

LAS NUEVAS TECNOLOGÍAS EN LA ACTIVIDAD ASEGURADORA

INSURTECH

*MARTÍN ZAPIOLA GUERRICO**

Fecha de recepción: 15 de octubre 2019

Fecha de aceptación 30 noviembre 2019

Disponible en línea: 30 de diciembre 2020

Para citar este artículo/To cite this article

ZAPIOLA GUERRICO, Martín. *Las nuevas tecnologías en la actividad aseguradora*, 53 Rev. Ibero-Latinoam.Seguros, 137-160 (2020). <https://doi.org/10.11144/Javeriana.ris53.ntaa>

doi:10.11144/Javeriana.ris53.ntaa

* Abogado en la Universidad de Derecho y Ciencias Sociales de la Universidad de Buenos Aires, socio fundador de Zapiola Guerrico & Asociados, tiene una extensa experiencia en litigios civiles y comerciales en los distintos niveles jurisdiccionales, incluyendo la instancia extraordinaria ante Tribunales Superiores provinciales y la Corte Suprema de Justicia de la Nación. Ha completado numerosos cursos relacionados a Seguros, Negociación, Mediación y otras áreas de la profesión legal: Pepperdine University School of Law (California, USA) “Mediation: The Art of Facilitating Settlement”; Harvard University (Massachusetts, USA): “Theory and Tools of the Harvard Negotiation Project” por Roger Fisher y Howard Raiffa; Harvard Business School: *Leading Professional Service Firms* (2007). Contacto: mzg@zgabogados.com.ar.

RESUMEN

El autor analiza el impacto de las nuevas tecnologías en la actividad aseguradora –fenómeno conocido como *Insurtech*– y destaca las posibles cuestiones jurídicas que pudieran surgir, entre ellas, el uso antijurídico de datos personales y el eventual sesgo discriminatorio de los algoritmos utilizados en la operatoria asegurativa. A los efectos de facilitar el debate jurídico de las distintas cuestiones tratadas, el artículo explica los conceptos básicos referidos a cada una de las tecnologías involucradas en *Insurtech*.

Palabras clave: *Insurtech*, nuevas tecnologías, algoritmos, datos personales, Privacidad, Discriminación.

ABSTRACT

The author analyzes the impact of new technologies in the insurance activity –a phenomenon known as Insurtech– and highlights possible legal issues that could arise, among them, the unlawful use of personal data and the eventual discriminatory bias of algorithms used in insurance operations. The article explains basics concepts related to each of the technologies involved in Insurtech, to facilitate the legal debate on their possible consequences.

Keywords: *Insurtech*, *New technologies*, *Algorithms*, *Personal data*, *Privacy*, *Discrimination*.

SUMARIO

1– Introducción. 2– ¿Qué se entiende por *Insurtech*? 3– Las distintas tecnologías involucradas a) Inteligencia Artificial. Algoritmos. b) *Big Data* c) Internet of Things. Telemática d) *Blockchain*. Contratos Inteligentes. 4– Impacto en las distintas áreas operativas del negocio de seguros a) Diseño de productos y suscripción, b) Comercialización c) Gestión de siniestros 4– Aspectos legales e interrogantes. 5– Conclusiones preliminares. Bibliografía.

1- INTRODUCCIÓN

El objeto del presente trabajo es analizar el impacto de las nuevas tecnologías en el negocio de seguros –fenómeno conocido como *Insurtech*– y al mismo tiempo destacar las posibles cuestiones jurídicas que podrían surgir como consecuencia de las prácticas y operatorias resultantes del fenómeno mencionado.

En esta presentación dedicaremos un espacio significativo al análisis conceptual de las tecnologías en cuestión y a otras cuestiones eminentemente operativas como las posibles aplicaciones en las distintas áreas del negocio del seguro. Si bien este abordaje puede resultar inusual en un análisis de carácter jurídico, entendemos que resulta muy importante explicar con claridad el funcionamiento básico de las distintas tecnologías (qué entendemos por Inteligencia Artificial, cuál es la función de un algoritmo, cómo funciona básicamente un “contrato inteligente”, etc.) para luego poder sacar conclusiones sobre las implicancias jurídicas de su aplicación.

Resulta claro que el derecho sigue a la realidad, y nunca la precede, razón por la cual creemos que resulta esencial conocer primero los aspectos esenciales de dicha realidad para luego intentar anticipar las implicancias jurídicas de la misma.

Hemos elegido analizar el impacto de las nuevas tecnologías recorriendo cada una de las áreas operativas del negocio asegurador, según las conocemos por nuestro trabajo profesional; de tal forma nos referiremos a las áreas de Diseño de Productos y Suscripción, Comercialización (directa e indirecta) y, finalmente, Gestión de Siniestros.

2- ¿QUÉ SE ENTIENDE POR *INSURTECH*?

El término *Insurtech* surge de la conjunción de las palabras inglesas *insurance* (seguros) y *technology* (tecnología) y está inspirada en el término *Fintech* (unión de *finance* y *technology*) que alude a un fenómeno que se anticipó en muchos años al de *Insurtech*.

El término tiene dos aplicaciones, distintas pero relacionadas:

- a) Por un lado, alude a la utilización de las nuevas tecnologías para mejorar y agilizar las transacciones y procesos de la industria aseguradora. Esta utilización está generando una mejora sustancial en los procesos y modelos tradicionales de negocios del sector asegurador.
- b) En segundo lugar, alude a las empresas de seguros que se constituyen desde su mismo inicio (*start-ups*) como organizaciones estructuradas en base a las nuevas tecnologías, a los efectos de brindar cobertura a sectores de consumidores más adeptos a los dispositivos digitales y que utilizan los mismos en aspectos sustanciales de su vida diaria. A diferencia de las aseguradoras ya establecidas o “tradicionales”, tienen la posibilidad de diseñar todos sus procesos, productos y sistemas –“desde cero”– con base en las nuevas tecnologías, y no están atadas o limitadas por sistemas tradicionales pre-existentes (*legacy systems*)¹.

¹ “Insurtech-the threat that inspires”, MCKINSEY, en <https://www.mckinsey.com/industries/financial-services/our-insights/insurtech-the-threat-that-inspires>.

De todas formas, existe una interacción creciente entre las *Insurtech* y las aseguradoras ya establecidas: en algunos casos las *Insurtech* son creadas por las propias aseguradoras “establecidas”² y en otros casos estas nuevas compañías proveen servicios a las ya establecidas a efectos de mejorar y “digitalizar” aspectos o sectores específicos de su operatoria.

3- LAS DISTINTAS TECNOLOGÍAS INVOLUCRADAS

A) Inteligencia artificial y algoritmos

A₁) Inteligencia Artificial:

El término “Inteligencia Artificial” (en inglés *Artificial Intelligence* o su sigla “AI”) fue acuñado por el científico John McCarthy en el año 1956 para definir “*la ciencia e ingeniería de producir máquinas inteligentes*”.

Ya años antes, el matemático y criptógrafo Alan Turing³ se preguntaba si las máquinas podían llegar a “pensar” como los seres humanos y a tal efecto ideó el luego llamado “Test de Turing”, que consiste en lo siguiente: se ubica en tres cuartos diferentes a una computadora, una persona, y una segunda persona que actúa como interrogador –que sólo puede comunicarse con la computadora y la otra persona mediante un sistema escrito tipo “telex” (o sea, aclaro para los más jóvenes, utilizando únicamente texto escrito). El “interrogador” debe realizar preguntas a ambos “participantes” para intentar descubrir cuál es el ser humano y cuál es la computadora. Si no lo logra, la computadora habrá aprobado el “Test de Turing”.

