Inteligencia artificial: una herramienta eficaz para detectar el fraude al asegurador

por Florencia Mangialardi(*)

Sumario: I. Introducción. – II. El fraude en el mercado asegurador. – III. Una conceptualización de la inteligencia artificial (IA). – IV. El uso de la IA por parte de las aseguradoras para detectar el fraude. – V. Beneficios en el uso de la IA en la lucha contra el fraude. – VI. Algunos riesgos que trae el uso de la IA. *Sesgos*. *Ciberdelincuencia*. – VII. Conclusión.

I. Introducción

El fraude en el mercado asegurador es un fenómeno a nivel mundial(1) y es de gran relevancia ya que existen múltiples tipos de maniobras delictivas que hacen que las compañías aseguradoras gasten millones de dólares en siniestros fraudulentos. A su vez, a medida que la tecnología avanza, los defraudadores se van "perfeccionando" utilizando las herramientas que van surgiendo a su favor.

El mercado asegurador se ha basado tradicionalmente en procesos manuales con tareas que consumen mucho tiempo y recursos como la gestión de datos de clientes, la suscripción de pólizas, la tramitación de siniestros y la revisión de documentos, entre otros. Con los avances tecnológicos, las aseguradoras pueden automatizar prácticamente todos esos procesos, mejorar la eficiencia, reducir los costos y crear nuevas oportunidades de crecimiento, nuevos modelos de negocios y nuevos ecosistemas.

La inteligencia artificial(2) tiene el potencial para revolucionar el sector asegurador en muchas áreas del mercado y también en la prevención y detección del fraude.

II. El fraude en el mercado asegurador

El fraude a las aseguradoras representa un grave problema para las compañías, ya que afecta su rentabilidad y la confianza de los asegurados y atenta contra su transparencia.

Pero no solo afecta a las aseguradoras, sino que también perjudica a toda la sociedad ya que provoca que se pongan en marcha innecesariamente organismos del Estado(3), como policías, bomberos, ambulancias, hospitales, entre otros, generando así la desatención de emergencias reales. Todo esto, además, genera mayores costos para los usuarios de los sistemas.

Existen distintos tipos de fraudes contra el asegurador(4): el externo que es el cometido por el asegurado o por un tercero ajeno a la relación contractual; el interno que es el realizado por personal interno de la aseguradora, ya sea gerentes, empleados, productores, abogados, médicos; y el mixto que es el que se realiza en connivencia dolosa entre el asegurado o un tercero con los agentes internos de la aseguradora.

A su vez, puede ocurrir que la acción defraudadora sea una acción premeditada y planificada, a lo que llamamos "fraude duro", es menos frecuente y de mayores montos; o que sea una acción no premeditada de montos menores, pero más frecuente, a lo que denominamos "fraude blando" o "mentiras blandas", en donde muchos consideran que no tienen consecuencia, pero claramente no es así, ya que también es un delito, y aumenta el costo del seguro que pagan todos.

El mayor inconveniente que creo que existe en este tipo de maniobras fraudulentas es que no hay un reproche por parte de la sociedad, ya que en definitiva no existe conciencia en que estamos frente a verdaderos delitos penales, sino que se interpretan como si fueran simples actos de picardía, lo que se debe a que hay una falta de educación y publicidad al respecto.

Otro problema es que son de difícil detección, los costos en investigación son muy altos ya que hay muchos procesos que siguen realizándose de forma manual, consumiendo mucho tiempo, recursos y por supuesto dinero y muchas veces esas investigaciones no llegan a buen puerto. También es un problema que en muchos casos se investigan a asegurados honestos que se sienten agraviados y hay poco interés de las aseguradoras en realizar denuncias penales, solicitando en su caso el desistimiento de los reclamos.

III. Una conceptualización de la inteligencia artificial (IA)

Si bien no existe una única definición de IA, puede describirse como la reproducción o imitación de los procesos de la inteligencia humana por parte de las máquinas y en particular de los sistemas informáticos. Es decir que, a través de las máquinas, se intenta imitar los procesos que abarcan el aprendizaje, el razonamiento, la resolución de problemas, la comprensión y percepción del lenguaje. Su objetivo fundamental es desarrollar sistemas que puedan funcionar de forma inteligente y autónoma(5).

