COMISIÓN N° 3
DERECHO DE DAÑOS

PONENCIAS

XXIX Jornadas Nacionales de
Derecho Civil
Buenos Aires, Argentina | 2024

UNIVERSIDAD
AUSTRAL

ÍNDICE

DAÑOS EN LA ERA DIGITAL: SESGOS ALGORÍTMICOS Y DISCRIMINACIÓN

Por Agustín Emanuel Álvarez Haron[1]

I. CONCLUSIONES

1. Luego de haber investigado y analizado cómo las inteligencias artificiales (que de hecho las encontramos a diario en el uso de las distintas plataformas que nos permiten escuchar música, mirar películas, etc;) impactan en nuestro día a día; he arribado a la conclusión de que tenemos la necesidad de contar con una rigurosa regulación en pos de brindar una mayor tutela a derechos tan fundamentales como lo es el derecho a la intimidad o el derecho a la imágen; ya que estas nuevas tecnologías influyen en ellos y los avasallan día a día.

2. Creo que la tecnología sigue avanzando a pasos agigantados y si bien hay sistemas que nos ayudan y parecieran brindarnos grandes ventajas en nuestra vida cotidiana, lo cierto es que como contrapeso podemos observar los grandes riesgos a los que nos encontramos sometidos como sociedad en todo el mundo, como consecuencia frente al avance y el crecimiento exponencial de estas nuevas tecnologías. En efecto, me parece que las juezas y jueces deberán a la hora de juzgar un caso de daños producto del uso indiscriminado de las IA, tener muy presente la función preventiva del derecho de daños, ya que justifica y activa su accionar, precisamente, el devenir de esos nuevos sistemas. En especial, producto de los sesgos caracterizantes de los algoritmos que se forman por la recolección de datos, en rigor de verdad, no es más que un claro reflejo de una sociedad machista y discriminatoria en la que , en líneas generales, seguimos conviviendo.

3. Es por eso que frente a este gran avance de la tecnología que avasalla consigo derechos de tal magnitud, se requiere una mayor

---

1 Agustin Emanuel Alvarez Haron, abogado recibido de la Facultad de Derecho de la Universidad de Buenos Aires con título en trámite orientado en Derecho Privado; con el aval de la Dra Julia Gomez, profesora Adjunta interina de las materias Obligaciones Civiles y Comerciales I y II en la Universidad Nacional de José c Paz; de la materia Derecho del Consumidor de la facultad de Derecho de la Universidad de Buenos Aires y de la materia Instituciones del Derecho Público I en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

actualización legislativa en pos de una mayor protección al ejercicio de derechos tan fundamentales como lo es el derecho a la intimidad o el derecho a la imágen, entre tantos otros.

4. Por último, es dable destacar la importancia de la protección de los datos personales (conf Ley 25.326 y CN); más aún en especial aquellos datos sensibles, dado que en relación al fallo que mencionare en el último capítulo, se debe afianzar una perspectiva de Derechos Humanos a la hora de regular a la IA y a la hora de analizar un caso de daños derivado del impacto de estas mismas.

II. FUNDAMENTOS

1. INTRODUCCIÓN

A lo largo del presente trabajo, me detendré en explicar y analizar el impacto de la actividad de los sistemas de Inteligencia artificial y cómo ello influye en el ejercicio regular de nuestros derechos, aun así, de aquellos inherentes a nuestra persona.

Trataré de remarcar la importancia de identificar aquellos sesgos que se encuentran plasmados en los patrones y algoritmos propios de la IA y cómo ello puede dar lugar a una acción de daños y, por lo tanto, originar una obligación de indemnización.

Por último, analizaré el fallo SyRI y lo mencionaré como una novedad jurisprudencial de la Corte de la Haya; y trazaré un paralelismo para luego explicar cómo se configurarán los 4 presupuestos de la responsabilidad civil en un caso hipotético de daños en el marco de la actividad indiscriminada de una Inteligencia Artificial en nuestra Argentina.

2. NUEVAS TECNOLOGÍAS: SU IMPACTO EN LOS DERECHOS PERSONALÍSIMOS.

Es ineludible negar que desde las últimas décadas del siglo pasado, nos encontramos atravesando un gran cambio producto de la aparición de las nuevas tecnologías. Desde mi corta edad de 24 años, puedo asegurar sin

duda alguna que la infancia de un niño de hoy en día, es distinta a la que tuve en mi niñez, pese a haber nacido bajo el predominio del Internet[2].

Actualmente nos encontramos inmersos en un mundo en el cual nuestras vidas transcurren a través de una pantalla de cualquier dispositivo electrónico. Estamos inmiscuidos en sociedades que, frente a este crecimiento exponencial por parte de las tecnologías que a priori pareciera no tener techo alguno, son realmente muy dinámicas. Este constante cambio como consecuencia de la rapidez y fluidez que provoca esta revolución tecnológica tan latente, introduce ciertos riesgos y, como consecuencia, la imperiosa necesidad de contar con un marco regulatorio que los contemple.

En este sentido, vale decir que el avance tecnológico a nivel mundial, genera un gran temor por parte de las sociedades del nuevo milenio. Es por ello que frente a estos riesgos producto de toda la mencionada evolución tecnológica, nuestro ordenamiento jurídico se ve obligado a contemplar estas nuevas circunstancias.