Existen innumerables definiciones sobre lo que debe entenderse por Inteligencia Artificial pero, a los efectos del presente trabajo hemos elegido la siguiente: **“un conjunto de técnicas de las ciencias de la computación que permiten a los sistemas informáticos realizar tareas que normalmente requieren inteligencia humana, tales como percepción visual, reconocimiento de la voz, toma de decisiones y traducción de idiomas”⁴.**

La mayoría de los programas de Inteligencia Artificial en la actualidad se elaboran con un propósito específico (v.g. para jugar al ajedrez, para predecir el clima, o asistir a clientes en una tarea determinada). Este tipo de aplicaciones de “IA” se conoce como *narrow AI* o *weak AI* (IA estrecha o IA débil). Para este tipo de aplicaciones los humanos han pre-definido qué datos, qué algoritmos y qué modelo de análisis

² Un ejemplo de este esquema en la Argentina es la nueva aseguradora Iúnigo -focalizada en Seguro Automotor- que es de propiedad de la tradicional compañía San Cristóbal, que opera en múltiples ramos de seguros.

³ Alan Turing lideró el proyecto que logró descifrar el código secreto “Enigma”, utilizado por los alemanes durante la Segunda Guerra Mundial y es considerado uno de los padres de las Ciencias de la Computación.

⁴ The Economist Intelligence Unit, https://perspectives.eiu.com/sites/default/files/Artificial_intelligence_in_the_real_world_0.pdf.

utilizar. Se construye y entrena una máquina que puede aprender –en base a los datos recibidos– como realizar una tarea determinada, pero únicamente esa tarea y ninguna otra. En muchas de esas tareas, las máquinas pueden superar a los humanos y por lo tanto tener habilidades “sobre-humanas”, pero sólo para una limitada tarea específica y no para tareas generales. Algunos ejemplos famosos incluyen a “DeepBlue” (IBM) venciendo a Garry Kasparow en ajedrez en 1997, a “Watson” (IBM) ganándole a los humanos en el juego de “Jeopardy” en 2011 y a “AlphaGo” (Google) venciendo en juego de Go en 2015⁵. Todas las manifestaciones de Inteligencia Artificial con las que tenemos contacto actualmente, aún las más sofisticadas, (como el Traductor de Google, el asistente digital Siri de Apple, etc.) son ejemplos de *narrow AI*.

Por oposición a la *narrow IA* tenemos la *Artificial General Intelligence* (“IA general”) o *strong AI* (“IA fuerte”) que se refiere a sistemas que pueden realizar cualquier actividad intelectual que puede desarrollar un ser humano (eso implica la habilidad de pensar en abstracto, plantear distintas estrategias, y recurrir a nuestra memoria y pensamientos para tomar decisiones o generar ideas creativas). *No existen en la actualidad –por ahora– sistemas que puedan considerarse como ejemplos de strong AI*. Este tipo de Inteligencia Artificial es la que vemos en películas como “Ella” (donde el protagonista se enamora de un sistema operativo que sólo conoce por su voz femenina y sensual) u otras películas de ciencia ficción en donde seres humanos interactúan con máquinas o sistemas operativos que tienen conciencia y sensibilidad y evidencian una capacidad intelectual generalizada⁶.

Una de las aplicaciones de la Inteligencia Artificial más utilizadas en la actualidad, y que generan más sistemas útiles para nuestra vida diaria, se denomina *Machine Learning* (“Aprendizaje Automático”), la cual consiste en dotar a los sistemas de la habilidad de **aprender automáticamente** y mejorar en base a su propia experiencia sin haber sido programados expresamente a tal efecto. Es el proceso por el cual una computadora detecta patrones o “regularidades” en determinados –y numerosos– datos que se le suministran para entrenarla. Si, por ejemplo, deseamos crear un algoritmo para detectar el “spam” en correos electrónicos, tendremos que “entrenar” al algoritmo exponiéndolo a muchos ejemplos de correos electrónicos que han sido previamente marcados (*tagged*) como *spam* o no *spam*. El algoritmo “aprende” entonces a identificar patrones en los ejemplos suministrados –como la aparición de determinadas palabras o combinación de palabras– que determinan la posibilidad de que un correo sea considerado como spam.

Con respecto a la actividad aseguradora, la técnica de *Machine Learning* puede utilizarse para reconocer rápidamente un reclamo fraudulento o reclamos que pueden ser tramitados aceleradamente por sus características, automatizar elementos de un proceso regular de gestión de siniestros o crear *chatbots* (programas de AI que pueden imitar una conversación humana interactiva en temas específicos) para atender consultas de los clientes.

⁵ “General vs narrow artificial intelligence”, Anders Arpteg, Medium.com, <https://medium.com/peltarion/general-vs-narrow-artificial-intelligence-d8faf296d4ab>.

⁶ “Distinguishing between Narrow AI, General AI and Super AI”, Tania D. Jajal, Medium.com. <https://medium.com/@tjajal/distinguishing-between-narrow-ai-general-ai-and-super-ai-a4bc44172e22>.

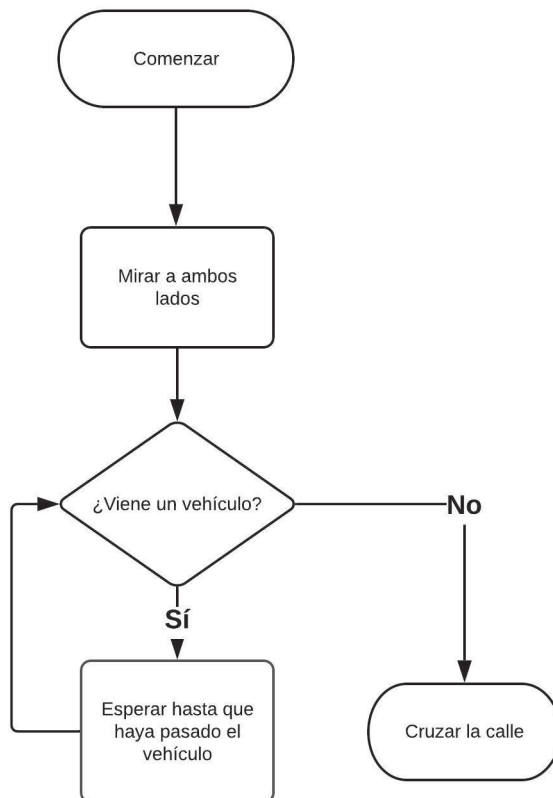
A2) Algoritmos

Los **algoritmos** son elementos esenciales de cualquier programa de computación y, asimismo, de los sistemas más complejos de Inteligencia Artificial.

Se denomina algoritmo a un *grupo finito de operaciones organizadas de manera lógica y ordenada que permite solucionar un determinado problema*. Se trata de un conjunto de instrucciones o reglas establecidas que, por medio de una sucesión de pasos, permiten arribar a un resultado o solución (en términos de la vida diaria, podemos decir que una receta de cocina es básicamente un algoritmo). En nuestra propia profesión, y sin ser conscientes de ello, aplicamos algoritmos –secuencias de pasos lógicos– constantemente, vg.: para arribar a un diagnóstico legal luego de recibir el “input” derivado del relato de nuestros clientes y los documentos que hemos analizado.

El diseño de un algoritmo comienza con la representación gráfica de los pasos a seguir (lo que se denomina “diagrama de flujo”, o *flowchart* en inglés), que luego se traduce a un programa informático mediante instrucciones o “líneas de código” en el lenguaje de computación pertinente.

A efectos de visualizar más claramente la idea, exhibimos a continuación un “diagrama de flujo” muy básico, con instrucciones para que un peatón cruce la calle:



Los algoritmos, desarrollados por programadores a los efectos de instruir a las computadoras para realizar nuevas tareas, son hoy elementos esenciales en todos los aspectos de nuestra vida “digital”: ellos organizan enormes cantidades de datos a los efectos de suministrarnos información y servicios, basados en ciertas instrucciones y reglas.

A los efectos del presente trabajo, es muy importante entender este concepto y sus implicancias, por cuanto *con las técnicas de **Machine Learning** comúnmente utilizadas en aplicaciones de Insurtech, no sólo los programadores diseñan los algoritmos, sino que los propios “algoritmos de aprendizaje” diseñados por aquéllos, generan a su vez nuevos algoritmos*, lo cual puede llevar a resultados no previstos originalmente.