Es considerada la cuarta revolución industrial, ya que las tecnologías de IA, asociadas a los macrodatos o inteligencia de datos (*big data*), probablemente trastocará el equilibrio mundial(6).

El mundo se encuentra ahora en la cúspide de una revolución tecnológica en IA que puede resultar tan tras-

Nota de Redacción: Sobre el tema ver, además, los siguientes trabajos publicados en El Derecho: *Reflexiones derivadas de ciertos aspectos del siniestro y reparos doctrinarios que me aparecen de la interpretación de la Excma. Cámara en lo Comercial*, por Emilio H. Bulló, ED, 236-1077; *Seguro de responsabilidad civil. Citación en garantía. Dirección del proceso. El depósito en pago de la suma asegurada y accesorias devengadas, ¿libera al asegurador citado en garantía?*, por Carlos Alberto Schiavo, ED, 244-1039; *Sistema de factor de atribución en el Código Civil y Comercial*, por Carlos A. Ghersi, ED, 267-878; *Los supuestos expresamente contemplados en el nuevo Código que eximen –total o parcialmente– la atribución de la responsabilidad*, por Juan Francisco González Freire, ED, 274-813; *Apuntes en torno a las medidas mitigadoras en el Código Civil y Comercial argentino, con especial atención a la responsabilidad civil por incumplimiento contractual*, por Daniel L. Ugarte Mostajo, ED, 275-504; *Criterios de atribución de responsabilidad civil. Razones de su evolución desde Vélez Sarsfield hasta el Código Civil y Comercial*, por Fernando Alfredo Ubiría, ED, 277-724; *Ilegalidad de la suspensión automática de cobertura por mora en el pago de seguro*, por Pablo Fernando Ceballos Chiappero, ED, 284-52; *Derecho de seguros: prescripción de las acciones derivadas del contrato de seguros. Necesidad de una armonización jurídica*, por Marcelo Oscar Vuotto, ED, 291-634; *¿Notificar o no notificar? La suspensión de cobertura asegurativa y el deber de información. A propósito de un fallo del STJ de La Pampa*, por Martín Moller Rombola, ED, 294-1131; *Criptoactivos: su interés asegurable y la aversión al riesgo*, por Sergio Sebastián Cerda, ED, 301; *Seguro de Riesgo Cibernético y las exclusiones de cobertura*, por Sergio Sebastián Cerda, ED, 301; *Nuevas tecnologías y seguros: inteligencia artificial y nuevos desafíos para la industria del seguro*, por Juan Ignacio Di Vanni, ED, 303. Todos los artículos citados pueden consultarse en www.elderechodigital.com.ar.

(*) Abogada egresada de la Facultad de Derecho y Ciencias Sociales, Universidad Católica Argentina (sede Rosario). Profesora Nivel Superior, Facultad de Derecho y Ciencias Sociales, Universidad Católica Argentina (sede Rosario). Especialista en Derecho de Seguros, Universidad de Salamanca, España. Especialista en Derecho de Daños, Pontificia Universidad Católica Argentina (CONEAU Res. 403/09). Especialista en Derecho Ambiental ante la Globalización, Universidad de Castilla La Mancha, Toledo, España. Presidente del Grupo Internacional de Trabajo "Combate contra el Fraude en el Seguro", del Comité Ibero-Latinoamericano (CILA) de la Asociación Internacional de Derecho de Seguros (AIDA).

(1) Por tal motivo hay muchas asociaciones que estudian el tema y la manera de combatir el fraude. Entre ellas, el Comité Ibero-Latinoamericano (CILA) de la Asociación Internacional de Derecho de Seguros (AIDA) tiene un grupo internacional de trabajo "Combate contra el Fraude en el Seguro"; CESVI fomenta lo que ha dado en llamar Cultura antifraude en Latinoamérica, organizando un concurso de casos de combate al fraude en seguros en la región; CESI Internacional organiza congresos y seminarios antifraude, anticorrupción y *compliance*.

(2) En adelante, IA.

(3) Andekian, L., "Cultura antifraude: los casos más exitosos de detección de fraudes en el mercado asegurador", Sesión Grupo de trabajo CILA, Combate contra el Fraude en el Seguro, disponible en www.youtube.com@asociacioncolombianadedere5994 (fecha de consulta: 29/4/2024), Asociación Colombiana de Derecho de Seguros (ACOLDESE); 10 de mayo 2023, disponible en https://www.youtube.com/watch?v=lL5iB2D6Ae8&t=683s (fecha de consulta: 29/4/2024).