Ahora bien, como ya he mencionado, el avance tecnológico que influye y entrelaza nuestras sociedades, impacta de lleno en nuestros derechos reconocidos y contemplados por nuestro ordenamiento jurídico tales sea como en los derechos personalísimos; como así también, en aquellos derechos desde la primera hasta la tercera generación.

En efecto, cabe mencionar a modo de ejemplificación, aquél proceso que se encontraba en plena gestación al cual se lo denominó como "Digitalización del sistema de salud"; acaecido en todo el mundo y acrecentado producto de la pandemia mundial por el COVID-19[3].

Frente a este proceso, la tecnología ofrece mejorar las prestaciones de salud como así también la digitalización propia del sistema de salud.

---

[2] Red informática mundial, descentralizada, que permite la transferencia casi inmediata de datos entre ordenadores; Real Academia Española.

[3] Enfermedad por Coronavirus (Covid-19); la cual fue advertida por primera vez en la localidad de Wuhan (china) el 31 de Diciembre de 2019; Organización Mundial de la Salud, sitio Web Oficial https://www.who.int/es/emergencies/diseases/novel-coronavirus-2019?adgroupsurvey={adgroupsurvey}&gad_source=1&gclid=Cj0KCQjwiOy1BhDCARIsADGvQnAUHvNVKsspck5X2_7Vorp0sdI3r2WBgw4MXaxm7x6EkwsPS9Zi_IIaAsS2EALw_wcB

En tal sentido y gracias a esta nueva realidad, la Organización Panamericana de la Salud[4] , a nivel internacional, se vió obligada a otorgar un marco regulatorio por lo que procedió a fijar ocho principios rectores para el uso apropiado de las tecnologías de información y comunicación[5].

De este modo podemos observar cómo la tecnología en la actualidad se ha inmiscuido en un terreno tan sensible como lo es el derecho a la vida y a la salud; es decir, se ha entrometido en aquellos derechos personalísimos de las personas que se encuentran íntimamente vinculados entre sí, contemplados y protegidos por nuestra Constitución Nacional[6] junto a los pactos y tratados internacionales. Vale recordar que los derechos personalísimos son aquellos que se caracterizan por ser innatos, precisamente, ya que son necesarios, esenciales,vitalicios de cada persona misma, en efecto.

Asimismo, cabe destacar que el sector de la salud es el que más utiliza la implementación de los Sistemas de Inteligencia Artificial (IA); producto de su gran utilidad científica como así también de su gran expeditez.

Antes de analizar las ventajas de la implementación de la Inteligencia Artificial en el ámbito de la salud, creo conveniente definir y explicar qué es una Inteligencia Artificial. Esta última encuentra diversas definiciones, pero puedo mencionar aquella que la describe como una disciplina que se encarga de comprender o construir entidades inteligentes. Actualmente, las IA se basan en métodos de aprendizaje automáticos/profundos que emplea algoritmos que imitan la estructura de las redes neuronales[7].

Retomando el campo de la "salud digitalizada"; vale decir que si bien las IA en dicho ámbito ofrecen ciertas ventajas como, por ejemplo, la rapidez

---

[4] La Organización Panamericana de la Salud es el organismo especializado de salud del sistema interamericano, encabezado por la Organización de los Estados Americanos, y también está afiliada a la Organización Mundial de la Salud .https://www.paho.org/es

[5]BETTINA BLANCO, *Valeria*; pág 191 en *La Disrupción Digital y sus impactos en el ser humano: una mirada jurídica; Directora* WEINGARTEN, Celia; Santa Fe Rubinzal- Culzoni, 2023.

[6] Constitución Nacional de la República Argentina.

[7] Pontoriero, *María Paula, pag 339,* en *La Disrupción Digital y sus impactos en el ser humano: una mirada jurídica; Directora* WEINGARTEN, Celia; Santa Fe Rubinzal-Culzoni, 2023.

en la obtención de un diagnóstico definitivo más temprano y preciso, mejorando la calidad de vida de los adultos mayores; lo cierto es que al utilizar este tipo de tecnología se asume ciertos riesgos. Ello, en el entendimiento de que los datos que se introducen a las IA provienen de distintas fuentes como puede ser de una historia clínica digital o del registro de consumo de medicamentos; dado que estos últimos suelen caracterizarse como "datos sensibles".

Por lo que, en efecto, se deben tomar los mayores recaudos posibles al momento de desarrollar estos sistemas de algoritmos, a fin de prevenir la ocurrencia de daños frente a los derechos personalísimos de los ciudadanos.

En atención a ello, cabe recordar que además del deber de resarcir que, eventualmente, aquellos desarrolladores de las IA (junto a otros sujetos que a lo largo del presente trabajo me detendré a detallar y analizar conforme a la responsabilidad civil que les compete) deberán cumplir frente a un daño cierto; también de manera anticipada deben cumplir con el deber de prevención del daño contemplado en el Art.19 de nuestra carta magna.. Este último, establece el deber genérico de no dañar a otro. Es por ello que nuestro Código de fondo consagra la función "bipartita" de la responsabilidad civil: prevenir y reparar.

A su vez, la función preventiva del derecho de daños, se encuentra plasmada a lo largo de todo nuestro ordenamiento jurídico, como lo es en el Art.52 de la Ley de Defensa del Consumidor; Art.30 de la Ley General del Ambiente 22.675; Art.1710 al Art.1715 del Código Civil y Comercial de la Nación; como así también el Art. 623 bis del Código Procesal Civil y Comercial de la Nación, así lo acoge..