Ya sea de forma intencionada o no intencionada los algoritmos utilizados, –por ej.– en un sistema de cotización de seguros, pueden arrojar resultados sesgados que eventualmente un juez podría considerar discriminatorios (primas exageradamente altas para quienes viven en determinada zona o pertenecen a determinado rango etario).

Por las razones expuestas, muchos especialistas resaltan la falta de transparencia de estos procesos y la importancia de que se diseñen mecanismos (como “cajas negras” de los procesos computacionales) que permitan registrar todos los cambios y comportamientos del sistema y así poder detectar cualquier defecto o “sesgo” del mismo⁷.

B) Big Data

Big Data se refiere al campo de las ciencias de la computación que estudia formas de analizar, procesar y extraer información útil de conjuntos de datos que son demasiados voluminosos o complejos para ser procesados por sistemas tradicionales de computación.

Es una nueva ciencia que *intenta entender y predecir el comportamiento humano –y otras cuestiones– mediante el estudio de enormes volúmenes de datos no estructurados*.

Las características más relevantes de los datos que son analizados como *Big Data* se conocen como “las 5 Vs”: Volumen, Velocidad, Variedad, Veracidad y Valor (utilidad para el objetivo buscado). Los datos pueden provenir de las más variadas fuentes, como, por ejemplo: registros de navegación en la web, videos de seguridad, patrones de clima, arribos de vuelos, dispositivos personales de monitoreo cardíaco, etc.

Algunos ejemplos de nuestra vida diaria, donde se recurre a técnicas de *Big Data*, son:

– Cada vez que ingresamos a Google o Facebook y vemos *avisos comerciales* ellos están basados en nuestras preferencias, historial de navegación, *likes* o pertenencia a grupos en Facebook, que “likearon” nuestros amigos, etc.

⁷ RODRÍGUEZ-PARDO José Miguel. “El Actuario ante Insurtech”. https://www.fundacionmapfre.org/documentacion/publico/i18n/catalogo_imagenes/imagen_id.cmd?idImagen=1108971.

– Cada vez que compramos *un boleto de avión*, los precios varían en base a la ruta elegida, demanda para esa ruta, demanda esperada de último minuto, cuán temprano hemos reservado el vuelo, etc.

– Con respecto a la actividad aseguradora, y específicamente el *Seguro Automotor*, existen dispositivos que se instalan hoy en nuestro automóvil y emiten en tiempo real datos sobre las rutas que elegimos, si frenamos y aceleramos bruscamente y muchos otros detalles que evidencian nuestro “estilo de conducción”. En base a tales datos se modifica la prima del seguro, premiando un estilo “conservador” o castigando un estilo “arriesgado” de conducir.

C) *Internet of Things* y Telemática

C₁) *Internet of Things*

El término *Internet of Things* o su sigla **IoT** (“Internet de las Cosas”) se refiere básicamente a extender la capacidad de conectarse en red y realizar tareas informáticas a objetos, dispositivos, sensores y otros elementos que normalmente no son considerados computadoras. Estos “objetos inteligentes” requieren mínima intervención humana para generar, intercambiar y consumir datos; normalmente pueden conectarse a distancia con otros “objetos inteligentes” o con computadoras remotas que analizan y administran la información recibida⁸.

Internet of Things también se refiere a una red cada vez más amplia –y que crece aceleradamente– de objetos conectados entre sí que son capaces de recolectar e intercambiar datos utilizando sensores y transmisores incorporados en su propia estructura. Termostatos, automóviles, luces, heladeras y todo tipo de dispositivos o “artefactos electrodomésticos” pueden conectarse a la **IoT**.

La tecnología **IoT** tiene suma relevancia para la industria aseguradora, dado que la posibilidad de recibir grandes cantidades de datos relevantes (*Big Data*) desde dispositivos utilizados por los asegurados, les permite a las aseguradoras conocer mejor el perfil y comportamiento de tales asegurados a los efectos del diseño y cotización de coberturas e inclusive les permite enviar mensajes o consejos de prevención de riesgos a sus asegurados en base a la información recibida de los dispositivos **IoT**.

C₂) Telemática

Telemática es la *tecnología que permite enviar, recibir y guardar información utilizando dispositivos de telecomunicaciones para controlar objetos remotos*. El término también se utiliza de manera más acotada para referirse al uso de tal tecnología en vehículos automotores.

⁸ “The Internet of Things: An Overview”, Internet Society. <https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf>.

Como podemos ver, la telemática es una tecnología naturalmente vinculada con la tecnología **IoT**.

D) Blockchain y Contratos Inteligentes

D1) Blockchain

Es una de las tecnologías que permiten formar una red distribuida de registros de datos que no cuenta con una administración centralizada (conocidas como **DLT**, por *Distributed Ledger Technology* –“Tecnología de Registros Distribuidos”). Si bien data de 1991, se hizo más conocida a partir de 2009, al ser la tecnología que hizo posible la operatoria de la criptomoneda *Bitcoin*.

Como su nombre lo indica –*Blockchain* significa “cadena de bloques” en inglés– es una secuencia encadenada de bloques o grupos de registros o datos que están unidos entre sí y así distribuidos entre distintos usuarios (denominados “nodos”). La **Blockchain** funciona como un registro inmutable de transacciones que no requieren de una autoridad externa a la red de nodos para validar la autenticidad e integridad de los datos, básicamente de la siguiente manera⁹:

- 1) Cada uno de los bloques está conformado por un conjunto de registros o datos, que se pueden ir agregando al bloque a medida que son validados por todos los “nodos” de la red.
- 2) Una vez que el nuevo registro es validado por la red, es agregado al último bloque de la cadena.
- 3) Cada bloque de la cadena contiene un código único que lo identifica, llamado **hash**, y también contiene el **hash** del bloque que lo antecede en la cadena.

La función del **hash** es clave para asegurar la autenticidad e inmutabilidad de cada dato y cada bloque incorporado a la cadena. *El hash es creado por un algoritmo que toma la información digital contenida en el bloque y genera una secuencia de letras y números en base a la misma*. Esta secuencia de caracteres tiene dos características importantes:

- a) Cualquiera sea el tamaño del archivo a identificar, *el algoritmo siempre generará una secuencia (hash) de la misma longitud*. Por ejemplo, tanto el **hash** de una frase corta describiendo una transacción, como el **hash** del libro “La Guerra y la Paz” de León Tolstoi –que contiene 587.287 palabras– tendrán la misma longitud.
- b) *Cualquier cambio que se le realice al “input” originalmente identificado, generará un nuevo hash*. De esta manera si, en nuestro ejemplo, se le cambia una coma a la

⁹ Información obtenida de “Blockchain Explained”, A Reuters Visual Guide, por MaryAnne Murray, en <http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html> y de “Blockchain for Dummies”, Telmo Subira Rodriguez, en <https://medium.com/swlh/blockchain-for-dummies-d3daf2170068>.

obra de Tolstoi esto quedará inmediatamente evidenciado porque su *hash* cambiará. *El hash es como la “huella digital” del contenido del bloque*, con la particularidad de que tal huella digital se modifica automáticamente cuando cualquier parte del contenido del bloque es modificado.

4) Dado que cada bloque de la cadena contiene el *hash* del bloque anterior, *es imposible modificar un bloque sin modificar toda la cadena*. Por ejemplo: si un “hacker” intenta remover, agregar o modificar cualquier dato del bloque N° 1, el *hash* de ese bloque se modificará; como ese *hash* forma parte también del contenido del bloque N° 2, el *hash* del bloque N° 2 también se modificará, y la anomalía se propagará del mismo modo a todos los bloques posteriores al bloque atacado. *Esto motivará que el usuario o “nodo” que aloja la cadena atacada la declare inválida*.

5) *La Blockchain no requiere de ninguna autoridad de certificación de la autenticidad de su contenido y ello es posible porque los datos están distribuidos y replicados en todos los “nodos” de la red. Cada “nodo” o usuario tiene su propia copia de toda la cadena de bloques y las transacciones registradas en la misma* y distribuye información de cualquier nueva transacción al resto de la red. De esta manera, no es posible para nadie alterar la información de la cadena, por cuanto no está alojada en una única entidad individual sino en una amplia red de “nodos” o usuarios.

