Big Data and Insurance: implications for innovation, competition and privacy*, The Geneva Association, 2018, (https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/big_data_and_insurance_-_implications_for_innovation_competition_and_privacy.pdf), p. 11 no pocas veces se ha argumentado que la elaboración de perfiles de los clientes puede socavar la equidad y crear efectos discriminatorios. Estas preocupaciones parecen especialmente relevantes en el sector de los seguros, ya que la elaboración de perfiles o la puntuación, —es decir, el riesgo individual o perfil de riesgo— constituye una característica inherente al modelo de negocio de los seguros.
El término «discriminación» se utiliza de forma diferente en el contexto de las distintas ciencias sociales. En economía, por ejemplo, no suele tener una connotación moral y se utiliza para describir un trato diferenciado, ya sea bueno o malo. En cambio, en la literatura jurídica, la «discriminación» suele considerarse como algo ilícito. En este caso, utilizamos el término de forma normativa, lo que implica que «los que deberían ser tratados igual no lo son». Evitar la discriminación implica, por tanto, que ciertas diferencias (como el género, la raza, orientación sexual, etc.) deben ser ignoradas. Por otra parte, la «discriminación» también incluye casos en los que «los que deberían ser tratados de forma diferente son tratados igual».
Esta definición de discriminación revela un dilema fundamental en el contexto de los seguros. Por un lado, los clientes de los seguros pueden ser tratados en función de

como el uso de las tecnologías y especialmente del análisis del *big data* puede generar una discriminación en la contratación en base a la optimización de los precios[105].

A la par que desencadenar toda una revolución en modelos asistenciales, cuidados, sanitarios, accesibilidad a pacientes en todo lo que es la telemedicina o telesalud y donde las barreras físicas se evaporan, y todo ello en base a datos, imágenes, tratamiento y procesación de las mismas, etc.[106], amén de entroncar en una fuerte raíz constitucional en base a la igualdad de oportunidades[107].

su riesgo individual, pero ello implica que los grupos protegidos pueden verse perjudicados si su riesgo es superior a la media. Por otro lado, no tratar a los individuos en función de su riesgo individual, implica que los grupos protegidos pueden verse perjudicados si su riesgo es superior a la media.

105. Evocativo el título del trabajo de DUENO, «Racist robots and the lack of legal remedies in the use of artificial intelligence healthcare», Conneticut Insurance L. J., 2021, vol. 27, pp. 337 y ss., y en el que examina la rápida aceleración del uso de la potente inteligencia artificial para tomar decisiones en materia de salud. La inteligencia artificial —asevera— promete muchas ventajas: una asistencia sanitaria asequible y accesible, precisión en los diagnósticos y la agilización de las tareas relacionadas con los procedimientos de autorización previa. Sin embargo, los peligros implican una discriminación indirecta, una forma insidiosa de impacto desigual, que implica prejuicios codificados inadvertidamente en que se codifican inadvertidamente en un algoritmo que perjudica de forma desproporcionada a los miembros de una clase protegida. Como la mayoría de los estadounidenses tienen un seguro de salud proporcionado por el empleador y regido por la Ley de Seguridad de Ingresos de Jubilación de los Empleados de 1974 (ERISA), este documento de los consumidores perjudicados por la discriminación por delegación. La historia de los seguros de salud explica por qué los seguros de salud proporcionados por el empleador se han disparado, lo que ha exacerbado la capacidad de crear un remedio adecuado. Este documento concluye que la legislación federal es para que nuestra estructura reguladora se adapte a la era de la informática.

106. Véase la sugerente aportación de CAES, «Access to and re-use of government data and the use of big data in healthcare», *cit.*, cuando en p. 194.

107. Así, sostiene POÇAS, «A lei 75/2021, o direito ao esquecimento e os seguros» Revista de direito comercial, 18-1-2022, pp. 127 y ss., parafraseando el artículo 13 de la constitución portuguesa p. 131: «... são ilícitas quaisquer discriminações arbitrárias ou carecidas de fundamento material, por parte de entidades públicas ou privadas, designadamente em função da ascendência, sexo, raça, língua, território de origem, religião, convicções políticas ou ideológicas, instrução, situação económica, condição social ou orientação sexual8. Abrangem-se tanto as discriminações diretas como indiretas (as que, assentando num critério aparentemente neutro, produzem efeitos materialmente infundados e desiguais para categorias de pessoas diversas)9. Por outro lado, o princípio da igualdade compreende a igualdade de oportunidades, ou seja, a criação pelo poder público —designadamente, por via legislativa— de fatores de discriminação positiva que colmatem uma desigualdade (de oportunidades) de facto, colocada no plano social, económico, cultural, etc».

La práctica no ignora, no puede hacerlo, la existencia de personas, de asegurados, con una mayor propensión o predisposición a ciertas enfermedades, o a sufrir un riesgo agravado de salud y que impacta de un modo severo en el seguro, sobre todo en los seguros de personas, vida y asistenciales. La tecnología, la genética, es evidente que puede ofrecer esos datos, esos cálculos, más allá de vanas conjeturas y vacuas predisposiciones, como el hecho mismo de condicionar el comportamiento conductual saludable de algunos asegurados a lo largo de la vida de la relación jurídica[108]. Todo bascula en torno al dato. Un dato y su uso al que no es exento la normatividad y sus límites regulatorios[109].

El uso y sobre todo, el uso ético del mismo, no es ni será en los próximos años una cuestión menor o irrelevante[110]. De la pasividad o ser un mero recipendiario de datos y cuestionarios suministrados por el potencial tomador/asegurado más las tablas de siniestralidad, se está pasando a un

108. En Portugal, tras la Ley 46/2006 que previene y prohíbe la discriminación directa o indirecta en razón de deficiencias o de riesgos agravados de salud, el impacto que esto puede tener en la contratación de seguros es capital. Así, POÇAS, cit., p. 134 entiende que un asegurado con riesgo agravado de salud es «que sofrem de toda e qualquer patologia que determine uma alteração orgânica ou funcional irreversível, de longa duração, evolutiva, potencialmente incapacitante, sem perspetiva de remissão completa e que altere a qualidade de vida do portador a nível físico, mental, emocional, social y económico sea causa potencial de invalidez precoce ou de significativa redução de esperança de vida». Y en los contratos ya existentes de seguro, afirma este impacto en p. 134 como «Por outro lado, o que preenche (ou não) a noção é a situação clínica objetiva da potencial pessoa segura, e não a política de seleção e avaliação do risco do segurador. Por outras palavras, o facto de a política de avaliação do risco, pelo segurador, determinar a aplicação de um sobreprémio a uma determinada patologia crónica não determina que a mesma seja qualificável como risco agravado de saúde, só o sendo se e na medida em que verifique os vários requisitos da noção lega».

109. Capital el libro editado por VOGL, *Big data law*, Cheltenham, 2021, sobre todo a partir de su capítulo segundo.

110. Sirva como botón de muestra el estudio de marzo de 2019 realizado por KPMG y UK Finance, Ethical use of customer data in a digital economy, (https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/ethical-use-customer-data-digital-economy). Sobre las ventajas de los seguros basados en datos, véase el excepcional estudio de MUÑOZ PAREDES, M.ª L., «Seguros *usage-based*: luces y sombras», *Inteligencia artificial y seguros de personas*, [VEIGA (Dir.)], Cizur Menor, 2022, (en prensa). Quien señala: «Con carácter general, todos los seguros basados en el uso, sea del ramo que sean y comporten la monitorización o no, propician la reducción del riesgo cubierto y eso de por sí es ya beneficioso para las partes del contrato, la comunidad de asegurados e incluso la sociedad en su conjunto. Este efecto es, sin duda, el más relevante de la adopción de este tipo de fórmulas y propicia que el seguro abandone su finalidad de cobertura pasiva de riesgos en pro de una función activa preventiva de siniestros, económicamente mucho más eficaz».

plano proactivo y pre-anticipativo. Y es que el uso masivo del dato cada vez genera relaciones y correlaciones más complejas y que impactan sin duda, en la medición última del riesgo y su control por parte de las aseguradoras[111]. A renglón seguido, no podemos dejar a un margen, toda eventual

111. En este sentido señala TISCHBIREK, «Artificial Intelligence and Discrimination», cit., p. 108 como: «mediante el uso de la IA, las correlaciones se vuelven mucho más complejas. A medida que el sistema se alimenta constantemente de datos, amplía continuamente su conjunto de patrones y aprende a idear nuevos modelos de agrupación de los datos para realizar evaluaciones de riesgo específicas para cada grupo cada vez más refinadas. Cuando se alimenta de datos relativos a los hábitos de compra, la IA puede aprender fácilmente a agrupar a las personas en categorías etiquetadas como A y B. Estas agrupaciones pueden corresponder con bastante precisión al sexo de las personas, aunque el sistema puede estar programado para ignorar cualquier dato directo sobre el sexo del solicitante. La IA puede aprender que las personas de la categoría A gastan más dinero en licores y cigarrillos que las de la categoría B. También puede aprender que las personas de la categoría B son más propensas a gastar dinero en medicamentos relacionados con el embarazo. Una vez alimentado con los datos de los clientes de la compañía de seguros, el algoritmo descubrirá rápidamente otras correlaciones bastante relevantes, incluso si los datos de los clientes son totalmente anónimos. El algoritmo podría aprender, por ejemplo, que las personas que reciben tratamiento por abuso de alcohol son clientes más baratos en el seguro médico (porque suelen morir más jóvenes) que las personas que dan a luz en un hospital al menos una vez en su vida. Como todos estos puntos se conectan automáticamente, no hay nadie que sospeche de estas correlaciones. La IA sólo sabe diferenciar entre los grupos A y B. No tiene ningún concepto de género. Aun así, es probable que el resultado de todas esas matemáticas sea un plan de seguros mucho más barato para las personas del clúster A que para la cohorte del grupo B. Además, como el algoritmo está en constante crecimiento y desarrollo, es posible que pronto sea capaz de llegar a correlaciones mucho más sofisticadas que las que acabamos de esbozar. A medida que estas correlaciones aumentan en complejidad, también se vuelven más y más opacas. Ni siquiera sus programadores —y mucho menos el solicitante medio de un plan de seguros— podrán seguir sus cálculos a un coste razonable». Y concluye el autor en p. 109: «Por todas estas razones, este último ejemplo de IA discriminatoria es la prueba definitiva de la eficacia de la doctrina del derecho antidiscriminatorio y de la estructuración jurídica de los procesos impulsados por la IA en general. Las soluciones técnicas al problema se ven obstaculizadas, ya que no existe —en sentido estricto— ningún problema técnico: los datos de entrada son representativos y completos. No se introduce ningún sesgo en el sistema en el sentido de que los factores perjudiciales, es decir, las diferencias en la esperanza de vida y en el «riesgo» de embarazo, están efectivamente distribuidos de forma desigual entre los sexos. Una corrección de los datos de entrenamiento no es posible, porque los datos de entrenamiento son correctos en primer lugar. Además, tampoco es prometedor eliminar el atributo sensible —en nuestro caso, el sexo— de la ecuación, ya que la IA puede «aprender» el sexo del solicitante de todos modos, como hemos visto. Al mismo tiempo, la configuración dinámica y siempre cambiante del algoritmo hace muy difícil —si no imposible— identificar retrospectivamente todos los factores decisivos en el cálculo de una tarifa de seguro específica».