Asimismo, cabe aclarar que el Deber de Prevención del Daño, a su vez impone tres conductas principales que, prima facie, busca evitar la producción de un daño, procurar su disminución y no gravar el daño ya producido[8].

Es por ello que creo que los desarrolladores de las IA deben tener especial consideración en el deber principal de prevención; ya que es un elemento primordial que tienen los magistrados a la hora de juzgar y analizar un caso de responsabilidad civil frente a la violación de datos

[8] BREGA, *Lisandro en Doctrina: La función preventiva de la Responsabilidad Civil, noviembre 2023. https://aldiaargentina.microjuris.com/2023/11/29/doctrina-la-funcion-preventiva-de-la-responsabilidad-civil/*

sensibles (en este supuesto) producto de la actividad propia de los sistemas tecnologicos.

A su vez, no puedo dejar de mencionar otros derechos personalísimos, también reconocidos por nuestro ordenamiento jurídico; como lo es el derecho a la imágen o el derecho al honor; a los que la tecnología desde hace ya varios años los entrelaza.

Por ejemplo, día a día nos encontramos expuestos a la detección facial de los teléfonos móviles, a las redes sociales o a plataformas digitales tales sean como Youtube, Spotify, Netflix, cuando estas al momento de elaborar perfiles nos sugieren cierto tipo de música o películas, utilizan inteligencia artificial[9].

En efecto, podemos observar que el uso de las IA afecta a estos derechos personalísimos referidos en los Arts.51.52.52 del Código Civil y Comercial de la Nación, como así también en nuestra Constitución Nacional

Podemos notar, en consecuencia, que en todos los supuestos aquí mencionados, tanto en el campo de la salud como en la esfera del entretenimiento (Spotify/Netflix) que de igual manera involucra derechos tan esenciales como lo son los personalísimos; cabe la posibilidad de que puedan surgir daños. Ya sea por errores de diagnósticos, errores en la programación y/o actualización de los Softwares[10], errores de los sistemas de las inteligencias artificiales o bien por el riesgo o vicio de la cosa, en el caso del presente trabajo, de las IA.

Asimismo, las denominadas inteligencias artificiales pueden provocar daños por los sesgos que presentan estas mismas, basados en la discriminación sistemática que pueden realizar a partir de sus algorítmos. En el capítulo siguiente me detendré a explicar y analizar dicha temática.

3. SESGOS ALGORÍTMICOS Y DISCRIMINACIÓN

[9] HIHGTON, *Casiano, Los daños derivados de la inteligencia artificial y del impacto de las nuevas tecnologías, UCA, Ciudad Autónoma de Buenos Aires, 2020. https://repositorio.uca.edu.ar/bitstream/123456789/10922/1/danos-derivados-inteligencia-artificial.pdf*

[10] Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora. Definición de la RAE.

Antes de adentrarme en el tema del presente capítulo, me gustaría reforzar el concepto de Inteligencia Artificial que he mencionado con anterioridad.

Los modelos de inteligencia artificial, para ser considerados como tal, requieren de una gran cantidad de datos para funcionar eficazmente[11]. La gran expansión del internet a lo largo y a lo ancho del planeta, ha generado un gran volúmen de datos, por lo que hoy en día se recopila mucha más información a cada minuto que en otros años pasados; dado que al haber muchas más fuentes de datos la información a la que hoy uno puede acceder es sobreabundante, no obstante lo cual dicha información no resulta ser verídica en su totalidad.

Sin embargo, cuando nos referimos a datos, concebimos una noción amplia del significado de la palabra, tal es así que hacemos referencia a imágenes, textos, sonido, redes, coordenadas, etc.

A su vez, la propia Inteligencia al ser utilizada va generando conocimiento de nosotros mismos, por lo que cada interacción de las personas humanas con estos sistemas, contribuye al crecimiento y mejora de la IA.

Es por eso que a través de todos los datos que incorporamos o generamos, la IA tiende a determinar lo que consumimos a toda escala, ya sea que nos puede recomendar productos/ servicios/orientación religiosa, etc atento a que este resultado se encuentra basado en un algoritmo, el cual la misma inteligencia ha logrado consolidar debido a nuestros gustos y preferencias que, de manera inconsciente, solemos suministrar diariamente.

En este sentido, es importante atender a la posibilidad de que la IA pueda crear perfiles incorrectos o bien sobrepasar los límites del consentimiento que la persona le ha cedido al brindar sus datos y/o preferencias, habiendo una responsabilidad civil y, en ese caso, la obligación de reparar el daño causado producto de las actividades propias de la IA; las cuales me detendré a analizar en detalle en el siguiente capítulo.

Ahora bien, teniendo una mejor noción de qué son y cómo funcionan las IA; los programas que utilizan estas últimas se presumen como neutros

[11]Pontoriero, *María Paula, pag 337,* en *La Disrupción Digital y sus impactos en el ser humano: una mirada jurídica; Directora* WEINGARTEN, Celia; Santa Fe Rubinzal-Culzoni, 2023.

dado a que uno puede pecar de ingenuo al pensar que trabajan de manera objetiva ya que es un sistema artificial, carente de sentimientos.

Sin embargo, vamos a ver que lo afirmado en el párrafo anterior dista mucho de lo que realmente son las IA.