(4) Compiani, M. F., "El fraude y su impacto en el Seguro", PDF, disponible en http://www.aidaargentina.com/wp-content/uploads/el-fraude-y-su-impacto-en-el-seguro.pdf (fecha de consulta: 29/4/2024).

(5) EALDE Business School; Webinar "Inteligencia artificial en seguros: oportunidades y amenazas", noviembre de 2023, disponible en http://www.youtube.com/@EaldeEs (fecha de consulta: 29/4/2024).

(6) UNESCO, "La cuarta revolución", 29/6/2018, disponible en https://courier.unesco.org/es/articles/la-cuarta-revolucion (fecha de consulta: 29/4/2024).

formadora para el crecimiento económico y el potencial humano como fueron la electrificación, la producción en masa y las telecomunicaciones en sus épocas[7].

La IA avanza a un ritmo acelerado y puede tener grandes beneficios para la humanidad. Sin embargo, su rápido avance también puede llevar a consecuencias negativas[8]. Actualmente la IA generativa[9] ha alcanzado una adopción sin precedentes, intensificando la preocupación por su impacto ético y legal, centrándose el debate en el marco laboral, la creación de contenido falso, la gestión de la propiedad intelectual, así como en la protección de los datos. De hecho, en marzo de 2023, el *Future of Life Institute* (con la participación de Elon Musk) pidió la pausa del desarrollo de IA hasta que se establezcan regulaciones que garanticen un uso ético. Es por ello que la Inteligencia Artificial Responsable (RAI) busca garantizar el buen uso de la IA y mitigar sus riesgos, siguiendo los principios, procesos y políticas necesarios para garantizar que la tecnología se desarrolla y opera siempre buscando un impacto positivo y protegiendo a los individuos y la sociedad[10].

IV. El uso de la IA por parte de las aseguradoras para detectar el fraude

Los modelos basados en *machine learning* o aprendizaje automático[11] permiten construir sistemas de predicción o clasificación con el objetivo de mejorar los diferentes procesos de gestión que se dan en las compañías de seguros. Al analizar grandes volúmenes de datos, se puede predecir el riesgo de siniestros y detectar patrones sutiles que indican posibles fraudes.

- Agentes conversacionales: Los *agentes conversacionales* son una de las herramientas más utilizadas. Son un tipo de tecnología que usa inteligencia artificial y que permite al sistema interacciones similares a las humanas. Combinan técnicas de *machine learning*, como procesamiento de lenguaje natural, reconocimiento de texto, reconocimiento de voz y sistema de gestión avanzada de diálogo, con el fin de replicar de la manera más precisa la interacción humana. Su principal objetivo es lograr una comunicación fluida y natural entre humanos-máquina, y tiene la capacidad de procesar cada pregunta formulada comprendiendo el contexto, tal y como lo haría un ser humano[12], por lo que no solo están siendo muy usados para ayudar a los clientes a encontrar información sobre las opciones y condiciones de las pólizas, hacer pagos y presentar reclamos, sino también para detectar fraudes.

Es el procesamiento del lenguaje natural (NLP) el que permite entender y procesar el lenguaje humano. En el sector de los seguros se utiliza, por ejemplo, para la clasificación de documentos de los clientes en diferentes categorías como pólizas de seguros, reclamaciones, facturas, etc., y como herramienta para la atención al cliente. También se utiliza para la evaluación de riesgos, ya que al analizar grandes cantidades de datos como informes de siniestros e informes de inspección se logran tomar decisiones más informadas sobre la suscripción y la fijación de precios. En lo que respecta a la detección de fraude: no solo se analizan los informes de siniestros e inspección, sino que además los correos electrónicos, chats, grabaciones y llamadas para extraer toda la información útil y detectar patrones sospechosos, lo que ayuda a las compañías de seguros a identificar y prevenir el fraude de manera más efectiva.