responsabilidad civil en ese uso del dato o en la actuación de los agentes inteligentes. ¿Cuál es en suma la responsabilidad que se le puede exigir a los agentes inteligentes?[112]

5. UN DESIDERÁTUM REAL Y POSIBLE: LA TRANSPARENCIA ALGORÍTMICA. MÁS ALLÁ DE LA ETICIDAD

¿Será o está siendo la inteligencia artificial un mecanismo de transformación cual acicate de la transparencia y competitividad *per se* de la actividad aseguradora?[113] Parte del problema no es el desarrollo y expansión digital, sino el uso de esas formas, *rectius*, instrumentos digitales[114]. Piénsese a modo de ejemplo el revolucionario uso que la información, el big data, y no solo su generación, sino sobre todo, su procesamiento y análisis, miles o millones

112. Se plantea 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., «¿Qué son exactamente los agentes inteligentes en términos jurídicos? ¿O deberían tratarse estos sistemas como personas jurídicas, algo parecido a los seres humanos? En este artículo, aboga por un estatus «intermedio» que ofrece el derecho civil alemán: Teilrechtsfähigkeit, un estatus de subjetividad jurídica parcial basado en ciertas capacidades jurídicas. En su aplicación, los agentes inteligentes serían tratados como sujetos jurídicos en la medida en que este estatus siguiera a su función de servidores sofisticados. Esto desviaría el «riesgo de autonomía» y llenaría la mayoría de las «lagunas de responsabilidad» sin los efectos secundarios negativos de la plena personalidad jurídica. Sin embargo, teniendo en cuenta el ejemplo de los animales, es poco probable que los tribunales reconozcan la Teilrechtsfähigkeit a los agentes inteligentes por sí solos. Esto exige que el legislador dé un pequeño empujón, que yo llamo la «regla del animal invertido»: Debería quedar claro por ley que los agentes inteligentes no son personas, pero que aún así pueden tener ciertas capacidades legales consistentes con su función de servicio».

113. En este marco véase el trabajo de GIRGADO, «Las propuestas regulatorias de la inteligencia artificial en la Unión Europea y sus implicaciones jurídicas en el contrato de seguro», *Transparencia y competitividad en el mercado asegurador*, [GIRGADO/GONZÁLEZ (Coords.)], Granada, 2021, pp. 73 y ss.

114. En este punto matiza VERSIGLIONI, «Se l´algoritmo scrive la sentenza, che almeno rispetti la lógica», (www.Ilsole24ore.com), 11 febrero 2020, «En la era digital, y más aún en la perspectiva de la inteligencia artificial, los antiguos temas relacionados con la relación entre la ley y la máquina y la relación entre el hombre y la máquina adquieren una dimensión hasta ahora impensable e involucran a todas las ramas del derecho: desde lo civil a lo penal, desde lo administrativo a lo laboral, desde lo bancario a lo fiscal, desde lo nacional a lo internacional y así sucesivamente..... Y al observar la dialéctica resultante —que afecta a muchos campos como la defensa, la salud, las finanzas, la ética— uno tiene la sensación de que no es lo digital en sí mismo, sino más bien las formas americanas de utilizar lo digital lo que es motivo de preocupación en Europa, al menos en lo que respecta al derecho».

de datos que influyen sobre el riesgo declarado y que ha sido base y objeto del contrato, suponen respecto a viejas *santa sanctorum* del contrato y del derecho de seguros como es el deber de declarar el riesgo, precontractual en esencia, y el posterior frente a toda agravación del mismo conforme, precisamente a ese riesgo que sirvió de basamento para el seguro[115].

Esa accesibilidad y manejo de datos y su tratamiento correlacionado y baremado gracias al uso del algoritmo puede llegar a incluso a extremos donde el propio portador del riesgo, el asegurado o —*Risikoträger*— ignore la entidad y calidad de los mismos. De un riesgo radiografiado y fijo —en base a datos etiquetados— salvo por los deberes de comunicar conforme al declarado inicialmente, tanto sus agravaciones como disminuciones, se abre la puerta a un riesgo en permanente o constante adaptabilidad a la realidad lo que ha de llevar aparejada su traducción a un coste real y eficiente de la prima y su cálculo, cuestión esta más compleja de suyo.

A ello unamos, además, el conocimiento y transparencia de los algoritmos que se utilizan, amén de la finalidad última, el cómo se desarrollaron y emplean, cómo se usa y con qué finalidad esa información, cómo se procede, en aras de una transparencia óptima e informada, a un eventual derecho de explicación de los algoritmos a los interesados[116]. Amén de un nunca

115. Sostienen TALESH/CUNNINGHAM, cit., p. 18 como los defensores de las insurtech sostienen que tanto el big data y la tecnología mejoran la velocidad y la eficiencia en todas las etapas del ciclo del seguro, desde la comercialización hasta la suscripción, la prevención de siniestros y la gestión de los mismos. El modelo tradicional de seguros requiere de datos y aprobaciones entre múltiples personas de la compañía de seguros. Con la disponibilidad de big data y los avances tecnológicos, las aseguradoras pueden ahora utilizar métodos baratos para recopilar grandes cantidades de información al tiempo de procesar las reclamaciones. El Insurtech también permite la personalización de las prácticas de suscripción —y por lo tanto— optimización de los precios, en lugar de limitarse a identificar a un individuo dentro de las agrupaciones de riesgo y asignarle un precio que tenga en cuenta el conjunto, pero no el individuo. Más que evaluar el riesgo por la edad, el código postal y el historial de accidentes, el big data permite a las aseguradoras ampliar los tipos de información que intervienen en sus prácticas de fijación y suscripción de tarifas. En teoría, estas variables independientes tienen el poder potencial de poder de predecir los siniestros. En algunos casos, los asegurados podrían pagar primas más bajas que de otro modo no estarían disponibles para ellos.

116. Sobre la necesidad de una base de datos públicos de algoritmos en aras a alcanzar la transparencia, nos habla WITTNER, «A public database as a way towards more effective algorithm regulation», *Regulating new technologies in uncertain times*, [REINS (Ed.)], Tilburg, 2019, pp. 173 y ss., p. 183 cuando advierte como el ideal de transparencia pública puede realizarse mejor a través de una base de datos pública de los algoritmos de toma de decisiones utilizados comercialmente. En este caso, los diferentes tipos

devaluado derecho al olvido sobre ciertos datos y su no exportabilidad a terceros[117].

Mas no podemos llamarnos a equívocos, ¿es el uso del algoritmo transparente o, por el contrario, opaco?, ¿debería exigirse siempre y en todo caso, con cualquier tipo de automatización de datos el divulgarse o publicarse el código fuente del sistema de procesamiento? Y en este caso, ¿cómo se abre esta caja negra? Una caja negra que desvelaría sesgos, discriminaciones u otros posibles daños que el uso ineficiente y poco ético, opaco, acabaría generando[118]. No puede o no podemos ignorar como la ausencia última de control de un algoritmo integrado en las tecnologías digitales tienen la potencialidad de generar sesgos sociales, como también desinformación, lo que ha llevado a afirmar y alertar primero, ante el riesgo de fundamentalismo de los datos y, segundo, de la facticidad de auditar los algoritmos[119].

de información y datos de y sobre los algoritmos utilizados por las empresas podrían agregarse y compartirse a través de un sistema graduado con actores interesados y de confianza. En esta sección se rastrearán algunos de los modelos de papel para una base de datos de este tipo o formas similares de lograr la transparencia pública, se analizarán los detalles de cómo podría organizarse y diseñarse, se examinarán los límites legales, así como las disposiciones del RGPD que pueden (o podrían con algunas modificaciones menores) utilizarse de forma beneficiosa, y se revisará el impacto normativo en la sistemática del RGPD.

117. Sobre este derecho al olvido, POÇAS, «A lei 75/2021, o dereito o esquecimento», cit., pp. 145 y ss.

118. No más gráfico puede ser WISCHMEYER, «Artificial Intelligence and Transparency: opening the black box», *Regulating artificial intelligence*, [WISCHMEYER/ RADEMACHER/ (Eds.)], Cham, 2020, pp. 75 y ss., cuando afirma en p. 76 «While transparency has always been a general principle of data protection (cf. Article 5(1)(a) General Data Protection Directive-GDPR), law-makers around the globe are currently starting to experiment with specific transparency requirements for automated decision-making systems (ADMs), including AI-based systems. In 2017, law-makers in New York City proposed to oblige any city agency «that uses, for the purposes of targeting services to persons, imposing penalties upon persons or policing, an algorithm or any other method of automated processing system of data» to, inter alia, «publish on such agency's website, the source code of such system». In 2018, the German Conference of Information Commissioners called for new laws which would make it mandatory for public authorities and private actors employing ADMs to publish detailed information on the «logic» of the system, the classifiers and weights applied to the input data and the level of expertise of the system administrators».