En rigor de verdad, la información que compone o retroalimenta los programas/software de las IA, suelen estar plagados de sesgos y prejuicios que fomentan e incrementan la discrimnación. Ello responde a una verdad indiscutible que es que los sesgos son inherentes al ser humano, por lo que los sistemas que se crean son un reflejo de la sociedad misma. Es por ello que a medida que los algoritmos aprenden de nuestros datos suelen replicar e incrementar estas diferencias, ya sea por cuestiones étnicas, por género, raza y cualquier otra categoría.

En tal contexto, estos sistemas se ven repletos de los denominados "Estereotipos[12]"; que claramente tienen un impacto en todo el despliegue de actividades que realizan estas nuevas tecnologías.

A su vez, es dable destacar que ciertas empresas multinacionales como "Amazon" o "Coca- Cola", suelen utilizar softwares que, por lo general, son una IA en la que su principal tarea es llevar a cabo los procesos de selección de personal. Dicha inteligencia analiza diversos Curriculums; el tono de voz e incluso hasta hace hincapié en las expresiones faciales de los postulantes; con el fin primordial de realizar una rigurosa selección del personal de la empresa. En tal sentido, con el objetivo principal de automatizar y acelerar estos procesos de incorporación de empleados; lo cierto es que las decisiones de la IA suelen estar influenciadas por aquellos sesgos propios del algoritmo que, como he mencionado anteriormente, son propios de las personas que crearon y retroalimentan este último. La inteligencia artificial, influenciada por estos sesgos, realiza sus propias conclusiones en torno a las capacidades de los postulantes para poder ocupar un futuro puesto.

En consecuencia, esto se vió reflejado en la práctica en aquellas empresas que se dedican a tareas de tecnología; ya que el propio sistema de la IA en su labor de selección de personal, escogía con un mayor porcentaje (muy elevado) a personal masculino, perjudicando de esta manera a aquellas mujeres que aspiraban a dicho puesto de trabajo; evidenciando la clara

[12] Imágen o idea aceptada comúnmente por un grupo o sociedad con carácter inmutable, definición de la RAE.

desigualdad estructural y sociedad machista en la que nos encontramos inmersos.

Por otra parte, si nos fuéramos al ámbito penal podemos encontrar ejemplos claros de lo antedicho. Resulta que en Estados Unidos existen sistemas predictivos de reincidencia penal en los diversos estados/jurisdicciones de la nación. Esta IA lo que hace es aconsejar al juez a la hora de otorgar beneficios a las personas privadas de su libertad, tales sea como libertades provisionales. Me parece que ya podemos deducir lo que eso significa y el propio desenlace que desencadena los dictámines de esta Inteligencia artificial; aún mas teniendo especial consideración los antecedentes históricos del mencionado país en cuanto a la discriminación, xenofobia y esclaviasmo acaecido. Es por eso que es indudable e innegable que estos patrones repetitivos y algoritmos que utilizan las IA no estén teñidos de sesgos discriminatorios basados en la raza, la demografía, el estatus económico y otras tantas cuestiones. Sesgos que se reproducen una y otra vez, ya que son el propio reflejo de la sociedad norteamericana.

Si bien este es un tema que requiere un arduo y gran extenso abordaje, lo cierto es que unos de los principales riesgos de la utilización de las IA son, precisamente, aquellos sesgos discriminatorios que pueden influir en las decisiones que tomen aquellas tecnologías y que pueden dar lugar, indudablemente, a una obligación de reparar los daños causados.

Me parece conveniente que a los fines de hacer efectivo este deber de prevención propio del Derecho de daños al cual me he referenciado tantas veces; se debe contemplar una regulación de las IA enfocada en proteger aquellos derechos de las personas, en especial, aquellos que se encuentran inherentes al ser humano y que si resultan vulnerados, se abra camino a la posibilidad de ejercer una acción por daños y perjuicios.

Si bien cada nación a lo largo del mundo en su marco regulatorio contempla distintos factores en pos de regular las IA; lo cierto es que se ha llegado a un consenso que es el reconocimiento de la necesidad de regular estos sistemas por todo los riesgos que podrían generar y la importancia del análisis de los presupuestos de la responsabilidad civil que eso conlleva. Por eso no podemos dejar de lado la imperiosa necesidad de proteger los derechos humanos de los ciudadanos, pese a estos riesgos.

Comparto que la tecnología ha generado grandes ventajas, impensadas siquiera hace 10 años atrás, pero en una suerte de balanza creo que pesa mucho más el ejercicio de los derechos de las personas por sobre

cualquier software que intente acelerar y facilitarnos la vida; por lo que va a ser tarea del legislador regular estas nuevas tecnologías que llegaron para quedarse y continúan su propio camino..

Asimismo, confío en que el legislador deberá tener en cuenta que estos sesgos pueden introducirse de manera inconsciente a las IA; por lo que el centro o el espíritu de la norma debe ser siempre en miras de proteger y tutelar el pleno ejercicio de los derechos fundamentales.

Me parece acertado que a nivel mundial se reconozca la necesidad de regular estos sistemas novedosos y que bajo ninguna circunstancia, una inteligencia artificial pueda ser capaz de avasallar derechos tán fundamentales como lo es el derecho a la imágen o al honor; por lo que también se deberá fomentar que los creadores o los desarrolladores de la IA; sean lo más heterogéneos y diversos posibles, en pos de erradicar (que a mi criterio me parece una tarea muy difícil) la discriminación que siempre estuvo tan presente en todas las sociedades.