- Sistemas basados en visión artificial: La visión artificial es una tecnología que permite interpretar y comprender el mundo visual que la rodea. En el sector de los seguros se lo puede utilizar para analizar imágenes y videos con el fin de identificar fraudes, evaluar daños y mitigar riesgos. Con esta tecnología se puede contar personas, detectar movimientos, realizar un análisis demográfico, identificar acciones e interacción entre elementos y analizar objetos y patrones que pueden pasar desapercibidas a la vista humana.

La visión artificial puede ser utilizada por las aseguradoras, por ejemplo, para analizar imágenes de accidentes entre vehículos y evaluar los daños para determinar cuánto puede costar la reparación, lo que ayudaría a detectar los fraudes en las reclamaciones. Este tipo de IA, si fuera utilizado en los procesos judiciales, podría contribuir a evitar no solo el fraude sino también los desgastes jurisdiccionales absolutamente innecesarios que estos reclamos traen aparejados.

A través de esta tecnología también podrían realizarse los análisis de las redes sociales de los reclamantes ya que en las mismas en general hay mucha información y su correcto análisis puede resultar muy eficaz para las aseguradoras a la hora de detectar engaños.

- Sistema de reconocimiento facial y de reconocimiento de voz: Tanto el reconocimiento facial como el de voz son aplicaciones de software biométricos con capacidad para identificar o comprobar de forma única a una persona. En el caso del reconocimiento facial, se realiza a través del análisis de patrones basados en sus contornos faciales, es decir, se trata de una autenticación biométrica que identifica a las personas a través de la medición de la forma y estructura únicas de sus caras. Aunque hay más de un programa de reconocimiento facial y pueden emplearse diferentes técnicas, todos funcionan sobre los mismos principios de identificación biométrica, como los escáneres de huellas digitales o el reconocimiento de voz[13]. Con ella podemos distinguir los rostros y las voces de los criminales.

- Cámaras: Por supuesto que todo elemento tecnológico que pueda filmar es una herramienta absolutamente útil a la hora de detectar un posible fraude contra el asegurador, por lo que las cámaras de seguridad en la vía pública como así también los drones y las *dash cam*[14] son fundamentales a tales fines.

Los drones permiten la recolección de información y análisis de zonas de difícil acceso, mediante cámaras de alta resolución. Pueden emplearse para numerosas tareas y resultan de gran utilidad, por ejemplo, en la comprobación de los siniestros agrícolas.

En otras oportunidades, he propuesto que a la hora de suscripción de un seguro automotor las compañías impongan la instalación y el uso de las "*dash cam*" a sus clientes ya que con dicho instrumento se pueden corroborar la veracidad de los accidentes y recopilar pruebas en caso de cualquier incidente[15].

- Sistemas de rastreo: Los sistemas de rastreo se están utilizando mucho y sobretodo en los casos en donde se produce un siniestro de robo o hurto de un vehículo. Hay distintas variedades de rastreos que aplican diferentes tecnologías, pero en definitiva lo que hace la diferencia es saber dónde estaba el vehículo en el momento en que se haya producido el robo o hurto del mismo[16].

(7) Etcheberry, M., "El impacto de la Inteligencia artificial en el mundo del trabajo", en Corvalán, J. G. (dir.), *Tratado de Inteligencia Artificial y Derecho*, Tomo III; Ciudad Autónoma de Buenos Aires, La Ley, 2021, p. 95.

(8) Kutter, G. E., "Inteligencia artificial y ética, un desafío para el mundo actual", *Microjuris*, 30/8/2023. Cita: MJ-DOC-17351-AR||MJD17351.

(9) La IA generativa es la que genera nuevo contenido, a partir de datos con los que han sido entrenados, a diferencia de los sistemas de IA tradicionales que no generan contenido, sino que a partir de datos reconocen patrones para predecir resultados. Véase, Colombo, M. C., "ChatGPT en la industria del Seguro. Algunas consideraciones en torno a su aprovechamiento, *Revista de Derecho de Seguros*, número 5, julio 2023, Cita: IJ-IV-DLXVI-799.

(10) MAPFRE, "Inteligencia Artificial Responsable", disponible en https://www.mapfre.com/media/Informe-IA-Responsable_-MAPFRE-Open-Innovation.pdf (fecha de consulta: 29/4/2024).

(11) Es un componente crucial de la inteligencia artificial que le permite aprender a través de algoritmos que se entrenan con base en datos suministrados. El algoritmo es capaz de modificar su propio comportamiento basándose en los datos de que dispone, por lo que se adapta y aprende de manera continua, mejorando su precisión con el tiempo.