119. No más claro y categórico puede ser el título del trabajo de GUSZCZA/RAHWAN/BIBLE/CEBRIAN/KATYAL, «Why we need to audit algorithm?», Harvard Business Review, 28 de noviembre de 2018, cuando sostienen como la auditoría de algoritmos debe ser interdisciplinaria para que tenga éxito. Debe integrar el escepticismo profesional con la metodología de las ciencias sociales y los conceptos de campos tales como la psicología, la economía del comportamiento, el diseño centrado en

Conviene, sin embargo, no dejar de lado que los procesos de tomas de decisiones de los sistemas basados en IA son, hasta cierto punto, absolutamente opacos y desconocidos por las personas sobre las que los datos arrojan información[120]. Mas, ¿puede o debemos mejor hablar y exigir una responsabilidad algorítmica?[121]

el ser humano y la ética. Un científico social pregunta no solo: «¿Cómo modelar y utilizar de manera óptima los patrones de estos datos?» pero pregunta además: «¿Es esta muestra de datos adecuadamente representativa de la realidad subyacente?» Un especialista en ética podría ir más allá al formular una pregunta como: «¿Es la distribución basada en la realidad actual la adecuada a utilizar?» Supongamos, por ejemplo, que la distribución actual de los empleados de nivel superior exitosos en una organización es desproporcionadamente masculina. La formación ingenua de un algoritmo de contratación sobre los datos que representan a esta población podría agravar, en lugar de mejorar, el problema.... ¿Se utiliza el algoritmo con un propósito engañoso? ¿Hay evidencia de sesgo interno o incompetencia en su diseño? ¿Indica adecuadamente cómo llega a sus recomendaciones e indica su nivel de confianza? Incluso si se lleva a cabo cuidadosamente, la auditoría de algoritmos seguirá planteando preguntas difíciles que solo la sociedad, a través de sus representantes electos y reguladores, puede responder. Por ejemplo, tomemos el ejemplo de la investigación de ProPublica sobre un algoritmo utilizado para decidir si una persona acusada de un delito debe ser liberada de la cárcel antes de su juicio. Los periodistas de ProPublica descubrieron que a los negros que no reincidieron se les asignaban puntuaciones de riesgo medio o alto con más frecuencia que a los blancos que no reincidieron. Intuitivamente, las diferentes tasas de falsos positivos sugieren un caso claro de sesgo racial algorítmico. Pero resultó que el algoritmo en realidad *lo hizo* satisfacen otro concepto importante de «equidad»: una puntuación alta significa aproximadamente la misma probabilidad de reincidencia, independientemente de la raza. Académico posterior investigación estableció que, en general, es imposible satisfacer simultáneamente ambos criterios de equidad. Como ilustra este episodio, los periodistas y activistas desempeñan un papel vital a la hora de informar a académicos, ciudadanos y encargados de formular políticas a medida que investigan y evalúan tales compensaciones. Sin embargo, la auditoría de algoritmos debe mantenerse distinta de estas actividades (esenciales).

120. Señala CHANDER, «The racist algorithm?», cit., p. 1029, como: «El programador no sólo debe dar instrucciones al ordenador con gran precisión, sino que dentro de las prácticas modernas de programación también requieren que el programador documente (o anote) lo que hace el programa. Debido a un proceso de programación que requiere tanto escribir instrucciones explícitas como documentar lo que hace el código, es menos probable que la discriminación inconsciente o subconsciente se acabe manifestando en la programación que, en definitiva, en la toma de decisiones humana».

121. Por su trascendencia y enfoque acertado, reproducimos la reflexión de MINTY, «Ethics, data and insurance», cit., cuando afirma: «Las aseguradoras siempre han sido responsables de cómo administran sus negocios. Esto podría ser para audiencias internas, como los directores independientes de la junta que representan los intereses de los inversionistas. Y esto también podría ser para audiencias externas, como el regulador.

El contenido, la potencialidad y extensión de los mismos que, indudablemente, distorsionará los viejos parámetros sobres los cuáles, hasta el presente hemos edificado el contrato y, especialmente, el contrato y estructura

Entonces, ¿cómo mantendrán esa responsabilidad las aseguradoras involucradas en esta transformación digital? Este es un desafío en dos niveles.
El primer nivel es relativamente práctico e involucra la rendición de cuentas y la responsabilidad. ¿Cómo juzgarán los directores no ejecutivos la veracidad de los proyectos de big data? ¿Tendrán acceso a la información correcta y la capacidad tanto para comprenderla como para cuestionarla y luego sopesar adecuadamente las respuestas? Esto es factible con algoritmos escritos a mano, pero ¿qué tan efectivo puede ser esto cuando se implementan algoritmos de autoaprendizaje? ¿Y qué sucede durante la transición de la toma de decisiones en gran parte humana a la toma de decisiones en gran medida algorítmica? ¿Cómo se asigna la responsabilidad?
He visto casos de cambios de política enormemente injustos que se atribuyen a «los datos,» ya que el elemento humano de una decisión transfiere la responsabilidad de un resultado injusto particular al elemento algorítmico. Sin embargo, ¿puede un agente artificial asumir responsabilidad moral? Eso es muy polémico. ¿Qué pasa con la alternativa: aceptará el elemento humano la responsabilidad por el comportamiento poco ético de sus procedimientos cada vez más autónomos?
Piensa en estas situaciones. En un entorno en el que las decisiones de suscripción se derivan de una combinación de participación algorítmica y humana, ¿debe aplicarse el código de ética de la empresa solo a lo último y no a lo primero? ¿Los valores éticos de su empresa se aplican solo al elemento humano y no al elemento algorítmico de «cómo se hacen las cosas aquí?» Y si ambos, ¿cómo se está poniendo esto en práctica?
A medida que se introducen algoritmos con cierto grado de capacidad de aprendizaje, ninguna persona tiene suficiente control sobre el aprendizaje de la máquina para poder asumir toda la responsabilidad por ellos. La naturaleza compleja y fluida de innumerables reglas para la toma de decisiones inhibe la supervisión. Y su diseño modular significa que ninguna persona o grupo podrá comprender completamente la forma en que un elemento algorítmico responde a otro. Por lo tanto, surge una brecha significativa entre el comportamiento del algoritmo y el sentido de responsabilidad por los resultados generados.
A lo que esto se suma es al considerable desafío de mantener la rendición de cuentas, no solo durante un período de transformación, sino de una transformación que en sí misma se construye alrededor de sistemas que hacen que sea más difícil hacerlo. Y es en torno a ese último punto que existe el segundo nivel de desafío para la rendición de cuentas.
El segundo nivel de desafío para la rendición de cuentas provendrá de los cambios que los datos y el análisis tienen en la cultura de las empresas. Esto sucederá de varias maneras, y describiré algunas de ellas aquí:

- La complejidad de la IA abrirá una brecha de responsabilidad entre las decisiones de las personas individuales y los efectos que producen esas decisiones. Aunque el perjuicio es evidente, los miembros de la compañía de seguros podrían dudar en verlo como su responsabilidad.
- Una dilución de la responsabilidad. Esa complejidad de la IA también puede hacer que las personas sientan que su aporte, su decisión, es tan marginal como para obviar cualquier responsabilidad por las consecuencias que resultan colectivamente. La opinión sería que «no pude haber hecho nada malo porque mi aporte ha sido muy marginal.»
- Un silo de responsabilidad. Esa complejidad también se traduce en una mayor compartimentación de acciones y decisiones sobre proyectos de IA. Es demasiado fácil para las personas, incapaces de ver cómo un resultado podría haber resultado de su silo particular, ignorarlo por completo.
- Un parpadeo de responsabilidad. Algunas personas piensan en cuestiones éticas solo en relación con los comportamientos de personas físicas reales. Como resultado, no logran ver, ni siquiera comprender, las implicaciones de las decisiones que toman en relación con la inteligencia «artificial».

del seguro. Sin que ello, mute o tergiverse la pretendida función social que todo contrato de seguro ha y debe cumplir en aras a una justicia natural del contrato entre las partes[122].

Es innegable que hoy existen nuevas formas de evaluar el riesgo, incluso puertas adentro del propio mundo digital, por ejemplo, ante los nuevos ciberataques[123]. Máxime en un momento en el que los ciberataques se intensifican de un modo exponencial, por ejemplo, en el secuestro de datos o ransomware, y alrededor de esto, la intensificación de sus costes. Y en una economía y actividad cada vez más interconectada y tecnologizada, ¿es o existe madurez cibernética en el asegurado? El saber, en suma, cómo opera y en qué marco concreto, la tecnología[124]. Tecnología desbordante de

122. En esta fusión entre lo tecnológico Insurtech y la digitalización sanitaria, afirma CAMEDDA, «La digitalizzazione del mercato assicurativo: il caso della Digital Health Insurance», cit., p. 568 como la oferta de modernas soluciones asegurativas más apegadas a los cambios de exigencias sanitarias de los ciudadanos, podría de hecho enfatizar la función social de los seguros de salud y su rol ad intra de los sistemas Welfare, contribuyendo a la prevención de las enfermedades y a la promoción de estilos de vida más sanos, «incoraggiandone» la adopción de descuentos sobre primas. Sobre la función social del seguro permítasenos la remisión a VEIGA, *Tratado del contrato de seguro*, 7.ª ed., tomo I, vol. I, Cizur Menor, 2021.
123. En el seguro, la disrupción digital apunta o apuntará en 2022 hacia áreas tales como: seguro médico y de viaje, potencialmente relacionado con pasaportes de vacunas y requisitos de viaje internacionales más complejos; productos que protegen contra los impactos de la crisis climática, como inundaciones, desastres naturales o eventos climáticos, donde estamos viendo un mayor uso de aprendizaje automático, seguros paramétricos y contratos inteligentes; y ciberseguro para respaldar la necesidad de una mayor protección digital, ya que todas las industrias experimentan una transformación similar. Vid., WILKINSON, «Digital disruption will accelerate in 2022», 1 de diciembre de 2021, (https://www.lexology.com/library/detail.aspx?g=0351c557-c870-480d-ac9f-8ad3f9a33657&utm_source=).
124. Categóricos afirman DEAKIN/MARKOU, «The law-technologie cycle and the future of work (March 2018)», University of Cambridge Faculty of Law Research Paper No. 32/2018. Available at SSRN: https://ssrn.com/abstract=3183061 or http://dx.doi.org/10.2139/ssrn.3183061, p. 6 afirman: «*technology never operates in a legal vacuum*».

continentes teóricos puramente jurídicos y que exigirán un desarrollo que va más allá de una mera adaptabilidad de éste a aquélla. ¿Se reinventará o simplemente evolucionará a la par el derecho y el ordenamiento?

Mas sin duda, inextricablemente unido a la serie de interrogantes precedentes, una de las claves de bóveda es que la tecnología irrumpa y revolucione las cadenas de valor del seguro sin que los esquemas tradicionales sean obstáculo, a lo sumo, una palanca evolutiva[125]; de modo que, ¿cómo a través de la inteligencia, del dato y del blockchain se puede redimensionar, agilizar y verticalizar el seguro y máxime, la cadena de valor?[126]

125. Así, afirma KELLER, *Big Data and Insurance: implications for innovation, competition and privacy*, The Geneva Association, 2018, (https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/big_data_and_insurance_-_implications_for_innovation_competition_and_privacy.pdf), p. 9: «Accordingly, a considerable amount of employee time is spent on processing data. There is therefore a great potential for automation of data processing. McKinsey estimates the automation potential to be 43 per cent of the time spent by finance and insurance employees. In non-life insurance, insurance fraud alone consumes almost 10 per cent of premiums».