4. DAÑOS DERIVADOS DE LAS IA Y SU RESPONSABILIDAD CIVIL.

Como mencioné a lo largo del presente trabajo, las IA ya sea producto de sus sesgos o bien por riesgos o vicio de las actividades de la inteligencia artificial aplicada, puede conllevar a la violación del deber genérico de no dañar y, por lo tanto, a la obligación de resarcir el daño ocasionado.

Dado que son muchas las situaciones del uso de la inteligencia artificial que pueden generar situaciones dañosas; en lo personal creo que frente a estos casos debemos contemplar con mayor énfasis, la función preventiva del derecho de daños, ya mencionada.

En atención a ello, me gustaría citar un fallo reciente del Tribunal de la Haya[13] que tuvo lugar el pasado 5 de febrero del año 2020; el fallo SyRI. Este instrumento legal es una IA que utilizaba el gobierno holandés para prevenir y combatir el fraude en el fuero de la seguridad social y los impuestos. En este sentido, esta tecnología recopila datos de los ciudadanos holandeses creando perfiles de riesgos a través de algoritmos. De modo tal, que esta IA permite elaborar informes de riesgos que le es muy útil al

[13] Principal Órgano de la Organización de las Naciones Unidas https://www.icj-cij.org/es

gobierno local. Sin embargo, este sistema para lograr optimizar su labor, analiza una gran cantidad de datos (entre ellos algunos muy sensibles) tales sea como aquellos que versan sobre el trabajo de las personas; datos en relación a sanciones de carácter administrativas[14]; datos sobre bienes muebles e inmuebles; sobre pensiones, endeudamiento y así la lista podría seguir sin límite, ya que literalmente este sistema analizaba todo dato que involucre a la persona misma.

Si bien todo el gran volúmen de información (de gran escala por cierto) de datos que recolecta esta Inteligencia Artificial se encuentra regulada por un órgano de contralor que es "La Autoridad Holandesa de Protección de Datos"; lo cierto es que el Tribunal en el mencionado fallo sostuvo que la legislación SyRI no cumple con el requisito establecido en el Artículo 8.2 del CEDH[15]Convenio Europeo de DDHH) dado que dicha norma protege el derecho al respeto de la vida privada. En ese sentido, los magistrados entendieron que dicho instrumento vulnera este derecho fundamental reconocido internacionalmente que es el derecho a la intimidad. Además, manifiesta que la intromisión en el ejercicio del derecho al respeto de la vida privada debe ser proporcional, de modo tal que no lo vulnere. El tribunal al evaluar la legislación de Syri tiene en cuenta ciertos parámetros que son los principios de transparencia; el de "limitación de la finalidad" y el de "minimización de datos"; en atención a que estos últimos dos principios conforman la proporcionalidad aplicada en la captación de datos; por lo que dicho tribunal ha llegado a la conclusión de que la legislación de la referida IA no se condice con estos principios.

En consecuencia, el tribunal ha ponderado la importancia del derecho al respeto a la vida privada que también presenta una íntima relación con el derecho a la igualdad de trato que hacen a la protección contra la discriminación. Finalmente, en el entendimiento que estos dos derechos mencionados han sido vulnerados producto de este sistema de IA por el uso indiscriminado de perfiles y de decisiones automatizadas; el tribunal decide anular la elaboración de perfiles para evitar fraudes en la seguridad social; ponderando estos derechos ya mencionados por encima de la labor de la referida IA. En efecto, el tribunal falla en este sentido con una perspectiva

---

[14] BATTAGLINI, *Manuela en Ética de los datos. Sentencias. Tecnología y sociedad. Transparencia, Febrero 2020.*

[15] Art.8 Convenio Para la Protección de los Derechos Humanos y las Libertades Fundamentales.

de Derechos Humanos ya que contempla la protección al derecho a la autonomía personal, al desarrollo personal y, por lo tanto, el derecho a la intimidad que se encontraban sometidos frente a la inobservancia de los legisladores locales en la aplicación de SyRI.

Por último, me gustaría analizar la responsabilidad civil que podría dar lugar a esta obligación de reparar y resarcir el daño ocasionado, frente a un hipotético caso en el cual una empresa se dedica a comercializar y a producir sistemas de IA de similares características al de SyRI.

En esta línea, a modo de mención cabe recordar los cuatro (4) presupuestos de la responsabilidad civil que deben concurrir para originar la obligación de indemnizar. Ellos son la antijuridicidad, el daño, el factor de atribución y la relación de causalidad.

En cuanto al primer elemento que es la antijuridicidad, podemos decir que se encuentra configurada por la violación al deber genérico de no dañar a otro (deber al que he hecho referencia en el capítulo I del presente trabajo); ya que en el hipotético caso de que una empresa Argentina produzca y comercialice esta IA que procesa datos y elabora informes de riesgos; por haber lesionado alguno de los derechos ya referenciados, se configura la misma. Tal es así que por el mero hecho de que esta empresa por acción u omisión produzca un daño, se configura el elemento de la antijuridicidad..

En concordancia con los Arts.1721 a 1737 y subsiguientes del Código Civil y Comercial de la Nación, cabe remarcar que, dejando atrás y por lo tanto superando el viejo esquema de responsabilidad civil Veleziano; la introducción de estos modelos de inteligencia artificial en la sociedad por parte de sus creadores o desarrolladores; conlleva la aparición de nuevos riesgos y, consecuentemente, la aparición de nuevos daños (como hemos visto en el fallo de SyRI).