6) Una vez que un bloque de transacciones es validado, puede ser agregado a la cadena y cada “nodo” de la red actualiza su información local con dicho agregado. *Inclusive si un hacker pudiera modificar la cadena alojada en uno de los nodos, la red no aceptaría ningún block de la cadena alterada*.

7) Para armar redes **Blockchain** es necesario recurrir a plataformas informáticas específicamente diseñadas a tal efecto, que cuentan con todas las funcionalidades necesarias a tal fin (una de las más conocidas es Ethereum¹⁰).

D2) Contratos Inteligentes

El término “Contrato Inteligente” o **Smart Contract**, como se lo conoce en inglés, define *cualquier contrato que es capaz de ejecutarse a sí mismo. Están escritos en un código o programa de computación que puede ser “corrido” en una computadora o red de computadoras, en lugar de estar escritos en lenguaje legal en un documento impreso*¹¹.

El programa en cuestión –básicamente– constata el cumplimiento de las condiciones establecidas por las partes para que se ejecuten o “disparen” las acciones o prestaciones pactadas oportunamente. Un ejemplo de este concepto, que convive hace décadas entre nosotros, es la máquina expendedora de bebidas (*vending machine*): cuando la máquina (mediante un programa interno) constata que alguien ha introducido dinero suficiente y ha elegido su opción de bebida, entrega la bebida inmediatamente; se ha

¹⁰ Ver <https://ethereumclassic.org/>.

¹¹ El término “Smart Contract” fue acuñado por el científico de la computación y criptógrafo Nick Szabo, definiéndolo como *un conjunto de promesas, especificadas en formato digital, incluyendo protocolos en base a los cuales las partes cumplen estas promesas*. (Nick Szabo, “Smart Contracts: Building Blocks for Digital Markets”, 1996).

concretado automáticamente un contrato de compraventa de bebidas entre el usuario y el propietario de la máquina expendedora.¹²

En la actualidad, los contratos inteligentes permiten comerciar y hacer negocios a personas que no se conocen entre sí, normalmente a través de Internet, sin la necesidad de una autoridad centralizada que actúe como intermediaria en tales transacciones jurídicas. Un ejemplo claro de ello son las transacciones de la criptomoneda *Bitcoin*, que se producen diariamente y en forma masiva en distintas partes del mundo, entre perfectos desconocidos.

En cuanto al negocio del seguro, un ejemplo muy claro es el programa “Fizzy” de la aseguradora Axa, que provee un Seguro de Retraso y Cancelación de Vuelos que se puede contratar desde un dispositivo móvil y funciona automáticamente. El contrato inteligente constata –a través de la información de tráfico aéreo– el momento en que aterriza y despegue el avión en cuestión y, si verifica un retraso superior a las dos horas o la cancelación del vuelo, acredita en forma inmediata una suma prepagada de dinero en la cuenta bancaria elegida por el pasajero (el programa abarca actualmente el 80% de los vuelos que se realizan en el mundo)¹³.

4– IMPACTO EN LAS DISTINTAS ÁREAS OPERATIVAS DEL NEGOCIO DE SEGUROS

La aplicación de las nuevas tecnologías antes mencionadas al negocio del seguro está llamada a tener un gran impacto en la operatoria y en la estrategia del negocio de seguros.

Las nuevas generaciones de “asegurables”, muy familiarizadas con las tecnologías digitales, tienden a ser menos leales a una compañía en particular y tratan a los productos y servicios financieros y de seguros como intercambiables, en la medida en que satisfagan sus necesidades personales. Valorán la practicidad y la conveniencia y prefieren ejecutar sus transacciones en forma remota, en lo posible sin una interacción directa con la institución. Para las nuevas generaciones es claramente preferible el uso de canales digitales disponibles las 24 horas, los 7 días de la semana, para recibir una cotización o denunciar un siniestro, que tener que concurrir a una oficina de la compañía o de su productor de seguros a tal efecto¹⁴. Obviamente estas preferencias definirán nuevos modelos de productos y servicios en el mercado de seguros, en una tendencia que difícilmente tenga vuelta atrás¹⁵.

¹² Ejemplo citado en el trabajo de Eva-Maria Barbosa, 12/4/2018, publicado en http://www.aida.org.uk/docs/SmartContracts_Blockchain_legal_v3.pdf

¹³ Se puede visualizar la experiencia de contratación del seguro en <https://fizzy.axa/en-gb/>

¹⁴ Ver al respecto “Insurtech-the threat that inspires”, McKinsey, en <https://www.mckinsey.com/industries/financial-services/our-insights/insurtech-the-threat-that-inspires>.

¹⁵ Una medida del avance de esta tendencia es que la inversión global en empresas Insurtech se sextuplicó en tan solo 4 años, pasando de 493 millones de dólares en 2014 a 3177 millones de dólares en 2018. Ver informe en <https://fintech.global/global-insurtech-funding-tops-3bn-in-2018/>.

A continuación, nos referiremos a las prácticas que ya comienzan a perfilarse en las distintas áreas operativas de las compañías de seguros, para luego analizar los principales desafíos legales que ellas pueden implicar.

A) Diseño de productos y suscripción

Los dispositivos móviles “inteligentes” (IoT) y la telemática permiten ofrecer productos que implican un ahorro para los clientes y un riesgo más bajo para las aseguradoras. La tecnología móvil habilita productos estilo *Peer to Peer* o **P2P** (que podría traducirse como “entre pares o “entre iguales”) y seguros *Usage Based* o *Pay as you go* (que se activan y desactivan en base a la necesidad del asegurado y sólo se pagan por los períodos o el uso efectivamente cubierto).

Un ejemplo de seguro **P2P** es el que provee la empresa alemana Friendsurance, que está habilitada como *broker* de seguros y ofrece seguros del hogar, responsabilidad civil personal y seguro automotor. *Los asegurados con un mismo tipo de cobertura forman pequeños grupos* (entre amigos, familiares o buscados en el sitio web de la empresa). Una parte de las primas que paga el grupo va a una suerte de “fondo de reintegro” y, si el grupo no presenta siniestros, sus miembros pueden recuperar hasta el 40% de las primas pagadas –provenientes del “fondo de reintegro”– al final del período de cobertura. Los siniestros se pagan con el dinero del “fondo de reintegro” y por lo tanto éste se va reduciendo con cada siniestro pagado. Los siniestros que exceden los fondos disponibles en el fondo son cubiertos por aseguradoras tradicionales, con las cuales Friendsurance tiene acuerdos comerciales, *pero los miembros del grupo nunca deberán pagar más que las primas pactadas*.

El beneficio del seguro **P2P** es que *la “presión de los pares” alienta a los miembros del grupo a tener una conducta “antisiniestral” (evitando a veces denunciar siniestros de valor no significativo) y, asimismo, que los propios miembros del grupo buscan incorporar nuevos miembros para incrementar la base de asegurados y “atomizar” la distribución del riesgo*¹⁶.

Con respecto al seguro *Usage Based*, existen varios ejemplos en el Seguro Automotor. La aseguradora estadounidense Metromile cobra la prima del seguro en base a las millas efectivamente recorridas por el automóvil asegurado, ofreciendo tarifas especialmente bajas para los conductores que no llegan a un determinado mínimo anual de millas recorridas. A efectos de controlar el uso del vehículo la aseguradora instala gratuitamente un dispositivo inalámbrico en el mismo (IoT).

El seguro *Pay as you Go*, antes mencionado, permite obtener *protección asegurativa muy rápida* contra riesgos específicos *durante un período relativamente corto de tiempo*. Esta posibilidad resulta muy importante para el desarrollo de los Microseguros, en especial los que asisten a microemprendedores de bajos recursos económicos,

¹⁶ “Technology and innovation in the insurance sector”, OECD. <https://www.oecd.org/pensions/Technology-and-innovation-in-the-insurance-sector.pdf>.

los cuales en el pasado resultaban complicados de administrar y poco atractivos para los aseguradores desde el punto de vista de su rentabilidad.