126. Un buen ejemplo y del que posteriormente nos haremos de nuevo eco, viene de la mano de la plataforma Insurwave. Como señalan HINNIGAN/MURTAGH/SHERIDAN, «InsurTech», cit., Insurwave busca digitalizar la mayor parte posible de la cadena de valor de los seguros. Actualmente opera principalmente en seguros marítimos (es decir, un mercado de seguros complejo y de alto valor) y está buscando expandirse a otras partes del sector de seguros. Insurwave es una plataforma de software que crea un ecosistema digital para que los participantes en la cadena de valor del seguro (asegurados / corredores / (re) aseguradores) realicen transacciones entre ellos. El caso de negocio de Insurwave es que, en el corto y mediano plazo, automatiza y digitaliza el intercambio de información utilizando blockchain, por lo que existe un acuerdo mutuo y comprensión de la información importante entre los participantes en la cadena de valor (reduciendo así el tiempo / costo administrativo para actualización de información). Por ejemplo, la ubicación geográfica del barco en un momento dado podría afectar el costo de las primas dependiendo de si el barco se encuentra en aguas internacionales «seguras» o «peligrosas».
Tres ejemplos simples de cómo podría evolucionar el modelo de negocio de Insurwave ayudan a ilustrar cómo un pionero podría obtener ventajas cuando se trata de InsurTech:
- *Asegurados como clientes principales:* a los asegurados se les ofrece un servicio que les permite captar mejor los riesgos individuales y gestionar la administración de sus programas de seguros de manera más eficiente. Con el tiempo, los asegurados se vuelven menos dependientes de los corredores para ayudar con el programa de seguros y pueden trabajar directamente con los aseguradores del panel. Además, los proveedores de seguros podrían intercambiarse con fricciones reducidas si los asegurados tienen información de riesgo mejor y más estandarizada. Los programas de riesgo a medida podrían convertirse en un producto más mercantilizado que podrían suscribir más aseguradoras.
- *Corredores como clientes principales:* los corredores trabajan con Insurwave para ofrecer a los asegurados un mejor servicio que la competencia. Al ofrecer este servicio

De otra parte, esta nueva tecnología ayudará, o debería hacerlo, a cubrir aquellas fallas o carencias de coberturas o riesgos asegurables haciéndoles más cognoscibles, mensurables y, por ende, evaluables de cara a su asunción y tarificación[127]. Pero también el dinamismo de todos cuantos concurren en la esfera aseguradora, permitiendo y exigiendo el cumplimiento de requisitos, así como las propias prácticas comerciales al margen de que las mismas se evacuen o realicen en un escenario tradicional o digital[128].

mejorado y al trabajar con los asegurados para mejorar su programa de seguros, es difícil desplazar a los corredores.
- *Aseguradoras como clientes principales:* las aseguradoras ofrecen a los asegurados tarifas mejoradas si trabajan con la aseguradora para hacer que el proceso sea más eficiente y permitir que la aseguradora acceda a datos más personalizados sobre los riesgos específicos a los que están expuestos los asegurados. Las aseguradoras obtienen una ventaja competitiva sobre sus competidores y potencialmente desplazan a los intermediarios de los asegurados con respecto a algunas partes de la cadena de valor. La dependencia de los asegurados en un conjunto de servicios proporcionados por una aseguradora (en conjunto con Insurwave) podría dificultar el cambio de aseguradora, de la misma manera que algunas empresas de tecnología ofrecen un ecosistema de productos / servicios a sus clientes, lo que hace que sea atractivo no cambiar.

127. Por esta vía apunta entre otros, KELLER, *Big Data and Insurance: implications for innovation, competition and privacy*, cit., pp. 10 y ss.

128. No más clara puede ser la sentencia de 22 de septiembre de 2021 del Tribunal Regional Superior de Karlsruhe, y en la que la Federación de Consumidores alemanes demanda a un corredor que operaba a través de plataformas digitales comparativas. No se informaba expresamente a los visitantes de la web que la comparación se basaba en una limitación de pólizas de seguros y contratos antes de que se presentase la decisión final perfectiva. El Tribunal Regional Superior de Karlsruhe sostuvo que el acusado actuó injustamente en el sentido de las secciones 3 (a) de la Ley contra la competencia desleal (UWG) no indicando claramente que su comparación representaba solo una selección de aseguradoras y pólizas de seguros. La sección 3 (1) de la UWG prohíbe los actos comerciales desleales. El Tribunal decidió que la oferta de la comparación de seguros no vinculante constituía un «acto comercial» en el sentido de la sección 3 de la UWG. El Tribunal argumentó que, con la oferta de la comparación de seguros no vinculante, se pretendía preparar una transacción comercial porque a los usuarios de la plataforma de comparación se les mostró la posibilidad de un corretaje de seguros posterior por parte de la demandada.
El Tribunal sostuvo que el acusado había violado las disposiciones de los parágrafos 60 (1) y 60 (2) de la Ley de Contrato de Seguro (VVG). Según esta norma, los corredores de seguros están obligados a basar su asesoramiento en un «número suficiente» de aseguradoras y contratos de seguros ofertados en el mercado, para que puedan hacer una recomendación basada en criterios profesionales sobre qué contrato de seguro se adapta a las necesidades. del asegurado.
En segundo lugar, en opinión del Tribunal, el corredor no proporcionó una base suficiente para el asesoramiento, ya que su portal de comparación muestra solo aproximadamente la mitad de las aseguradoras en el mercado. El demandado, como corredor,

Tecnología en definitiva, que cambia incluso los patrones tradicionales de riesgo, la intensidad y frecuencia de los mismos, pudiendo ayudar a mitigarlos o reducirlos si se aplican dispositivos y sensores tecnológicos que facilitan información precisa e incluso autoejecutan ciertas instrucciones (casas inteligentes, relojes que miden la presión arterial y otros parámetros de salud, conducción inteligente y autónoma, internet de las cosas, etc.)[129]. Pero los algoritmos que se emplean en la inteligencia artificial actúan *ex ante*, para prevenir[130].

tenía la obligación básica de considerar en su asesoramiento a todas las aseguradoras del mercado (par. 60 (1) de la VVG). Un corredor está exento de esta obligación solo si señala claramente el hecho de que la selección de aseguradores es limitada (par. 60 (1), segunda oración).
Sin embargo, no era lo suficientemente transparente y claro colocar un aviso de este tipo solo detrás de un hipervínculo con una ventana emergente. Además, una referencia a «información para el consumidor», que a su vez contiene un enlace a «aseguradores participantes» y «no participantes», no puede ser una referencia expresa a un número limitado de aseguradores. Además, si un corredor decide basar su asesoramiento solo en un número limitado de aseguradoras y contratos, debe indicar, antes de la presentación de la declaración de contrato por parte del tomador del seguro, en qué mercado e información está prestando su servicio, así. como los nombres de las aseguradoras en las que se basa su asesoramiento. Esto requeriría más que enumerar las aseguradoras participantes; requeriría la participación de mercado y la importancia relativa de las empresas participantes en relación con las demás aseguradoras. Si el corredor no puede proporcionar esta información, debe estimarla y marcarla como una estimación. Comentan esta sentencia SCHILLING-SCHULZ/SCHEIFLER, «Transparency requirements for insurance brokers on comparison platforms», 14 de diciembre de 2021, (https://www.lexology.com/commentary/insurance/germany/arnecke-sibeth-dabelstein/transparency-requirements-for-insurance-brokers-on-comparison-platforms?utm_source=2bGeneral%2bsection&utm_campaign=Lexology%2bsubscriber%2bdaily%2bfeed&utm_content=Lexology%2b-Daily%2bNewsfeed%2b2021-12-15).

129. Concluyente MARTÍN, «Insurtech - not a zero sum game», cit., p. 62 indica además como la tecnología «is an enabler for the traditional insurance industry model to move from one of post-loss reactive reimbursement to one of proactively managing down customers´risks. The latter model of risk prevention is significantly more valuable and can change insurance from the grudge purchase that many customers view it as today. Increased personalization of the product will further the appeal».

130. Con razón DUENO, «Racist robots», cit., p. 347 afirma como los reguladores de seguros ya están realizando «auditorías de algoritmos», pero no están equipados para comprender los matices de los algoritmos de aprendizaje automático y sólo están preparados para responder una vez que se ha descubierto una disparidad. Los reguladores de seguros no son informáticos y no pueden examinar la IA ex ante para garantizar su seguridad. La IA está diseñada para predecir resultados futuros, por lo que, a menos que se desarrollen remedios legales ex ante, el daño sólo puede remediarse una vez que ya se ha producido.

Pero de cara a medir la fiabilidad de datos y la tecnología en su acceso y valoración, hagámonos la siguiente reflexión, a saber, ¿qué ocurre si se introduce un algoritmo errado sobre el impacto o incidencia del cáncer de piel por ejemplo en función de la raza o por el contrario sin tener en cuenta estadísticamente la probabilidad, así como la intensidad y tipificación de estas neoplasias en función de la raza? No podemos pues ignorar como los factores que, aunque lo hemos ido esbozando a lo largo del mismo, sí tiene entidad e intensidad propia a la hora de discriminación en el seguro, cuál es el de la raza, han de tenerse en cuenta *ex ante* o *ex post*, auditación del algoritmo, a la hora de realizar las predicciones y proyecciones.

¿Acaso no debemos evaluar críticamente el algoritmo?[131] Y no tanto por que, *per se*, puede conformarse como un colectivo o etnia que se discrimine como tal, cual por la propensión por ejemplo a sufrir determinados tipos de cáncer en función del color de la piel[132]. La inteligencia artificial a través

131. En este ámbito señala HUERGO LORA, «Inteligencia artificial», cit., al hablar de si los algoritmos son «conservadores» surge en ocasiones la necesidad de evaluarlos de forma que se vigile si todos los criterios utilizados para calcular la predicción son aceptables jurídicamente, y también para utilizar siempre datos actualizados, puesto que por ejemplo, en un contexto de progresiva paridad de sexos, utilizar datos antiguos puede llevar a que se reproduzcan patrones e reducida participación femenina. O que el algoritmo halle correlaciones a partir de factores que, como ocurre con la religión, el sexo o la raza, no puedan ser utilizados para otorgar un trato diferente y en ese caso será necesario prescindir de ellos.