Frente a tal escenario y si tuviéramos que aplicar el viejo esquema de responsabilidad del código Velezano (antes de su reforma de la ley 17.711) en el cual un sujeto respondía de manera subjetiva por dolo o por culpa únicamente; pareciera a priori que ese eventual daño quedaría sin reparación alguna. Por lo que luego de la reforma del código de Vélez y con la sanción del nuevo código civil y comercial, se logra evidenciar que se ha contemplado nuevas realidades de la sociedad y, gracias a ello, el sistema de responsabilidad civil vigente contempla a su vez la responsabilidad objetiva. El art 1721 del mencionado código determina que la atribución de un daño

al responsable puede tener fundamentos en factores subjetivos (dolo o culpa) y a su vez en factores objetivos, En tal caso, este factor objetivo se configura por la introducción de un elemento peligroso a la sociedad y es por ello que el guardián o dueño de la cosa, pese a haber actuado con la debida diligencia, deberá responder frente a un daño. En el ejemplo aludido, recordando la definición que nos brinda el citado código de fondo en su Art.1737; podemos asegurar que hay un daño por la lesión al derecho a la privacidad de las personas frente al uso desmedido de esta IA.

Asimismo, podemos observar que frente a este nuevo esquema de responsabilidad civil, la base del sistema deja de ser la responsabilidad y pasa a ser la reparación integral en sí. No podemos dejar de lado la obligación de seguridad que se encuentra presente en el caso en cuestión. Esta obligación y principio a la vez, supone incorporar al mercado productos o servicios seguros conforme la normativa vigente (Ley de Defensa del Consumidor 24.240); por lo que este derecho a la seguridad tutela la cobertura de los riesgos contractuales; extracontractuales, individuales y colectivos que puedan sufrir aquella parte vulnerable reconocida como la más debil, que se encuentra en una posición inferior, los consumidores.

En cuanto al elemento de la relación de causalidad o nexo causal; se debe poder trazar un nexo adecuado de causalidad entre el daño acreditado y la conducta del responsable o, en este caso, la intervención de una cosa que se encuentre dentro de su esfera de custodia o garantía.

En efecto, la relación causal es el factor aglutinante[16] que hace que el daño y el riesgo introducido en la sociedad por parte de esta empresa (en este caso la propia IA); se integren en la unidad del acto que es fuente de la obligación a indemnizar.

En conclusión, me parece sumamente importante tener en cuenta los riesgos que conlleva la implementación de las IA y el impacto que tiene estas nuevas tecnologías en nuestros derechos, por lo que advierto una constante necesidad en la actualización normativa en pos de regular y, de esta manera, prevenir a su vez eventuales daños causados por el avance tecnológico que avasalla nuestros derechos día a día, aunque de manera inconsciente así sea.

[16] P;M. B c/ B;R,D y otro s/daños y perjuicios, Cámara Nacional de apelaciones en lo civil, 27/11/2023

5. BIBLIOGRAFÍA

- Red informática mundial, descentralizada, que permite la transferencia casi inmediata de datos entre ordenadores; Real Academia Española.

- Enfermedad por Coronavirus (Covid-19); la cual fue advertida por primera vez en la localidad de Wuhan (china) el 31 de Diciembre de 2019; Organización Mundial de la Salud, sitio Web Oficial https://www.who.int/es/emergencies/diseases/novel-coronavirus-2019?adgroupsurvey={adgroupsurvey}&gad_source=1&gclid=Cj0KCQjwiOy1BhDCARIsADGvQnAUHvNVKsspck5X2_7Vorp0sdI3r2WBgw4MXaxm7x6EkwsPS9Zi_IIaAsS2EALw_wcB

- La Organización Panamericana de la Salud es el organismo especializado de salud del sistema interamericano, encabezado por la Organización de los Estados Americanos, y también está afiliada a la Organización Mundial de la Salud .https://www.paho.org/es

- BETTINA BLANCO, Valeria; pág 191 en La Disrupción Digital y sus impactos en el ser humano: una mirada jurídica; Directora WEINGARTEN, Celia; Santa Fe Rubinzal- Culzoni, 2023.

- Constitución Nacional de la República Argentina.

- Pontoriero, María Paula, pag 339, en La Disrupción Digital y sus impactos en el ser humano: una mirada jurídica; Directora WEINGARTEN, Celia; Santa Fe Rubinzal- Culzoni, 2023.

- BREGA, Lisandro en Doctrina: La función preventiva de la Responsabilidad Civil, noviembre 2023. https://aldiaargentina.microjuris.com/2023/11/29/doctrina-la-funcion-preventiva-de-la-responsabilidad-civil/

- HIHGTON, Casiano, Los daños derivados de la inteligencia artificial y del impacto de las nuevas tecnologías, UCA, Ciudad Autónoma de Buenos Aires, 2020. https://repositorio.uca.edu.ar/bitstream/123456789/10922/1/danos-derivados-inteligencia-artificial.pdf

- Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora. Definición de la RAE.

- Pontoriero, María Paula, pag 337, en La Disrupción Digital y sus impactos en el ser humano: una mirada jurídica; Directora WEINGARTEN, Celia; Santa Fe Rubinzal- Culzoni, 2023.