Gracias a las posibilidades que otorgan las tecnologías de **Big Data** e **IoT** las aseguradoras pueden elaborar productos cada vez más específicos y adaptados al perfil del asegurado, *permitiendo decisiones de suscripción más “segmentadas”, apuntadas a premiar a los asegurados de bajo riesgo y estimular la prevención del siniestro* (más adelante hablaremos de las posibles objeciones jurídicas con respecto a esta estrategia).

Estas tecnologías también *permiten brindar cobertura a personas sin una historia siniestral que sirva de referencia a los efectos de cotizar la prima del seguro, o pertenecientes a sectores etarios que se perciben como especialmente riesgosos*. Por ejemplo, en el Seguro Automotor los adolescentes son normalmente considerados como un segmento de mayor riesgo pero, mediante los dispositivos inteligentes (**IoT**) –que aportan datos en tiempo real sobre el “estilo de manejo” de cada uno– puede resultar que un adolescente con estilo de manejo prudente pueda obtener un seguro más barato que alguien de edad más madura que maneja desaprensivamente¹⁷.

Lo mismo se puede decir para los seguros de vida, con respecto a personas de mayor edad, pero estilos de vida sanos y no sedentarios, lo cual se puede medir con “relojes inteligentes” del estilo del *Apple Watch* o el *Fitbit*. Existen ejemplos donde las aseguradoras ofrecen beneficios económicos a los asegurados que utilizan estos dispositivos y se comprometen a determinadas metas de actividad¹⁸.

También en el Seguro del Hogar podemos ver ejemplos de aseguradoras que proveen a sus asegurados de dispositivos inteligentes, que mediante múltiples sensores detectan peligros vinculados con fuego, humo, inundación, cortes de electricidad, etc. y avisan automáticamente al asegurado y a un servicio de seguridad y asistencia¹⁹.

En todos estos ejemplos podemos ver que *las posibilidades que otorga Insurtech pueden llevar a un cambio de paradigma: de la indemnización de las consecuencias del riesgo a la prevención del mismo*²⁰.

El contacto permanente entre asegurado y asegurador –vía dispositivos móviles– y la enorme cantidad de información que recibe el asegurador sobre el asegurado y los riesgos cubiertos, le permite a aquél no sólo analizar sino también predecir el comportamiento del asegurado y advertirlo sobre potenciales peligros.

¹⁷ En Argentina la aseguradora Integrity ofrece esta cobertura, denominada “Snapcar Integrity”. Se puede ver un video explicativo en <https://youtu.be/Y0VB-f6z55M>, que muestra con claridad el espíritu de este tipo de coberturas.

¹⁸ La aseguradora estadounidense John Hancock ofrece a sus asegurados relojes Apple Watch, que pueden resultar sin costo si los mismos cumplen determinados objetivos. Ver <https://www.johnhancockinsurance.com/vitality-program/apple-watch.html>.

¹⁹ Ver <https://www.the-digital-insurer.com/dia/bnp-paribas-internet-of-things-based-home-insurance-offering/>.

²⁰ “Insurtech: Where are we now”. Norton Rose Fullbright, Febrero 2017. <https://www.nortonrosefulbright.com/en/knowledge/publications/db154724/insurtech-where-are-we-now>.

Esto les permitirá a los aseguradores evaluar el riesgo cubierto con más precisión, determinar más acertadamente el precio de las coberturas y reducir la siniestralidad de sus asegurados.

En este sentido, algunos especialistas prevén que en el futuro la rentabilidad de las aseguradoras puede pasar más por los ingresos derivados de su función de asesores proactivos en la prevención del riesgo, que por las primas percibidas para la eventual indemnización del siniestro (muchas carteras estarán constituidas por asegurados de bajo riesgo –en gran medida gracias a las nuevas tecnologías– y eso derivará en un menor volumen de primas).

B) Comercialización

Aquí nos referiremos tanto a la comercialización directa (la realizada *por la propia aseguradora*) como la indirecta (realizada *a través de intermediarios*, como productores o *brokers*).

Como hemos visto hasta ahora, las técnicas vinculadas con *Insurtech* permiten al asegurador una relación más directa, interactiva y –en definitiva– más satisfactoria con el asegurado, desde el momento mismo de la oferta y venta de la cobertura asegurativa. Esto ha llevado a algunos especialistas a hablar de un efecto de “desintermediación” del negocio del seguro. Sin embargo, la realidad muestra que las *Insurtech* se están concentrando más en mejorar toda la “cadena del valor” del negocio de seguros que en “desintermediar” la relación con el cliente/asegurado²¹, y que las técnicas de *Insurtech* también pueden resultar de gran utilidad para mejorar la oferta de servicios de productores y *brokers*.

Con respecto a la venta directa, la tecnología de *Machine Learning* y los *chats-bots* permiten a las aseguradoras facilitar enormemente el proceso de cotización y venta de un seguro al consumidor final. Los *chats-bots* (o asesores robóticos), que usualmente adoptan nombres propios humanos, son capaces de mantener una conversación (muy específica, por cierto) con el cliente en lenguaje natural, guiándolo en todo el proceso de compra del seguro. Estos “diálogos” puede mantenerlos el cliente desde su dispositivo móvil en cualquier momento, normalmente sin intervención de agentes humanos, lo cual agiliza y hace más espontánea y atractiva la idea de contratar un seguro.

Si bien los “Contratos Inteligentes” se encuentran todavía en una etapa cuasi experimental en el negocio del seguro, ya permiten avizorar un futuro en el que muchos seguros simples y “parametrizados” (como el ejemplo del Seguro de Retraso y Cancelación de Vuelos *Fizzy* de AXA) permitirán un proceso totalmente automatizado desde la adquisición del seguro hasta el pago del siniestro.

²¹ Según un informe de la consultora Mc Kinsey, sobre un total de 500 casos comerciales bien conocidos, el 61% de las *Insurtech* se focalizó en mejorar y “empoderar” la cadena de valor y sólo el 30 % hizo foco en “desintermediar” la relación con el cliente/asegurado. Ver <https://www.mckinsey.com/industries/financial-services/our-insights/insurtech-the-threat-that-inspires>.

Con respecto a la comercialización indirecta, mediante productores y *brokers*, las tecnologías vinculadas con Inteligencia Artificial y asesoramiento robótico (*chat-bots*) permiten ir más allá de la experiencia ya exitosa de los *aggregators* o “agregadores”²², mejorando el proceso de comparación de cotizaciones y adquisición del producto finalmente elegido.

Cabe esperar también un papel importante de los intermediarios en el armado y administración de seguros **Peer To Peer**, cuyo funcionamiento describimos en párrafos anteriores.

C) Gestión de Siniestros

Las tecnologías vinculadas con Inteligencia Artificial, la **IoT** y la creciente conectividad con el asegurado a través de dispositivos móviles ofrecen enormes oportunidades para la agilización y automatización del proceso de administración de siniestros, desde el mismo momento de la notificación del evento y hasta la liquidación y pago del mismo.

Comenzando con la notificación inicial del siniestro, existen aplicaciones que permiten al asegurado informar de inmediato la ocurrencia del siniestro –con la asistencia de *chat-bots* en el proceso– e inclusive enviar fotos y videos a la aseguradora para facilitar la investigación y liquidación del mismo. Asimismo, los propios dispositivos inteligentes (**IoT**) que se encuentran en el vehículo, el hogar o la propia persona del asegurado, pueden detectar en tiempo real la ocurrencia del siniestro y aportar información valiosa a la aseguradora. Este acto inicia el proceso que luego continúa con la administración y tratamiento del siniestro, su liquidación, y finalmente su reparación o pago de la indemnización o beneficio pertinente.

Al recibir la primera notificación, las aplicaciones de Inteligencia Artificial pueden cumplir dos funciones de suma importancia:

1) Discriminar entre siniestros simples, de proceso automatizable, o siniestros complejos, que requieren de asistencia humana especializada para su procesamiento. Existen técnicas avanzadas de **Reconocimiento de Imágenes** y **Machine Learning** (y otras aplicaciones de **IA**) que permiten realizar esta “segmentación” automática de los siniestros. El propio sistema puede luego direccionar el reclamo hacia un proceso automatizado o asignarlo a un ajustador especializado para su tratamiento.