132. Entre otros, véase el estudio de BRADFORD, «Skin center in skin of color», (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2757062/), donde señala como El cáncer de piel es la neoplasia maligna más común en los Estados Unidos y representa entre un 35 a 45% de todas las neoplasias en caucásicos (Ridky, 2007), 4 a 5% en hispanos, 2 a 4% en asiáticos y 1 a 2% en negros (Halder y Bridgeman-Shah, 1995; Gloster y Neal, 2006). La incidencia de cáncer de piel ha ido en aumento entre los caucásicos (Ridky, 2007), pero sigue siendo relativamente baja en las personas de color. Los datos han sido limitados para las poblaciones que no son de raza blanca, lo que dificulta la determinación precisa de la incidencia y la mortalidad. La baja incidencia de cánceres de piel en los grupos de piel más oscura se debe principalmente a la fotoprotección proporcionada por el aumento de la melanina epidérmica, que filtra el doble de radiación ultravioleta (UV) que en la epidermis de los caucásicos (Montagna y Carlisle, 1991). Los melanosomas más grandes y melanizados de los grupos de piel más oscura absorben y dispersan más energía que los melanosomas más pequeños de los caucásicos (Brenner y Hearing, 2008). Por lo tanto, la radiación ultravioleta, el factor predisponente más importante para el cáncer de piel en los caucásicos, juega un papel menor en las personas de color. Cuando el cáncer de piel se presenta en personas de color, los pacientes suelen presentar un estadio avanzado y, por lo tanto, un peor pronóstico en comparación con los pacientes caucásicos (Cormier et al, 2006; Hu et al, 2006). Además, ciertos tipos de cáncer de piel, como el dermatofibrosarcoma protuberans, predominan en las personas de color (Halder y Bridgeman-Shah, 1995). La distribución anatómica puede ser

del estudio de imágenes captadas por el propio asegurado o usuario, así como la introducción de ciertos algoritmos puede analizar precisamente imágenes conducentes a neoplasias[133]. Piénsese en el mero hecho de otor-

diferente o no a la observada en los caucásicos, según el tipo específico de cáncer de piel. El tratamiento es generalmente el mismo entre todos los grupos raciales. Las predicciones estiman que para el año 2050, los hispanos, asiáticos y negros representarán aproximadamente el 50% de la población de EE. UU. (Oficina del Censo 2000, Gloster y Neal, 2006). Por lo tanto, dada la presentación clínica a menudo atípica, la dificultad para detectar ciertas características como la variación del color en la piel oscura y la pigmentación de algunos cánceres de piel que generalmente no están pigmentados en los caucásicos, los médicos y otros profesionales de la salud deben mantener un alto grado de sospecha al examinar las lesiones cutáneas en personas de color (Halder y Bridgeman-Shah, 1995). En esta revisión, se analizarán las diferencias en los factores de riesgo, la presentación clínica y la mortalidad asociadas con los cánceres de piel en negros, asiáticos e hispanos en comparación con los caucásicos. Se incluirán las formas de cánceres de piel que pueden presentarse de manera atípica en personas de color y consisten en cáncer de células basales (BCC), cáncer de células escamosas (SCC), melanoma, linfoma cutáneo de células T (CTCL), sarcoma de Kaposi (KS) y dermatofibrosarcoma protuberans (DFSP).

133. Así, FREEMAN/DINNES/CHUCHU/TAKWOINGI/BAYLISS/MATIN/JAIN/WALTER/WILLIANS/DEEKS, «Algorithm Based Smartphone Apps to Assess Risk of Skin Cancer in Adults: Systematic Review of Diagnostic Accuracy Studies», BMJ, 10 de febrero de 2020, (https://www.bmj.com/content/368/bmj.m127), indican como hay varias tecnologías de diagnóstico disponibles para ayudar a los médicos generales y dermatólogos a identificar con precisión los melanomas al minimizar los retrasos en el diagnóstico. El éxito de estas tecnologías depende de que las personas con lesiones cutáneas nuevas o cambiantes busquen el asesoramiento temprano de los profesionales médicos. Se requieren intervenciones efectivas que orienten a las personas a buscar una evaluación médica adecuada.
Las aplicaciones para teléfonos inteligentes («aplicaciones») para el cáncer de piel brindan un enfoque tecnológico para ayudar a las personas con lesiones sospechosas a decidir si deben buscar atención médica adicional. Con los teléfonos inteligentes modernos que poseen la capacidad de capturar imágenes de alta calidad, se han desarrollado una gran cantidad de aplicaciones de «piel» con una variedad de usos. Estas aplicaciones para la piel pueden proporcionar un recurso de información, ayudar en el autoexamen de la piel, monitorear las condiciones de la piel y brindar consejos u orientación sobre si debe buscar atención médica. Entre 2014 y 2017, se identificaron 235 nuevas aplicaciones dermatológicas para teléfonos inteligentes.
Algunas aplicaciones de cáncer de piel funcionan enviando imágenes desde la cámara del teléfono inteligente a un profesional experimentado para su revisión, que es esencialmente un diagnóstico de tele dermatología basado en imágenes. Sin embargo, son de creciente interés las aplicaciones para teléfonos inteligentes que utilizan algoritmos incorporados (o «inteligencia artificial») que catalogan y clasifican imágenes de lesiones en alto o bajo riesgo de cáncer de piel (generalmente melanoma). Estas aplicaciones devuelven una evaluación de riesgos inmediata y una recomendación posterior al usuario. Las aplicaciones con algoritmos incorporados que hacen un reclamo médico ahora se clasifican como dispositivos médicos que requieren aprobación regulatoria.

gar, por ejemplo a través del algoritmo una puntuación x o y más baja o inferior a personas que poseen unas determinadas características físicas que además se identifican con grupos muy determinados por raza o por sexo, por lo que estamos ante una discriminación indirecta, pero conocida y que el algoritmo o su formulación matemática crea o que, curiosamente, puede sortear según se formule[134].

La práctica conoce errores de sesgo de género y tipos de piel en los sistemas comerciales de la inteligencia artificial. Así, en programas de análisis facial que se han comercializado se han descubierto sesgos y tasas de error para determinar el sexo de los hombres de piel clara y en piel oscura. En estos casos, en mujeres de piel más oscura, las tasas de error se disparan a un 34 %[135].

Piénsese además, como el uso de las tecnologías y especialmente del análisis del *big data* puede generar una discriminación en la contratación en base a la optimización de los precios[136]; y ello en base al análisis de la capacidad

Estas aplicaciones pueden ser dañinas si las recomendaciones son erróneas, especialmente si una falsa seguridad provoca retrasos en la obtención de una evaluación médica por parte de las personas. Se ha aplicado el marcado CE (Conformit Europenne) para permitir la distribución de dos aplicaciones basadas en algoritmos en Europa, una de las cuales también está disponible en Australia y Nueva Zelanda. Sin embargo, ninguna aplicación cuenta actualmente con la aprobación de la Administración de Drogas y Alimentos de los Estados Unidos (FDA) para permitir su distribución en los Estados Unidos y Canadá. Además, la Comisión Federal de Comercio de Estados Unidos ha multado a los especialistas en marketing de dos aplicaciones (MelApp y Mole Detective) por «afirmar engañosamente que las aplicaciones analizaron con precisión el riesgo de melanoma».

134. Correctamente HUERGO LORA, cit., señala como la utilización de algoritmos ayuda a objetivar decisiones, desplazado, en todo o en parte, a factores subjetivos que tradicionalmente vienen utilizándose para tomar decisiones. «Decisiones que se mueven en contextos de incertidumbre, puesto que si se tratara de decisiones que pudieran ser objetivadas en función de reglas calaras, no se plantea ni la discrecionalidad ni la inteligencia artificial».

135. Vid. HARDESTY, «Study finds gender and skin-type bias in commercial artificial-intelligence systems», 11 de febrero de 2018, (https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212).

136. Evocativo el título del trabajo de DUENO, «Racist robots and the lack of legal remedies in the use of artificial intelligence healthcare», Conneticut Insurance L. J., 2021, vol. 27, pp. 337 y ss., y en el que examina la rápida aceleración del uso de la potente inteligencia artificial para tomar decisiones en materia de salud. La inteligencia artificial —asevera— promete muchas ventajas: una asistencia sanitaria asequible y accesible, precisión en los diagnósticos y la agilización de las tareas relacionadas con los procedimientos de autorización previa. Sin embargo, los peligros implican una discriminación indirecta, una forma insidiosa de impacto desigual, que implica

crediticia, o del mismo lugar habitacional del asegurado, cuando no, una discriminación de entrada al seguro[137]. *A sensu contrario*, un eficaz manejo y gestión analítica de los datos puede hacer asegurables riesgos que hasta el presente no lo eran o en la práctica se hacían de un modo insuficiente[138]. El riesgo pasa a ser la discriminación algorítmica[139].

Entre los que se encuentra sin duda, un mayor conocimiento del riesgo, pero, sobre todo, de paso, un control más exhaustivo del mismo por parte de la entidad aseguradora. Ello implica un acercamiento más natural a la entidad del verdadero riesgo que una aseguradora está o puede asumir de modo real y constante durante toda la vida de la relación jurídica, lo que aboca, además, a una nivelación real del coste del seguro.

---

prejuicios codificados inadvertidamente en que se codifican inadvertidamente en un algoritmo que perjudica de forma desproporcionada a los miembros de una clase protegida. Como la mayoría de los estadounidenses tienen un seguro de salud proporcionado por el empleador y regido por la Ley de Seguridad de Ingresos de Jubilación de los Empleados de 1974 (ERISA), este documento de los consumidores perjudicados por la discriminación por delegación. La historia de los seguros de salud explica por qué los seguros de salud proporcionados por el empleador se han disparado, lo que ha exacerbado la capacidad de crear un remedio adecuado. Este documento concluye que la legislación federal es para que nuestra estructura reguladora se adapte a la era de la informática.

137. Sobre este punto, clave el artículo de MUÑOZ PAREDES, M.ª L., «La discriminación de los asegurados en el precio del contrato fijado con uso del big data», *Transparencia y competitividad en el mercado asegurador*, [GIRGADO/GONZÁLEZ (Coords.)], Granada, 2021, pp. 263 y ss., especialmente a partir de las pp. 274 y ss.
138. Sostiene KELLER, cit., p. 10 como los datos más detallados permiten a las aseguradoras ofrecer productos que se adaptan a las necesidades del asegurado, incluyendo seguros a la carta o propuestas de pago por uso. Este tipo de seguros basados en el uso garantizan que los consumidores paguen en función del riesgo real, por ejemplo, cuando conducen en lugar de cuando el coche está en el garaje. Una mejor comprensión de los riesgos también facilita el desarrollo de nuevos tipos de cobertura y mejora los riesgos existentes y emergentes (como el riesgo cibernético, por ejemplo). El mejor uso de los datos también puede permitir a las aseguradoras desarrollar productos de seguro para riesgos elevados que hasta ahora no se podían asegurar. Por ejemplo, los pacientes que padecen enfermedades hasta ahora no asegurables podrían compartir datos relacionados con su estado físico y beneficiarse de ofertas de atención individualizada. En resumen, los beneficios sociales y económicos del uso mejorado de los datos son mayores en las líneas de negocio en las que:
— el coste del riesgo moral y la selección adversa es elevado
— existe un gran potencial de reducción de riesgos mediante mitigación y prevención, y/o
— existe un alto grado de infraseguro.
139. Vid., SORIANO ARNANZ, *Data protection for the prevention of algorithmic discrimination*, Madrid, 2021.

Conocido en todo momento el riesgo y con capacidad de reacción sobre el mismo, ¿existen los mecanismos que se ajusten a una prima óptima constante y no *ex post*?[140]; ¿acaso debemos ignorar que en la práctica hasta ahora las variaciones de la prima o coste del seguro poco o nada tenían que ver en definitiva con el estado del riesgo? La base, no era el riesgo real, sino el riesgo declarado que podía ser más próximo o menos a la entidad verdadera del riesgo existente. No pocas veces demediado en el cálculo de coste en función de índices de siniestralidad o en la aplicación de bonificaciones-penalizaciones.