- Imágen o idea aceptada comúnmente por un grupo o sociedad con carácter inmutable, definición de la RAE.

- Principal Órgano de la Organización de las Naciones Unidas https://www.icj-cij.org/es

- BATTAGLINI, Manuela en Ética de los datos. Sentencias. Tecnología y sociedad. Transparencia, Febrero 2020.

- Art.8 Convenio Para la Protección de los Derechos Humanos y las Libertades Fundamentales.

- P;M. B c/ B;R,D y otro s/daños y perjuicios, Cámara Nacional de apelaciones en lo civil, 27/11/2023

DESAFÍOS DE LA INTELIGENCIA ARTIFICIAL EN EL MARCO DE LA RESPONSABILIDAD CIVIL

Por Virginia Angeli[1]

El éxito en la creación de la inteligencia artificial podrá ser el evento más grande en la historia de la humanidad. Desafortunadamente también podría ser el último, a menos que aprendamos a evitar los riesgos" - Stephen Hawking

I. CONCLUSIONES

1. Los sistemas de inteligencia artificial pueden afectar los derechos fundamentales de los individuos, por lo que la respuesta jurídica frente a los daños que generen debe darse con basamento en el respeto, protección y promoción de la dignidad humana.

2. El reconocimiento y resguardo del derecho de protección de datos personales, especialmente vulnerado mediante los sistemas de inteligencia artificial, exige la adopción de medidas de privacidad y de seguridad reforzadas.

3. La función preventiva reglamentada en nuestro ordenamiento jurídico cobra un rol preponderante ante el riesgo derivado de los sistemas de inteligencia artificial.

4. Se propicia una atribución de responsabilidad objetiva con fundamento en el riesgo creado -sin distinción de grado- frente a daños causados por sistemas de inteligencia artificial que afectan los derechos personalísimos del individuo, en cuanto debe prevalecer la protección de la dignidad humana respecto del interés en fomentar el desarrollo e innovación tecnológica.

II. FUNDAMENTOS

1. INTRODUCCIÓN

[1] Docente Titular de la cátedra de Derecho Privado VIII de la Facultad de Derecho y Ciencias Sociales de la Universidad Católica de Córdoba.

La inteligencia artificial (IA) se ha desarrollado de manera tal que hoy podemos afirmar que no existe un aspecto de la vida del ser humano que sea ajeno a su influencia.

Nos encontramos en la era de la digitalización, donde la IA presenta una enorme capacidad para transformar la vida económica, política y social a nivel global. Sin embargo, a la par de los beneficios que su desarrollo trae aparejado, también plantea desafíos en términos de protección de los derechos fundamentales de las personas[2].

En este contexto, surge el interrogante sobre si las respuestas jurídicas tradicionales del derecho de daños son suficientes o si resulta necesaria una nueva reglamentación.

2. LA INTELIGENCIA ARTIFICIAL: APROXIMACIÓN CONCEPTUAL

La Real Academia Española define a la inteligencia artificial (IA) como "la disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico"[3].

Por su parte, el Reglamento del Parlamento Europeo sobre Inteligencia Artificial, la define como "sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales"[4].

Según su implementación, estos sistemas pueden clasificarse en inteligencia artificial débil o fuerte.

---

[2] Disposición 2/2023, Recomendación para una Inteligencia Artificial confiable, Jefatura de Gabinete de Ministros, Subsecretaría de Tecnologías y de la Información, ciudad de Buenos Aires, 1/06/2023.

[3] https://dle.rae.es/inteligencia?m=form#2DxmhCT.

[4] Reglamento de Inteligencia Artificial, Resolución Legislativa del Parlamento Europeo, 13 de marzo de 2024, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.pdf.

En términos generales, se utiliza IA débil cuando se implementa un algoritmo para la realización de una tarea concreta. Abarca una amplia gama de tecnologías y técnicas, incluyendo al aprendizaje automático, procesamiento de lenguaje natural, reconocimiento de voz, y visión por computadora, entre otras.

Por otro lado, la IA compleja o fuerte es aquella imitadora de las habilidades cognitivas humanas, pudiendo llegar a resolver todo tipo de problemas sin basarse en patrones previamente analizados o estudiados sino habiendo aprendido a razonar, y crear o decidir a partir de ello[5].

Estos sistemas de inteligencia artificial exigen articular respuestas jurídicas frente a los daños que pueden generar.

3. EL EPICENTRO DE AFECTACIÓN: LA DIGNIDAD HUMANA

A tal fin, la mirada debe estar puesta en los derechos fundamentales, cuyo eje es la dignidad humana.

La dignidad inviolable e intrínseca de cada ser humano (art. 51, CCCN) constituye la base del sistema universal, indivisible, inalienable, interdependiente e interrelacionado de derechos humanos y libertades fundamentales.

Por consiguiente, el respeto, la protección y la promoción de la dignidad humana son aspectos esenciales a lo largo del ciclo de vida de los sistemas de IA.

De allí que la ética debe considerarse como una base dinámica para la evaluación y la orientación normativas de las tecnologías de la IA, tomando como referencia la dignidad humana, el bienestar y la prevención de daños y apoyándose en la ética de la ciencia y la tecnología[6].