2) La **Inteligencia Artificial** aporta herramientas útiles para el reconocimiento temprano de situaciones de fraude. Actualmente existen aplicaciones que detectan indicios de fraude analizando las inflexiones de la voz y el lenguaje del denunciante, en un reclamo telefónico o en un diálogo por video. Las técnicas de **Big Data** y **Machine Learning** permiten detectar *patrones de fraude* en un siniestro determinado, basán-

²² Un agregador es un sitio web que permite obtener cotizaciones de distintas aseguradoras, llenando un formulario con los detalles del seguro a contratar. Normalmente no permiten la adquisición de la póliza elegida pero son un elemento muy útil para que el asegurable compare y elija. Dos ejemplos muy exitosos son comparethemarket.com y confused.com.

dose en la comparación con una enorme cantidad de situaciones similares, analizadas en tiempo real.

Si el siniestro es categorizado como simple, puede ingresar en un proceso automatizado de liquidación, reparación a través de una red de talleres autorizados de la aseguradora o, en su caso, pago de la indemnización o beneficio. Por ejemplo, la aseguradora estadounidense *Lemonade* posee un sistema de denuncia de siniestro guiada por *chat-bots*, que guía al asegurado para obtener el pago final del siniestro en cuestión de segundos²³.

También la conexión de la aseguradora, por vía telemática, a distintos registros públicos y privados, permitirá constatar la identificación del asegurado, titularidad de bienes asegurados y pre-existencia, etc., facilitando de este modo el trámite de validación del reclamo siniestral.

Cabe destacar que, con la ayuda de las tecnologías de **Big Data** e **IoT**, es probable que en el área operativa de siniestros de las aseguradoras se incorpore la propia prevención de los mismos. Por ej.: un “dispositivo inteligente” o “caja negra” instalado en el vehículo de un asegurado puede detectar señales de conducción errática o “distraída” por parte del mismo y enviar una advertencia por vía electrónica al conductor. En el seguro del hogar, el sistema puede enviar una advertencia de tormenta eléctrica al asegurado, aconsejándole de desconecte determinados aparatos electrodomésticos. Abundan los posibles ejemplos y todos permitirían una importante disminución de la siniestralidad²⁴.

Por último, y con relación a la tramitación de los siniestros, cabe prever una importante simplificación –en determinadas líneas de seguro– cuando se generalice la utilización de los **Smart Contracts**, dado que los mismos permiten la automatización de todo el proceso, desde la propia contratación del seguro hasta el eventual pago del beneficio.

4. ASPECTOS LEGALES E INTERROGANTES

Como hemos visto en los párrafos precedentes la aplicación de las tecnologías *Insurtech* abre enormes posibilidades en beneficio de los asegurados.

El mayor contacto e interacción entre aseguradoras y asegurados, y el procesamiento automatizado, “inteligente” y veloz de cantidades masivas de información, permitirán el desarrollo de productos más adaptados a los clientes, una más adecuada valoración del costo del seguro y, en definitiva, una mejor experiencia general para el asegurado.

Sin embargo, determinadas características de las tecnologías mencionadas, o la forma concreta en que sean aplicadas, puede llevar a situaciones que afecten los derechos de los asegurados y de terceros.

²³ “Claims in the digital age: How insurers can get started”, Abril 2018, McKinsey. <https://www.mckinsey.com/industries/financial-services/our-insights/claims-in-the-digital-age>.

²⁴ Ídem, nota anterior.

A continuación, analizaremos algunas de las cuestiones legales, que ya aparecen evidentes, sin pretender un análisis exhaustivo sino más bien “exploratorio” del tema.

A) Privacidad y protección de datos personales

Una de las más obvias preocupaciones deriva de las tecnologías vinculadas con **Big Data e IoT**: los dispositivos inteligentes que los asegurados mantienen en sus hogares o portan en sus automóviles –o sobre sí mismos– transmiten una enorme cantidad y variedad de información sobre el asegurado, y su tratamiento inadecuado puede afectar su privacidad y la de su grupo más cercano.

Los datos enviados por una “caja negra” ubicada en el automóvil del asegurado, o el reloj inteligente que lleva en su muñeca van más allá de los que son estrictamente necesarios para que la aseguradora determine el comportamiento (anti-siniestral o pro-siniestral) del asegurado y su impacto sobre las primas que debe pagar. Las aseguradoras no sólo tendrán datos sobre el comportamiento como conductor del asegurado sino también sabrán adonde viaja, que domicilios visita y con qué frecuencia.

Resulta de suma importancia que las aseguradoras traten con responsabilidad y corrección la información que reciben. En este sentido es primordial que respeten el principio de “minimización de datos” –tratamiento adecuado, pertinente y *limitado a lo necesario en relación a los fines para los que fueron recolectados*–, y que no conserven los datos personales más allá del plazo estrictamente necesario para el cumplimiento de la finalidad de su tratamiento.

Con respecto a las nuevas tecnologías, la legislación más avanzada y actualizada proviene de la Unión Europea: la resolución 2016/679, comúnmente conocida como **GDPR** (por *General Data Protection Regulation* –“Regulación General de Protección de Datos”) contiene disposiciones específicas relativas al *tratamiento de datos a gran escala (Big Data)* y el *proceso automatizado de toma de decisiones en base a datos personales*.

La legislación actualmente vigente en la Argentina (Ley N° 25.326, promulgada el 30/10/2000) no contiene actualmente disposiciones similares, pero el Poder Ejecutivo ha presentado al Congreso un proyecto de nueva Ley de Protección de los Datos Personales²⁵, que básicamente replica las disposiciones pertinentes de la **GDPR**.

Comentamos a continuación las más relevantes:

1) El proyecto introduce dos principios importantes para esta nueva era tecnológica: i) el principio de **responsabilidad proactiva**, que implica que el responsable o encargado del tratamiento *debe adoptar las medidas técnica y organizativas apropiadas* a fin de garantizar un tratamiento adecuado de los datos personales y de las obligaciones de la ley, y *que le permitan demostrar a la autoridad de control su efectiva implementación*; y ii) **la protección de datos desde el diseño y por defecto**, que significa que el

²⁵ Proyecto presentado ante el Congreso de la Nación el 19/9/2018. Ver texto completo en https://www.argentina.gob.ar/sites/default/files/mensaje_ndeg_147-2018_datos_personales.pdf.

responsable del tratamiento debe *aplicar medidas tecnológicas y organizativas tanto con anterioridad como durante el tratamiento de datos*, las cuales deben ser adoptadas *teniendo en cuenta el estado de la tecnología*, así como *el riesgo que entraña el tratamiento para el derecho de sus titulares*.

2) Con respecto al *tratamiento de datos en gran escala (Big Data)* el proyecto establece dos obligaciones de relevancia para los responsables del tratamiento de datos:

a) Deben designar un **Delegado de Protección de Datos**, quien: i) debe reunir condiciones de idoneidad, capacidad y conocimientos específicos para el cumplimiento de sus funciones, ii) *ejerce sus funciones sin recibir instrucciones de nadie y sólo responde al más alto nivel jerárquico de la organización* iii) tiene obligaciones muy específicas con respecto al diseño de los sistemas de tratamiento de datos y el cumplimiento de las disposiciones de la ley y iv) *actúa como referente ante la autoridad de control ante cualquier consulta* sobre el tratamiento de datos.

b) Deben llevar a cabo, en forma obligatoria, una **Evaluación de Impacto** relativa a la protección de datos personales cuando realicen el tratamiento de *datos sensibles a gran escala* (datos sensibles son básicamente los que afectan la esfera íntima de su titular con potencialidad de originar una discriminación ilícita y arbitraria como, *vg., la información referente a la salud*).

3) Con relación al *proceso automatizado de toma de decisiones en base a datos personales*, el proyecto incorpora importantes disposiciones:

a) Al referirse al derecho de acceso a los datos del titular de los mismos y la consecuente obligación a cargo del responsable del tratamiento de los datos, el proyecto establece que se debe informar expresamente “La existencia de decisiones automatizadas, incluida la elaboración de perfiles a que se refiere el art. 32 y, al menos en tales casos, información significativa sobre la lógica aplicada, sin que ello afecte derechos intelectuales del responsable del tratamiento” (art 28, inciso h).