Y es que, a la postre, no van a ser pocas las actividades entrecruzadas además con una cobertura aseguradora, donde el dato, la incertidumbre y la toma de decisiones algorítmicas replanteen no sólo la actividad en sí misma profesional, piénsese en lo médico ya sea en diagnosis o en terapia, y en la que la metodología basada en ontologías soporta la creación de grandes bases de datos.

Tecnología en definitiva, como hemos hecho referencia en epígrafes anteriores, que cambia incluso los patrones tradicionales de riesgo, la intensidad y frecuencia de los mismos, pudiendo ayudar a mitigarlos o reducirlos si se aplican dispositivos y sensores tecnológicos que facilitan información precisa e incluso autoejecutan ciertas instrucciones (casas inteligentes, relojes que miden la presión arterial y otros parámetros de salud, conducción inteligente y autónoma, internet de las cosas, etc.)[141]. Pero los algoritmos que se emplean en la inteligencia artificial actúan *ex ante*, para prevenir[142].

---

140. Afirma y pone sobre el debate algo que hasta el presente era la pauta de comportamiento lógico entre las partes, a saber, MUÑOZ PAREDES, M.ª L., «Seguros *usage-based*», cit., «Así, lo habitual es que, hasta tiempos muy recientes, la aseguradora tuviera contacto con el cliente en el momento de contratar, en el de un eventual siniestro y en el momento de la renovación, pero no hubiera, por regla general, un contacto continuado. Pero, la introducción del *Big Data* en el seguro con la consiguiente digitalización del contrato ha propiciado que haya una mayor relación con la compañía. También 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, generalmente a través del uso de dispositivos telemáticos, lo que permite introducir también un sistema de reducción de primas diferente al legal, en principio más favorable al asegurado, por lo menos al asegurado que se implique en la disminución real del riesgo».
141. Concluyente MARTÍN, «Insurtech - not a zero sum game», cit., p. 62 indica además como la tecnología «is an enabler for the traditional insurance industry model to move from one of post-loss reactive reimbursement to one of proactively managing down customers´risks. The latter model of risk prevention is significantly more valuable and can change insurance from the grudge purchase that many customers view it as today. Increased personalization of the product will further the appeal».
142. Con razón DUENO, «Racist robots», cit., p. 347 afirma como los reguladores de seguros ya están realizando «auditorías de algoritmos», pero no están equipados para compren-

Ahora bien, ¿es fiable esa tecnología?[143], ¿puede exigirse una cierta eticidad o cuando menos que, quiénes la empleen se comporten éticamente y que, en su caso, respondan y rindan cuentas?[144] Pensemos en el supuesto de actuación de un pirata o hacker informático que tras un ataque de ran-

der los matices de los algoritmos de aprendizaje automático y sólo están preparados para responder una vez que se ha descubierto una disparidad. Los reguladores de seguros no son informáticos y no pueden examinar la IA ex ante para garantizar su seguridad. La IA está diseñada para predecir resultados futuros, por lo que, a menos que se desarrollen remedios legales ex ante, el daño sólo puede remediarse una vez que ya se ha producido.

143. Señalaba y aún hoy día siguen siendo sumamente actuales los argumentos de REIDENBERG, «Lex informática», cit., p. 582 «Los matices de Lex informática exigen que su uso sea un cuidadoso ejercicio. Por ejemplo, las reglas de política de información situadas en lo más profundo de la arquitectura de las redes, como las incorporadas a los protocolos de transmisión, tendrán más fuerza que las situadas a un nivel superior en los servidores o los ordenadores de los usuarios. Las opciones de nivel superior, en general, proporcionan más flexibilidad y mayor oportunidad de personalizar las políticas de flujo de información que las reglas diseñadas para todas las transmisiones de la red. Sin embargo, la flexibilidad de las configuraciones tecnológicas también significa que estas reglas tecnológicamente pueden ser eludidas. Si las opciones de configuración que establecen reglas se encuentran en el disco duro de un usuario, los usuarios pueden ser capaces de eludir la configuración y establecer una regla diferente. Por ejemplo, un adolescente podría instalar una nueva versión del software de navegación por Internet para eludir las restricciones parentales instaladas en el PC familiar. Sin embargo, si el software de la red incorpora una norma tecnológica, las posibilidades de eludirlas. Por ejemplo, un protocolo de red podría exigir que se incluyan códigos de contenido en todas las cadenas de datos: sólo la información con codificaciones seleccionadas se transmitiría al mismo adolescente que supiera cómo eludir el filtro de contenido local. En este caso, el adolescente no podría eludir la regla de la red.
El poder de Lex informática para incrustar reglas de orden público y no derogables en los sistemas de red no es benigno».

144. La Comunicación de la Comisión Europea de 8 de abril de 2019 establece entre los requisitos para generar una inteligencia artificial fiable, una serie de directrices, entre ellas, tal y como subraya en el apartado 2.1 la propia comunicación, se deben instaurar «mecanismos que garanticen la responsabilidad y la rendición de cuentas de los sistemas de IA y de sus resultados, tanto antes como después de su implementación. La posibilidad de auditar los sistemas de IA es fundamental, puesto que la evaluación de los sistemas de IA por parte de auditores internos y externos, y la disponibilidad de los informes de evaluación, contribuye en gran medida a la fiabilidad de la tecnología. La posibilidad de realizar auditorías externas debe garantizarse especialmente en aplicaciones que afecten a los derechos fundamentales, por ejemplo, las aplicaciones críticas para la seguridad». Y en ámbitos de responsabilidad téngase en cuenta el «Informe sobre responsabilidad derivada de la inteligencia artificial y otras tecnologías digitales emergentes» del Grupo de Expertos sobre responsabilidad y nuevas tecnologías de la Comisión Europea (Liability for Artificial Intelligence and other emerging digital technologies, Report from the Expert Group on Liability and New Technologies).

somware exige un pago voluntario, ¿es ético incluso para una aseguradora abonar estas actuaciones ilícitas y delictivas?[145] Más allá del embrujo y el

145. Este es el supuesto que plantea la sentencia de la Corte Suprema de Indiana de 18 de marzo de 2021, G&G Oil Co. of Ind. v. Contl» W. Ins. Co. 165 NE3d 82 (Ind. 2021), y en la que lo que se cuestiona en último término es si es asegurable un pago voluntario ¿Se puede asegurar o pagar a un pirata informático después de un ataque de ransomware en virtud de la cobertura de fraude informático de una póliza contra delitos comerciales? Ciertamente en no pocas ocasiones los ataques de ransomware están cubiertos por el seguro. En este caso, el asegurado no pudo acceder a su sistema informático debido a un ataque de ransomware y, finalmente, se puso en contacto con el hacker para negociar la liberación de sus servidores mediante el pago de cuatro bitcoins valorados en casi 35.000 dólares. Posteriormente, el asegurado presentó una reclamación de cobertura bajo su póliza, específicamente bajo la parte de cobertura de delitos comerciales de la disposición «Fraude informático», que cubría la pérdida «resultante directa del uso de cualquier computadora para causar una transferencia de dinero de manera fraudulenta». La aseguradora se negó a tal resarcimiento, afirmando que el asegurado rechazó la cobertura de piratería y virus informáticos. Debido a que Bitcoin se transfirió voluntariamente, el pirata informático no «transfirió fondos directamente» del asegurado. Se interpuso una acción de sentencia declaratoria, y ambas partes pidieron juicio sumario. En la apelación, la Corte Suprema de Indiana concluyó que la transferencia voluntaria de Bitcoin fue bajo coacción y no tan remota como para romper la cadena causal del ataque de ransomware y, por lo tanto, «resultó directamente del uso de una computadora». Sin embargo, el tribunal también examinó el término «causar una transferencia de manera fraudulenta» y concluyó que no era ambiguo y puede entenderse que significa «obtener por engaño». El tribunal señaló que la evidencia ante él sobre el evento iniciador de la piratería no era suficiente para determinar si la transferencia realmente se había obtenido mediante fraude o si los servidores del asegurado simplemente carecían de las garantías adecuadas. En última instancia, el caso se remitió para más procedimientos, pero esta es, sin embargo, una opinión favorable para los asegurados que están sujetos a ataques de ransomware. En última instancia, el caso se remitió para más procedimientos, pero esta es, sin embargo, una opinión favorable para los asegurados que están sujetos a ataques de ransomware. La Corte Suprema de Indiana concluyó que la transferencia voluntaria de Bitcoin fue bajo coacción y no tan remota como para romper la cadena causal del ataque de ransomware y, por lo tanto, «resultó directamente del uso de una computadora». Sin embargo, el tribunal también examinó el término «causar una transferencia de manera fraudulenta» y concluyó que no era ambiguo y puede entenderse que significa «obtener por engaño». El tribunal señaló que la evidencia ante él sobre el evento iniciador de la piratería no era suficiente para determinar si la transferencia realmente se había obtenido mediante fraude o si los servidores del asegurado simplemente carecían de las garantías adecuadas. En última instancia, el caso se remitió para más procedimientos, pero esta es, sin embargo, una opinión favorable para los asegurados que están sujetos a ataques de ransomware.
Como bien señala JORDAN, «Recent events highlight the importance of corporate entities assessing their cyber risk», 21 de mayo de 2021, (https://sdvlaw.com/insights/recent-events-highlight-the-importance-of-corporate-entities-assessing-their-cyber-risk), al comentar esta sentencia afirma: «El ataque cibernético de alto perfil en

asombro inicial de lo que pueden hacer por sí estas nuevas tecnologías, no podemos obviar que las mismas son capaces de generar por sí, bien sea la propia inteligencia artificial como el empleo de otras tecnologías emergentes tales como el internet de las cosas, la cadena de bloques, riesgos nuevos, incluso muy distintos o ignotos a los actuales, pero que nos permitirá a los juristas tensionar o saber qué grado de resistencia tienen los principios de