(12) Colombo, M. C., "ChatGPT en la industria del Seguro. Algunas consideraciones en torno a su aprovechamiento; *Revista de Derecho de Seguros*, número 5, julio 2023. Cita: IJ-IV-DLXVI-799.

(13) Puglia, A. D., "Inteligencia artificial aplicada a la seguridad."; en Corvalán, J. G. (dir.), *Tratado de Inteligencia Artificial y Derecho*, Tomo II, Ciudad Autónoma de Buenos Aires, La Ley, 2021; p. 440.

(14) Se trata de cámaras de video diseñadas para colocar en el interior del vehículo, apuntando hacia delante, que registran todo lo que acontece frente al vehículo.

(15) En algunos países son obligatorias y en otros están prohibidas o al menos se desaconseja su uso por vulnerar el derecho a la privacidad de las personas que circulan por la vía pública, entre otros riesgos.

(16) Betancur Ruiz, C. A., "Nueva tecnología de rastreo de vehículos, como ayuda en la detección de fraudes de seguros, escenario actual en Brasil", Asociación Colombiana de Derecho de Seguros (ACOLDESE), Sesión Grupo de trabajo CILA. Combate contra el fraude en el seguro, 10 de mayo 2023, disponible en https://www.youtube.com/watch?app=desktop&v=lL5iB2D6Ae8&t=683s (fecha de consulta: 29/4/2024).

V. Beneficios en el uso de la IA en la lucha contra el fraude

Lo interesante de la utilización de la inteligencia artificial en la detección del fraude es que esta tecnología podrá no solo recabar toda la información, sino que además podrá analizarla, lo que puede resultar muy beneficioso en la identificación temprana de fraudes. Con ella se mejora la eficiencia del proceso e incrementa la precisión, lo que hace que haya una reducción significativa de los falsos positivos y disminuye a su vez la necesidad de revisar manualmente reclamaciones legítimas.

Asimismo, hay una reducción en los costos de investigación y a través del análisis de datos históricos hay una prevención de futuros fraudes.

VI. Algunos riesgos que trae el uso de la IA

Por supuesto que, al igual que en cualquier otro ámbito, el uso de esta tecnología trae aparejados algunos riesgos complejos como ser los sesgos y la discriminación que puede haber en estas decisiones automatizadas y también la protección de la privacidad de los datos de los asegurados, entre otros, por lo que deberán gestionarse de manera adecuada para poder aplicarla de forma segura, confiable y, en definitiva, sostenible[17].

Sesgos

Los agentes conversacionales pueden verse afectados por algoritmos sesgados que lo pueden llevar a tomar decisiones incorrectas a la hora de evaluar un posible fraude o detectar a los defraudadores.

Principalmente, la cuestión radica en que son las propias personas a cargo del manejo de los algoritmos quienes le transfieren –consciente o inconscientemente– sus sesgos, promoviendo así la discriminación directa e indirecta, y reafirmando prejuicios e inequidades frente a identidades diversas, nacionalidad, género, nivel adquisitivo o color de piel[18].

La toma de decisiones de las personas no es ajena al error ni a la subjetividad. No obstante, en el caso de la IA, esta misma subjetividad puede tener efectos mucho más amplios, y afectar y discriminar a numerosas personas sin que existan mecanismos como los de control social que rigen el comportamiento humano[19].

Existe un consenso generalizado en cuanto a que uno de los requerimientos para una regulación que apunte a prevenir la discriminación con el uso de algoritmos es la transparencia. Los algoritmos deben ser auditables, transparentes y explicables[20].

Ciberdelincuencia

Por medio de la IA se recolectan, analizan y utilizan datos de los clientes que pueden contener información sensible tales como antecedentes médicos, crediticios, etc.

A medida que se expanden las capacidades de las tecnologías basadas en IA, también lo hace su potencial de explotación criminal[21].

Los delincuentes informáticos buscan obtener acceso no autorizado a esos datos de los clientes para fines malintencionados, como fraude, robo de identidad o espionaje. Si los datos no están debidamente protegidos estos riesgos van a aumentar significativamente comprometiendo así la seguridad del asegurado y de la aseguradora.