Es importante destacar que el proyecto establece, en todos los casos, que “la información debe ser suministrada en forma clara, exenta de codificaciones y, en su caso, acompañada de una explicación de los términos que se utilicen, en lenguaje accesible al conocimiento medio de la población...” (art. 28, 1º párrafo). A nuestro modo de ver, *estas disposiciones son la clave para que el asegurado pueda detectar y –eventualmente– cuestionar judicialmente, cualquier sesgo discriminatorio en los algoritmos utilizados* para decisiones de suscripción o cotización de la prima, entre otras (tema al que nos referiremos con más detalle más adelante).

b) El art. 32 –1º párrafo– del proyecto establece que el titular de los datos “tiene derecho a oponerse a ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos, incluida la elaboración de perfiles, que le produzca efectos jurídicos perniciosos o lo afecte significativamente de forma negativa”. Si bien a continuación se plantea la excepción a este derecho cuando la decisión automatizada que es “...necesaria para la celebración o la ejecución de un contrato entre el titular de los

datos y el responsable del tratamiento” (como sería un contrato de seguros), el texto aclara más adelante que en ese caso “el responsable del tratamiento debe adoptar las medidas adecuadas para salvaguardar los derechos del titular de los datos”.

En conclusión, en base al texto comentado el asegurado no podrá oponerse a la utilización de decisiones automatizadas basadas en sus datos personales al suscribir un contrato de seguros, pero sí podrá exigir que la aseguradora tome todas las medidas necesarias para salvaguardar sus derechos, para –por ej.– evitar un trato discriminatorio (el **GDPR** –art. 22– menciona expresamente entre estas medidas el derecho a obtener la intervención de una persona humana en el proceso de decisión).

B) Posibles sesgos de los algoritmos. Discriminación

Cómo adelantamos al referirnos a la tecnología del Machine Learning y el funcionamiento de los algoritmos, su uso en sistemas automatizados de cotización y venta de seguros puede arrojar resultados sesgados o discriminatorios (tanto intencionados como no intencionados).

Un sistema automatizado de cotización puede valorar de forma exageradamente alta el costo de un seguro por la edad del solicitante, el lugar donde vive, etc. (lo que los sajones conocen como *profiling*). Ello puede llevar inclusive a que determinados sectores de la población no puedan acceder a una cobertura y resulten “*inasegurables*”.

Como vimos en su momento, los algoritmos son diseñados originalmente por humanos y pueden contener desde su origen una lógica intencionadamente sesgada o que pudiera considerarse discriminatoria. Pero con la tecnología del “aprendizaje automatizado” o *Machine Learning*, el propio sistema informático es capaz de generar nuevos algoritmos como parte de su proceso de aprendizaje, con lo cual la lógica del proceso puede volverse más opaca e impredecible, arrojando resultados no buscados por los humanos que diseñaron el sistema. Por las características señaladas, y en su caso, es muy importante que el titular de los datos tenga acceso a los mismos y a la forma en que son tratados y que reciba información precisa y en lenguaje inteligible al respecto por parte del asegurador (ver lo dispuesto por el Proyecto que hemos comentado en el punto A), apartado 3), inciso a) precedente).

Para el caso de violación de los derechos del titular de los datos, el proyecto prevé recursos administrativos ante la Autoridad de Aplicación y la posibilidad de iniciar una acción judicial de amparo de trámite sumarísimo (Acción de Habeas Data) “para tutelar los derechos que resulten restringidos, alterados, lesionados o amenazados por un tratamiento de datos personales contrario a la presente Ley por parte de las autoridades públicas o de particulares” (art. 80).

Cabe destacar que en la Argentina la Acción de Habeas Data está contemplada en la propia Constitución Nacional (en su art. 43, que también prevé el recurso de amparo “contra toda forma de discriminación”, entre otros supuestos de violación de derechos particulares o de incidencia colectiva).

La posibilidad de que los procesos automatizados de toma de decisiones vinculadas con el seguro arrojen resultados sesgados o discriminatorios es una preocupación bastante generalizada entre los especialistas del tema, a nivel mundial.

Se ha señalado que la posibilidad de entender la lógica interna o “explicabilidad” de un algoritmo es esencial para responder a los posibles reclamos relativos a resultados discriminatorios u otro tipo de consecuencias antijurídicas. Para mitigar estos riesgos, *es importante desarrollar herramientas operativas que permitan la “introspección” del algoritmo*, para proveer una explicación –en lenguaje llano– sobre sus operaciones y poder *mostrar registros auditables sobre la forma en que el algoritmo ha operado a lo largo del tiempo*²⁶.

C) Soporte exclusivamente digital de los contratos y las operaciones. Cuestiones de prueba

Una de las consecuencias de la “digitalización” de la relación entre asegurado y aseguradora –incluyendo los distintos aspectos de la interacción legal y contractual entre los mismos– que implica el fenómeno *Insurtech*, es que puede dificultar la prueba de las operaciones jurídicas realizadas y la efectiva manifestación de la voluntad de las partes.

Ya en la actualidad se pueden contratar seguros desde un teléfono celular y, de ahí en más, realizar todo tipo de actos jurídicos vinculados con el seguro contratado en forma digital.

En un futuro próximo seguramente se generalizarán los “contratos inteligentes” (*Smart Contracts*) que se suscriben con un simple “click” y se ejecutan totalmente sin intervención humana. A ello debemos agregar un futuro donde muchas transacciones y operaciones constarán únicamente en registros digitales descentralizados (DLT), en base a la tecnología *Blockchain*.

¿Cómo puede entonces acreditarse la propia existencia del contrato y sus operaciones vinculadas en el caso de ser necesario, por ejemplo, cuando surge un conflicto legal?

En la Argentina, la Ley de Seguros (N° 17.418) establece lo siguiente:

– El contrato de seguros es *consensual*; los derechos y obligaciones recíprocos del asegurador y el asegurado empiezan desde que se ha celebrado la convención, aún antes de emitirse la póliza (art. 4).

– El contrato de seguros solo puede probarse por escrito; sin embargo, *todos los demás medios de prueba, inclusive cualquier medio digital, serán admitidos, si hay principio de prueba por escrito* (art. 11).

Para determinar que considera la ley como *principio de prueba por escrito* debemos recurrir a lo dispuesto por el Código Civil y Comercial de la Nación (CCCN).

²⁶ BOWMAN, Courtney. “Insurtech Legal & Regulatory Challenges”, 12/4//2018, <http://www.aida.org.uk/docs/Data-Protection-and-Compliance-Challenges-InsureTech.pdf>.

A este respecto el art. 1020 se refiere al “principio de prueba instrumental” en los siguientes términos: “Se considera principio de prueba instrumental cualquier instrumento que emane de la otra parte, de su causante o de parte interesada en el asunto, que haga verosímil la existencia del contrato”.

A su vez, el art. 286 del CCCN se refiere al concepto de “*expresión escrita*” de la siguiente manera:

“La expresión escrita puede tener lugar por instrumentos públicos, o por instrumentos particulares firmados o no firmados, excepto en los casos en que determinada instrumentación sea impuesta. Puede hacerse constar en cualquier soporte, siempre que su contenido sea representado con texto inteligible, aunque su lectura exija medios técnicos”.

De acuerdo a lo expuesto, podemos concluir que, según el derecho argentino, tanto el asegurado como la aseguradora podrían acreditar la existencia del contrato mediante i) *cualquier instrumento emanado de la contraparte, de su causante o de la parte interesada, con texto inteligible, que haga verosímil la existencia del contrato* ii) *aunque no esté firmado* y iii) *que conste en cualquier soporte, inclusive obviamente el digital* y iv) *aunque su lectura exija medios técnicos*.