Colonial Pipeline Company es un recordatorio conmovedor de los riesgos nuevos y en constante evolución que enfrentan los asegurados corporativos. Además del riesgo de pérdida o daño por causas convencionales, como daño físico a la propiedad y el equipo, las empresas también deben contemplar su exposición a pérdidas relacionadas con transacciones electrónicas e información almacenada electrónicamente. Si bien las organizaciones prudentes toman nota y se comprometen a mejorar su ciberseguridad, un enfoque integral que maximice la protección debe incluir una consideración y un análisis cuidadosos de la cobertura de seguro. En el caso de Colonial Pipeline, la empresa fue víctima de un ataque de «ransomware», que presenta una categoría de malware que retiene los datos de una organización como rehenes, generalmente mediante el cifrado de los archivos, hasta que se realiza el pago. Se informó que Colonial Pipeline capituló y pagó a los piratas informáticos aproximadamente $ 5 millones en rescate. Afortunadamente, Colonial Pipeline puede tener pólizas de seguro cibernético, lo que podría ayudar a mitigar el impacto de este ataque en su negocio. Sin embargo, se desconocen los términos específicos de la cobertura. Sin embargo, preocupantemente, muchos en la industria de la energía y la energía renuncian a dicha cobertura. Una encuesta reciente de 125 empresas de petróleo y gas indicó que el 74 % no tiene seguro de ciberseguridad o cobertura para violaciones de datos, a pesar de que el 38 % de esas empresas aumentaron sus presupuestos de ciberseguridad en 2020. Si bien mejorar la infraestructura de TI de una organización es, sin duda, un componente esencial para protegerse contra las amenazas cibernéticas, la cobertura de seguros también es importante.
Desafortunadamente, obtener una cobertura de seguro adecuada puede ser un desafío. La capacidad ha disminuido y las primas son altas a medida que los transportistas se retiran del mercado. Por ejemplo, una de las mayores aseguradoras de Europa, AXA, ha anunciado que dejará de suscribir pólizas de ciberseguridad en Francia que reembolsan a los clientes por pagar a los atacantes. Además, la cobertura obtenida no cubre necesariamente todo el espectro de riesgos asociados con las lesiones cibernéticas. Dicho seguro a menudo tiene matices. Por ejemplo, es posible que una póliza cibernética que cubra pérdidas por fraude no se aplique a pérdidas por un incidente de ransomware, como lo que experimentó Colonial Pipeline Co. Un caso reciente relacionado con ransomware destaca cómo las aseguradoras pueden negar la cobertura bajo las disposiciones tradicionales de fraude informático para este tipo de ataques cibernéticos, argumentando que los ataques de ransomware son más «similares a un acto de robo que a un fraude» y que las exclusiones relacionadas con pérdidas por un virus informático o aplicar piratería. La Corte Suprema de Indiana finalmente anuló los fallos de los tribunales inferiores que apoyaban los argumentos de la aseguradora en lugar de determinar que la póliza cubre la pérdida. Sin embargo, el caso ilustra los desafíos que las empresas pueden enfrentar al presentar reclamos bajo pólizas cibernéticas por pérdidas relacionadas con computadoras».

responsabilidad civil y sus marcos actuales, así como si estamos ante una necesaria adaptación o por el contrario, un cierto salto al vacío que debe ser capaz de escribir algún apartado distinto y nuevo del sistema de responsabilidad.

Pero no podemos perder de vista que uno de los grandes retos de estas nuevas tecnologías frente a los viejos marcos jurídicos, es el de su optimización, es decir, el de una necesaria convergencia entre aquellas y éstas. Ambos, derecho y tecnología, han de evolucionar, pero han de hacerlo en paralelo, lo que no empece que uno se anticipe al otro. Una convergencia que puede ser de confrontación o de colaboración, de modo que puede ser colaborativa o en su caso, de ataque para reducir el alcance o acondicionarlo a otros intereses disruptivos[146]. Sin que de momento ni unos ni otros tengan en su mano la fórmula idónea para conseguir esta optimización, una optimización que viene marcada ya por una realidad irreversible[147].

La fuerza del dato, la secuenciación y análisis inmediato de los mismos, debilitarán la contundencia y quizá categorización del *alea*, pero no lo eliminarán. La incertidumbre del siniestro subsiste, tanto en el *an* como en el

146. Gráficos, DEAKIN/MARKOU, «The law-technologie cycle and the future of work (March 2018)», cit., p. 10 afirman: «El mismo proceso de normalización está en marcha hoy en día en la economía emergente de plataformas, aprendizaje de máquinas y grandes datos. Corporaciones como Uber (no es el único ejemplo, simplemente es el más prominente) invierten fuertemente en prácticas de lobby y en litigios para anular leyes que aumentan sus costes. Vemos esto en los intentos de la filial británica de Uber en el intento de relajar las leyes de licencias de taxi a su favor, una estrategia que fue reivindicada por un fallo judicial».
147. No le falta razón a UNSWORTH, «Smart Contract This! An Assessment of the Contractual Landscape and the Herculean Challenges it Currently Presents for «Self-executing» Contracts», *Legal Tech, Smart contracts and Blokckchain*, [CORRALES/FENWICK/HAAPIO (Eds.)], Singapore, 2019, pp. 17 y ss., cuando postula esa necesidad convergente entre una tecnología que califica de brillante y una contratación que sin embargo tacha de «viejas y polvorientas prácticas de contratación». El autor suizo, sugiere una manera de desencriptar el significado de los contratos existentes, un proceso que se denomina «Optimización de contratos digitales» y que se compara con las tareas civilizatorias que le impuso a Hércules su primo, enemigo y patrocinador, Euristeo. Para ilustrar mejor los desafíos que se encontrarán durante la convergencia, el enfoque se mantiene específica y deliberadamente en segmentos de contratación más complejos (normalmente acuerdos de negocio a negocio) como proyectos de infraestructura o seguros de líneas comerciales. Muchos de los ejemplos vendrán de los seguros porque este es un paradigma popular de contratación compleja. Por ello el autor partirá de formas de contratos más simples y estándar —que generalmente son más fáciles de convertir en contratos más inteligentes— simplemente para comparar y contrastar con los segmentos de contratación más complejos.

quando. Pero sí se seleccionará con mayor precisión el riesgo, los elementos y circunstancias de éste, anti seleccionando sus exclusiones, sus limitaciones.

Y todo ello, sin olvidar, que ese dato, esos datos obtenidos a tiempo real y frecuentemente a lo largo de toda la relación jurídica de seguro, tanto en la fase precontractual como en la perfectiva y de ejecución, son y serán datos sensibles, que afectan y engloban la esfera personal e íntima del propio asegurado o portador del riesgo. Y es que, el individuo ha creado, genera identidades digitales, directa o indirectamente, a través de datos sobre su persona, su profesión, sus hábitos, su participación en redes, etc[148].

Es cierto que no todo dato que se cobije dentro del *big data* será un dato personal, un dato sensible, pero sí habrá datos que tengan que ver con la conducta, con los hábitos, con la esfera más íntima y reservada del asegurado y otros que atañan a su estado de salud, enfermedad, trabajo, profesión, ocio, etc.

Recuérdese también la existencia de técnicas tanto de anonimización como de seudonimización sobre los datos personales. Siendo el primero un concepto ya conocido en nuestro ordenamiento en la norma anterior de protección de datos y la segunda, un concepto de nuevo cuño introducido por el Reglamento General de Protección de Datos[149]. Con la anonimización se evita la asociación e identificación de unos datos concretos con el titular o persona titular de los mismo. Se impide el riesgo de asociación a una persona de esa información atinente a su esfera de protección y dignidad persona de modo que no se la puede identificar.

Por su parte se entiende por seudonimización, tal y como define el RGPD, aquella información que, sin incluir los datos denominativos de un sujeto, permiten identificarlo mediante información adicional, siempre que ésta figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable[150].

148. No le falta razón a GIORDANO, «La blockchain ed il trattamento dei dati personali», *Blockchain e Smart Contract*, {BATTAGLINI/TULLIO (a cura di)}, Milano, 2019, pp. 99 y ss., p. 99 cuando afirma que la identidad on line es una unión entre una representación digital (ya sea en la forma username, avatar, código unívoco identificativo, etc..) y el singular individuo.
149. Sobre esta anonimización, vid. entre otros, GIORDANO, «La blockchain ed il trattamento dei dati personali», *cit.*, en especial pp. 107 y ss.
150. Técnicas de desidentificación, tanto la de anonimización como la de seudonimización que, a juicio de ALVES LEAL, «Big data», cit., p. 206 son atractivas para los responsables por el tratamiento de los big data, habida cuenta que, de este modo, estos datos pueden

La automatización que la tecnología trae y traerá solo en el modo de cómo se accede, cómo se gestiona y analiza la información implicará la dilución de esos deberes, al menos en la intensidad de su esencia y ejecución, pero también provocará que el riesgo real esté perfectamente ajustado o alineado en cada momento con el riesgo asegurado. Ahora bien, ese automatismo, esta sustantivación si se quiere esencial y santo y seña de la tecnología y de algunas de sus dimensiones, sobre todo, del *smart contract*, debe también, al jurista, conferirle cierta prudencia y la nitidez de saber deslindar y diseccionar qué estamos o a qué nos referimos cuando hablamos de una automatización que, como la desintermediación, no hay que entenderla, al menos de momento, como absoluta y sin interacción humana de algún tipo[151]. No estamos aún en esa fase.

Y es que la acción o interacción humana está presente todavía, bien sea de un modo directo de las partes, o una de ellas, bien, a través de terceros, los conocidos como «oráculos». El que una transacción se despliegue a través de una cadena de bloques y lleve implícita una cierta confianza por las partes, no significa que toda la gestión o desarrollo obligatorio y prestacional de una relación jurídica recaiga absolutamente en el ordenador o por el *software* de un ordenador[152].

permanecer a salvo de la aplicación de la normativa del Reglamento. Ello no impide minimizar el riesgo que pueden existir de re-identificación del titular de los datos que puede ser propiciada por las técnicas propias del big data. Advierte así la autora lusa de que en los modelos de análisis de big data generalmente tratan con bloques de datos (personales y no personales), los cuales, si aisladamente considerados no permiten la identificación del titular de los datos, sin embargo, cuando se combinan o se intersecccionan con otros bloques de datos, sí permiten esa identificación. Señala GIORDANO, «La blockchain ed il trattamento dei dati personali», cit., p. 108 que por anonimización debe entenderse el resultado del tratamiento (sucesivo) de datos personales (raccolti all´origine e identificativi) al fin de impedir irreversiblemente la identificación de la persona interesada propiamente a través de una técnica de anonimización. El resultado de tal actividad, cual técnica aplicada a los datos personales, debería ser, en el estado actual de la tecnología, permanente como una cancelación, lo que debería suponer la imposibilidad sucesiva de volver a tratar esos datos personales.
151. Se debe en puridad distinguir por ejemplo entre la ejecución de un Smart contract y la ejecución de las prestaciones implícitas en un Smart contract. En este ámbito, véase el trabajo de NICOTRA, «L´Italia prova a normare gli smart contract, ecco come: pro e contro», (www.agendadigitale.eu/documenti/Litalia-prova-a-normare-gli-smart-contract-ecco-come-pro-e-contro).
152. Compartimos el criterio de CERRATO, «Contratti tradizionali», cit., p. 284 que afirma como es cierto que bien puede ser, incluso en la mayor parte de los casos lo es, que las condiciones de la eficacia del contrato dependan de un factor externo a la cadena, de modo que sea necesario el recurso a un «oracolo» che es de todos modos un intermediario (humano) o un programa elaborado o gestionado por un intermediario humano,

La intervención humana está presente, como lo está, además, en el desarrollo e introducción de la redacción del lenguaje contractual y su traducción a un lenguaje codicial algorítmico. ¿Quién y cómo se traducen pues las cláusulas contractuales y condicionados a lenguaje informático?