En definitiva, el mercado asegurador está expuesto a lo que llamamos ciberataque, que es el esfuerzo intencionado de robar, exponer, alterar, inutilizar o destruir datos, aplicaciones u otros activos mediante el acceso no autorizado a una red, sistema informático o dispositivo digital[22].

Actualmente hay una gran cantidad de ciberdelitos, y distintos tipos de ataques[23], que generan enormes y diversos daños, no solo por la afectación de datos personales o confidenciales, sino también perjuicios económicos por el impacto reputacional negativo, la interrupción de actividad (en caso de que así se haya hecho), los costos de recuperación para la desinfección de la infraestructura, entre muchos otros.

Los aseguradores tienen que asegurarse de que los datos confidenciales de los clientes estén debidamente encriptados, seguros, actualizados, monitoreados para detectar cualquier actividad sospechosa.

VII. Conclusión

El fraude a las aseguradoras es un mal que aqueja a la sociedad y muy difícil de erradicar por la falta de conciencia en cuanto a que estamos frente a delitos penales que nos afectan a todos y no solo a las compañías de seguros.

Existen múltiples herramientas que ofrece la tecnología, que las aseguradoras pueden aprovechar no solo para crecer en el mercado sino también para poder detectar y prevenir los fraudes, debiendo tomar las medidas necesarias para garantizar que estos modelos de inteligencia artificial no contengan sesgos y estén diseñados para resistir una posible manipulación por parte de los defraudadores.

Es un gran desafío para las empresas de seguros anticiparse y así utilizar las herramientas tecnológicas y la inteligencia artificial para detectar y prevenir el fraude de manera más eficiente y precisa, protegiendo así sus intereses y los de sus asegurados.

VOCES: SEGURO - DAÑOS Y PERJUICIOS - RESPONSABILIDAD CIVIL - CÓDIGO CIVIL Y COMERCIAL - CONTRATO DE SEGURO - NEGOCIO COMERCIAL - INTERNET - TECNOLOGÍA - INFORMÁTICA - DELITO INFORMÁTICO - OBLIGACIONES - CONTRATOS - ACTOS DE COMERCIO - SEGURO DE RESPONSABILIDAD CIVIL - GRUPOS ECONÓMICOS - PERSONAS JURÍDICAS - CLÁUSULAS CONTRACTUALES - *PHISHING* - BASE DE DATOS - ENTIDADES FINANCIERAS - COMUNICACIONES ELECTRÓNICAS

(17) MAPFRE, "Inteligencia Artificial Responsable", disponible en https://www.mapfre.com/media/Informe-IA-Responsable_-MAPFRE-Open-Innovation.pdf (fecha de consulta: 29/4/2024).

(18) Martínez, C. I., "Responsabilidad civil derivada del uso de algoritmos: la cuestión de la jurisdicción internacional cuando el demandado no cuenta con radicación en Argentina", *Microjuris*, 27/2/2021. Cita: MJ-DOC-15787-AR|MJD15787.

(19) Caraballo, M., "Inteligencia artificial. Inequidad y discriminación en cajas negras", en Corvalán, J. G., (dir.), *Tratado de Inteligencia Artificial y Derecho*, Tomo I, Ciudad Autónoma de Buenos Aires, La Ley, 2021, p. 287.

(20) Tolosa, P., "Algoritmos, estereotipos de género y sesgos. ¿Puede hacer algo el derecho?", en Corvalán, J. G., (dir.), *Tratado de Inteligencia Artificial y Derecho*, Tomo I, Ciudad Autónoma de Buenos Aires, La Ley, 2021, p. 328.

(21) Puglia, A. D., "Inteligencia artificial aplicada a la seguridad."; en Corvalán, J. G., (dir.), *Tratado de Inteligencia Artificial y Derecho*, Tomo II, Ciudad Autónoma de Buenos Aires, La Ley, 2021, p. 447.

(22) Zapiola Guerrico, M., "Los ciberataques y su impacto en el seguro", *Revista de Derecho de Seguros*, número 5, julio 2023. Cita: IJ-IV-DLXVI-803.

(23) Rubén, R., "25 Tipos de ataques informáticos y cómo prevenirlos", 20 de enero de 2018, disponible en https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/ (fecha de consulta: 29/4/2024).