D) Implicancias sobre las obligaciones de información a cargo del asegurado

Como vimos en párrafos precedentes, las tecnologías de **Big Data e IoT** permitirán a las aseguradoras contar con abundante y detallada información sobre el estado del riesgo asegurado e inclusive sobre la ocurrencia de un siniestro y distintos aspectos del mismo.

Entendemos que tal realidad tendrá un impacto al momento de analizar las obligaciones de información del asegurado y las eventuales consecuencias de un incumplimiento formal de las mismas. Cuestiones como la reticencia, agravamiento del riesgo asegurado e información sobre el siniestro y sus circunstancias deberán tomar en cuenta el eventual conocimiento de las mismas por parte de la aseguradora gracias al uso de las tecnologías mencionadas.

E) Cuestiones de naturaleza regulatoria

Existen otras cuestiones legales, que son motivo de preocupación para los organismos de contralor en distintas partes del mundo:

a) Segmentación de los grupos asegurados vs. principio de solidaridad:

Tradicionalmente, el principio de solidaridad constituye uno de los pilares de la técnica del seguro. Las aseguradoras forman grupos numerosos de asegurados con coberturas homogéneas, pero, naturalmente, con diferentes niveles de riesgo. Si perjuicio de que puedan pagar distintos valores de prima en base a determinados parámetros (inclusive mecanismos de *scoring*), todos contribuyen a formar un fondo de primas

que permite pagar los siniestros sufridos por los distintos miembros del grupo. Bajo este sistema, y el principio de solidaridad, los asegurados con riesgo más bajo –y que no sufren siniestros– de alguna manera subsidian a los asegurados con mayor nivel de riesgo (vg. conductores menos prudentes o que circulan por barrios más peligrosos en el seguro automotor, o personas con una salud más frágil en el seguro de vida).

La posibilidad de que las aseguradoras obtengan información tan amplia y en tiempo real, mediante las tecnologías de *Big Data* e *IoT*, puede llevar a las aseguradoras a formar grupos *más segmentados* de asegurados de bajo riesgo y que muchos asegurados de riesgo más alto no puedan conseguir seguro (los “*inasegurables*” que mencionábamos en párrafos anteriores).

Dependerá de los organismos de contralor definir mecanismos y controles para evitar que eso ocurra, o mitigar su impacto.

b) Contextos regulatorios más “amigables” para las nuevas *Insurtech* (*Sandbox*).

Otro tema que analizan distintos organismos regulatorios es la eventual necesidad de que las nuevas *Insurtech* puedan manejarse inicialmente con regulaciones menos exigentes (vg. con respecto a capitales mínimos exigibles), dentro de un ámbito más acotado de actuación que las aseguradoras tradicionales, a los efectos de posibilitar su desarrollo y crecimiento.

El término inglés *sandbox* significa “corral de arena”, esos espacios donde los niños juegan en un entorno seguro y protegido, hasta que crecen lo suficiente para jugar libremente en todo el parque.

El tema es que estos *sandbox* regulatorios no impliquen una competencia desleal con las compañías tradicionales: esa es la medida de equilibrio que deben encontrar los organismos de contralor.

5. CONCLUSIONES PRELIMINARES

1) Resultan claros los beneficios de las tecnologías *Insurtech*, tanto para los asegurados como para las aseguradoras. Es previsible un crecimiento exponencial del fenómeno, por cuanto permite satisfacer la forma de operar y consumir de las nuevas –y no tan nuevas– generaciones. Hoy utilizamos nuestros celulares para comprar bienes y servicios de todo tipo (pasajes, alojamiento, electrodomésticos y toda especie de bienes muebles, servicios financieros, *delivery*, etc.) y obviamente las coberturas asegurativas no serán una excepción a esta tendencia.

2) Las nuevas tecnologías (especialmente *Big Data*, *IoT* y *Machine Learning*) otorgan enormes posibilidades a las aseguradoras para prever el futuro comportamiento de sus asegurados y prevenir siniestros. Resulta probable que presenciemos, quizás a largo plazo, un cambio del paradigma asegurador: de pagar siniestros a prevenirlos (mayores ingresos por la administración de los riesgos y menores ingresos por su cobertura asegurativa). Dicho sea de paso, este cambio estaría en línea con el que viene

experimentando el Derecho de Daños, a partir de los siniestros ambientales: *evitar el daño es siempre mejor que intentar repararlo*.

3) Las mismas tecnologías que reportan mayores beneficios para los asegurados, al permitir que las aseguradoras obtengan información para construir un perfil más certero de los mismos, ajustar más adecuadamente las primas y crear productos más convenientes a sus necesidades (*Big Data*, IoT y *Machine Learning*), son paradójicamente las que más riesgos implican para los asegurados en términos de privacidad y protección de datos personales. También se le debe prestar atención a posibles prácticas discriminatorias (intencionadas o no intencionadas) y al eventual problema de los “inasegurables”.

4) En términos de la profesión legal, cada vez aparece como más importante que los abogados adquiramos conocimientos multidisciplinarios, o al menos sensibilidad y respeto hacia los mismos. Es muy probable que los conflictos legales vinculados con el seguro involucren, cada vez más, ingredientes tecnológicos que debemos conocer para asesorar debidamente a nuestros clientes y defenderlos en juicio.

BIBLIOGRAFÍA

- ARPTÉG Anders (2018). General vs narrow artificial intelligence. Recuperado el 29 de mayo de 2019 en <https://medium.com/peltarion/general-vs-narrow-artificial-intelligence-d8faf296d4ab>.
- BARBOSA, Eva-María (2018). *Smart Contracts*. Recuperado el 29 de mayo de 2019 en http://www.aida.org.uk/docs/SmartContracts_Blockchain_legal_v3.pdf.
- BERRY, Nicholas (2017). *Insurtech: Where are we now*. Recuperado el 29 de mayo de 2019 en <https://www.nortonrosefulbright.com/en/knowledge/publications/db154724/Insurtech-where-are-we-now>.
- BOWMAN, Courtney (2018). *Insurtech Legal & Regulatory Challenges*. Recuperado el 29 de mayo de 2019 en <http://www.aida.org.uk/docs/Data-Protection-and-Compliance-Challenges-InsureTech.pdf>.
- <https://www.oecd.org/pensions/Technology-and-innovation-in-the-insurance-sector.pdf>
- Internet Society (2015). *The Internet of Things: An Overview*. Recuperado el 29 de mayo de 2019 en <https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf>.
- JAJAL, Tannya D. (2018). Distinguishing between Narrow AI, General AI and Super AI. Recuperado el 29 de mayo de 2019 en <https://medium.com/@tjajal/distinguishing-between-narrow-ai-general-ai-and-super-ai-a4bc44172e22>.
- MCKINSEY (2017). *Insurtech—the threat that inspires*. Recuperado el 29 de mayo de 2019 en <https://www.mckinsey.com/industries/financial-services/our-insights/Insurtech—the-threat-that-inspires>.
- MCKINSEY (2018). *Claims in the digital age: How insurers can get started*. Recuperado el 29 de mayo de 2019 en <https://www.mckinsey.com/industries/financial-services/our-insights/claims-in-the-digital-age>.

MURRAY, Mary Anne (2018). *Blockchain Explained*. Recuperado el 29 de mayo de 2019 en <http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html> y de.

OECD (2017). *Technology and innovation in the insurance sector*. Recuperado el 29 de mayo de 2019 en.

RODRÍGUEZ-PARDO, José Miguel (2017). *El Actuario ante Insurtech*. Recuperado el 29 de mayo de 2019 en https://www.fundacionmapfre.org/documentacion/publico/i18n/catalogo_imagenes/imagen_id.cmd?idImagen=1108971.

SUBIRA RODRIGUEZ, Telmo (2018). *Blockchain for Dummies*, Telmo SUBIRA RODRIGUEZ, Recuperado el 29 de mayo de 2019 en <https://medium.com/swlh/Blockchain-for-dummies-d3daf2170068>.

The Economist Intelligence Unit (2016). *Artificial Intelligence in the real world*. Recuperado el 29 de mayo de 2019 en https://perspectives.eiu.com/sites/default/files/Artificial_intelligence_in_the_real_world_0.pdf.