Ello implicará, además, que deberes como el de la declaración del aumento del riesgo o, *a sensu contrario*, de disminución del mismo, vayan perdiendo la importancia que hasta el presente han generado para el contrato y para el devenir mismo de la relación jurídica, al claudicar el tamiz o filtro intrapersonal del tomador o del asegurado anclado ahora en el dinamismo de la tecnología y la digitalización de la información a través de medios, sensores, análisis dinámicos y paramétricos de la información. Pero cambia, además, la gestión del siniestro, del contrato, los costes y gastos de transacción, la liquidación del contrato y resarcimiento pago del daño.

Optimizando tiempos, recursos y costes[153]. Cuestión distinta y desde una óptica plúrime de manifestaciones de estas tecnologías, como sobre todo los contratos inteligentes y las cadenas de bloques, —(no necesariamente unidas y condicionadas la una a la otra)[154]—, ¿están cambiando los pilares del derecho contractual o, en verdad, las formas y métodos de contratación de las partes?[155] ¿*Sustantiam* o solo adjetivación circunstancial?

en relación al que el «comportamiento» de las partes deben basar en la fiducia, como en las relaciones tradicionales.

153. Insiste NAYLOR, *Insurance Transformed: technological disruption*, Palmerston North, 2017, p. 36 y 37 en como por ejemplo con Blockchain, «substantially removes the need for third-party payments systems and will be a vital part of real-time insurance as it will allow near-zero-cost transactions».
154. Enfatiza de modo reiterado esta situación, con razón, SANZ BAYÓN, «La ejecución automática de los contratos: una aproximación a su aplicación en el sector asegurador», *cit.*, pp., cuando asevera «aunque Insurtech y Blockchain no son conceptos identificables ni unívocos, el primero y en general los llamados tecno seguros, pueden adoptar esta infraestructura para facilitar la gestión y tramitación de las pólizas (las de cobertura dinámica o paramétrica), al mismo tiempo que se garantiza criptográficamente la documentación e integridad de las mismas.... Insurtech no tiene por qué ir de la mano de un registro distribuido, sino simplemente, operar mediante los referidos Smart Contracts, sin necesidad de «tokenizar» los contratos de seguro como activos digitales, ni que todas las partes del contrato estén interconectadas mediante una red de nodos computacionales compartiendo el mismo protocolo criptográfico».
155. Desde este enfoque, señala MIK, «Smart contracts: a requiem», cit., p. 2 como desde un plano teórico, se ejemplifica la tendencia a confiar en la tecnología para mejorar o incluso reemplazar las instituciones tradicionales y sustituir la toma de decisiones humanas subjetivas e impredecibles por algoritmos objetivos y predecibles. En el mundo de los «contratos inteligentes», la confianza se basa en la computación, no

Mas, todas estas nuevas tecnologías digitalizadoras, aun siendo conscientes que no todas se asienten bajo este parámetro, ¿tienen capacidad de distorsionar el *status* quaestionis pacífico en materia de tutela, de información, de simetría, de equilibrio contractual entre las partes y preservar el sinalagma? O planteado de otro modo, ¿pueden esos datos, esos códigos o traducciones a lenguaje máquina que se introducen en la programación o en el *software* ser o estar intencionadamente manipulados por quién los crea? Esto ha llevado a la doctrina a plantearse hipótesis como veremos más adelante sobre si el algoritmo puede errar o no, o incluso a cuestionar su propia neutralidad valorativa[156].

El uso de datos de un modo masivo e indiscriminado lleva implícito un riesgo cuando se trata de datos personales[157]. Riesgos sobre el contenido, la esencia e intensidad y difusión o no de los mismos. Ahora bien, la mera posibilidad de analizar y gestionar esos datos, esa información, rompe la brecha que, hasta el presente ha existido entre el riesgo real y el riesgo declarado *versus* riesgo asegurado, con el reflejo que ello propende hacia el valor del interés asegurado, la tarificación de la prima y las posibilidades de infraseguro y sobreseguro.

en la confianza en el sistema legal o en el conocimiento previo de una contraparte. Supuestamente, esta «confianza digitalizada» garantiza que lo que se ha acordado se haga realmente».

156. Sobre esto último imprescindible la lectura del espléndido artículo y blog de TAPIA HERMIDA, «Responsabilidad derivada del uso de la inteligencia artificial. Informe del Grupo de Expertos de la Comisión Europea de 2019 (1). Características esenciales de los regímenes de responsabilidad derivada de la inteligencia artificial y el uso de otras tecnologías digitales», cit., cuando tras apuntar la responsabilidad civil penal o administrativa en la que pueden incurrir quienes diseñan, distribuyen o utilizan en el mercado financiero los ingenio de la IA y otras tecnologías digitales afirma: «... el «mito de los algoritmos neutrales» nos llevaba a constatar que la realidad de las cosas —siempre tozuda por constatable (por ejemplo, cuando se examina la jurisprudencia sobre delincuencia financiera digital)— muestra que los algoritmos pueden mentir, engañar y manipular (y ser manipulados) mediante, por ejemplo, prácticas en el mercado de valores de multiplicación patológica de órdenes («quote stuffing»), de indicios falsos («spoofing»), de órdenes contradictorias prácticamente simultáneas («churning») y de anticipación parasitaria («sniffers). Y de ello inferíamos que «es precisa una labor regulatoria que identifique los responsables del uso de los algoritmos y prevenga y sancione este tipo de prácticas en defensa de los consumidores, sean estos clientes bancarios, inversores o asegurados».
157. En este punto, interesante la aportación de ORTEGA GIMÉNEZ, «Tratamiento ilícito de los datos de carácter personal, contratos de seguro y derecho internacional privado», RES, 2019, n.º 179, pp. 225 y ss., quién se hace eco en p. 227 de como la rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales.

A su lado, un concepto propio, la inteligencia artificial[158]; susceptible de desglosarse en varios planos y diversas manifestaciones y desde diferentes ópticas, la propia que decide en base a megadatos, inabarcables para el cerebro humano y, que lo lleva a cabo conforme a cómo se le ha programado y, la más inquietante para un sistema jurídico que es cuando esa misma inteligencia es capaz de un lado de realizar un razonamiento lógico y automático, y de otro, de adoptar decisiones por sí misma, de forma autónoma y al margen de la programación hecha y de la supervisión del ser humano[159]. Y la magnitud de esa afectación es vastísima, caracterizada tanto por la amplitud como por lo ignoto e indeterminación cuando no indecibilidad en este momento de su alcances reales y posibles[160].

158. Sobre el riesgo de caer en el reduccionismo de asociar únicamente la inteligencia artificial con los robots, MUÑOZ VILLAREAL/GALLEGO CORCHERO, «Inteligencia artificial e irrupción de una nueva personalidad en nuestro ordenamiento jurídico ante la imputación de responsabilidad a los robots», *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y aseguramiento*, [MONTERROSO (Dir.)], Valencia, 2019, pp. 67 y ss., p. 69.

159. Véase el análisis que sobre estas dos inteligencias y la responsabilidad civil, sobre todo, la última, lleva a cabo, ATIENZA NAVARRO, «La responsabilidad civil por daños causados por sistemas de inteligencia artificial. *(A propósito de la* Resolución del Parlamento Europeo de 16 de febrero de 2017, *con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica)*», Homenaje al profesor Rubén Stiglitz [VEIGA (Dir.)], Cizur Menor, 2020, pp. 2 y ss., quién señala como el primer tipo de inteligencia artificial se basa en casos en que el sistema toma decisiones de forma autónoma pero con base en unos algoritmos para los que ha sido programado, manejando una cantidad de datos (los famosos *big data*) que ningún ser humano sería capaz de utilizar. Sin embargo, la decisión adoptada por el sistema no se debe a un proceso de aprendizaje de la máquina; el robot ha sido programado para decidir y decide, pero, insisto, a partir de una base de datos existente, de la que extrae conclusiones (tipo reglas lógicas —«si...entonces»—) o bien, cuando lo necesita, ampliando la base de datos ya existente a nuevos hechos y reglas, de los que extrae también conclusiones. Este tipo de inteligencia artificial la encontramos presente en un sinfín de actividades industriales, sanitarias, docentes, de transportes, etc. La segunda, consiste en que «el algoritmo ya es capaz de pensar (tras un proceso de aprendizaje en el que interactúa y extrae datos de su entorno) y de actuar o tomar decisiones con total autonomía respecto de quien los creó o programó; hasta el punto de que su creador (esto es, el programador o entrenador) en ocasiones ni siquiera sabría decir por qué ha actuado así».

160. No le falta razón a MONTERROSO, «Introducción», *Inteligencia artificial y riesgos cibernéticos. Responsabilidades y aseguramiento*, [MONTERROSO (Dir.)], Valencia, 2019, p. 17 al referirse a la inteligencia artificial cuando asevera: «A pesar de la indefinición que rodea en estos momentos al concepto de inteligencia, o precisamente por esa indeterminación conceptual, la difusión de las tecnologías dotadas de IA, como soluciones a una infinidad de problemas de orden práctico, suponen un gran reto para los científicos que analizan su repercusión social».

12

¿Son necesarias reglas especiales para los daños causados por Inteligencia Artificial?[1]

M.ª Luisa Atienza Navarro
Profesora Titular Derecho Civil
Universitat de València

1. Este trabajo ha sido realizado en el marco del Proyecto de Investigación «Hacia una protección del cliente más global». AICO GV-2019. Generalitat Valenciana. Este trabajo es una parte abreviada de la ponencia presentada a la Asociación de Profesores de Derecho Civil para las Jornadas que se celebran en Granada los días 19 a 21 de octubre de 2023, que será objeto de publicación en los próximos meses. Como allí advierto, recojo ideas de otros estudios en los que, a lo largo de los últimos años, me he ocupado del tema de la responsabilidad civil por daños causados por la inteligencia artificial. Principalmente: *Daños causados por inteligencia artificial y responsabilidad civil*, Atelier, Barcelona, 2022; «¿Una nueva responsabilidad por productos defectuosos? Notas a la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por daños causados por productos defectuosos de 28 de septiembre de 2022 (COM/2022/495)», *InDret*, n.º 3, 2023; «Distintos modelos para la responsabilidad civil por los daños causados por la inteligencia artificial. A modo de comparación entre distintas propuestas de la Unión Europea», en AA.VV.: *Perspectivas regulatorias de la inteligencia artificial en la Unión Europea*, (coord.: Miquel Peguera Poch), Reus, Barcelona, 2023.