En este marco, cobra relevancia la protección de los datos personales. El derecho a proteger los datos personales deriva de la autodeterminación

---

[5]Ruano, María Candela, "El ABC de la inteligencia artificial a partir de una óptica de los derechos humanos. Desde las personas y para las personas", TR LALEY AR/DOC/1431/2024.

[6] Recomendaciones UNESCO sobre la ética de la inteligencia artificial, 23/11/2021.

que toda persona tiene de decidir qué datos relativos a su propia existencia pueden ser divulgados por terceros.

Los datos personales se vinculan con las manifestaciones de la personalidad, y por ende, su violación implica afectar, en primer lugar, la esfera de su intimidad, su zona de reserva a la cual no se puede ingresar sin un expreso consentimiento.

El derecho de protección de datos personales, de cuyo tratamiento mediante los sistemas de IA surge la principal afectación a la dignidad de la persona en sus distintas proyecciones, es considerado actualmente como un derecho distinto y complementario a los derechos a la privacidad, el honor, la inviolabilidad del hogar, las comunicaciones privadas y conceptos conexos.

Siguiendo los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales adoptados por el Comité Jurídico Interamericano (CJI) y aprobados por la Asamblea General de la OEA en 2021[7], debe adoptarse una perspectiva transversal de género y de derechos humanos que identifique los impactos diferenciados del tratamiento de datos y los haga visibles, pesando sobre los responsables de los datos la obligación de adoptar las medidas necesarias para mitigar estas disparidades e impedir que su tratamiento menoscabe la dignidad y la privacidad de las personas, sobre todo, de aquellas que enfrentan situaciones de especial vulnerabilidad.

Según el contexto cultural, social o político, la categoría de datos personales sensibles incluye -al solo fin ejemplificativo-, los datos relacionados con la salud, vida sexual, orientación sexual, creencias religiosas, filosóficas o morales, afiliación sindical, datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, opinión política u origen racial o étnico, información sobre cuentas bancarias, documentos oficiales, información recopilada de niños y niñas o geo localización personal.

Frente al alto riesgo de daño que implica el tratamiento de estos datos personales sensibles a través de la IA, se exige la adopción de medidas de privacidad y de seguridad reforzadas.

---

[7]https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

Los daños no deseados (riesgos de seguridad) y las vulnerabilidades a los ataques (riesgos de protección) deben prevenirse y eliminarse a lo largo del ciclo de vida de los sistemas de IA para garantizar la seguridad y la protección de los seres humanos, lo que debe lograrse mediante el desarrollo de marcos de acceso a los datos que sean sostenibles, respeten la privacidad, y fomenten un mejor entrenamiento y validación de los modelos de IA que utilicen datos de calidad.

4. MARCO NORMATIVO DE PROTECCIÓN DE LA DIGNIDAD HUMANA

En cuanto al núcleo esencial de protección jurídica vigente en la materia, debemos destacar que la Constitución Nacional consagra la inviolabilidad del domicilio, como también de la correspondencia epistolar y los papeles privados (art. 18), mientras que dispone que las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están solo reservadas a Dios y exentas de la autoridad de los magistrados (art. 19).

La Declaración Universal de los Derechos Humanos contempla en su art. 11 la protección de la honra y de la dignidad. En esta línea, consagra que nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. Y concretamente dispone que toda persona tiene derecho a la protección de la ley contra esas injerencias o ataques.

En idéntico sentido, el Código Civil y Comercial prescribe la inviolabilidad de la dignidad de la persona humana como eje central de protección jurídica, y luego contiene diversas normas específicas sobre los derechos que emanan de ella (arts. 51, 52, 53, 279, 1004, 1097, 1770).

Respecto de los datos personales, rige en nuestro país una ley específica en la materia desde el año 2000 (ley n.° 25.326), pero su reconocimiento y protección como derecho humano y esencial, presenta un avance sobresaliente con la sanción de la ley nº 27.699, que aprueba el Protocolo modificatorio del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, también conocido como Convenio 108+. Dicha ley fue publicada en el Boletín oficial el día 30 de noviembre de 2022, convirtiendo a la República Argentina en el segundo país de América Latina en ratificar el Convenio 108+.

5. REGLAMENTACIÓN EN MATERIA DE INTELIGENCIA ARTIFICIAL[8]

En el ámbito internacional, se destaca el Reglamento Europeo de Inteligencia Artificial sancionado en el mes de marzo del 2024. Es la primera ley integral en materia de inteligencia artificial del mundo que busca regular los usos de la IA para limitar los riesgos que de ellos se derivan. Su principal aporte radica en la realización de un enfoque basado en el riesgo, definiendo así, cuatro niveles de riesgo para los sistemas de inteligencia artificial (riesgo inaceptable, riesgo alto, riesgo limitado o riesgo mínimo).

A nivel interno, existen hasta la fecha tres proyectos de ley que proponen una reglamentación integral sobre el tema.

Se ha presentado el proyecto de ley sobre "Regulación y uso de la inteligencia artificial", por la diputada Anahí Costa en el año 2023.

También existe el proyecto de ley sobre "Principios rectores para el desarrollo, implementación y utilización de sistemas basados en inteligencia artificial (IA) dentro del territorio argentino", presentado por el senador Juan Carlos Romero, en el año 2023. Su objeto es establecer controles y principios rectores para el desarrollo, implementación y utilización de sistemas basados en Inteligencia Artificial (IA) dentro del territorio argentino, con el fin de salvaguardar la dignidad, los derechos humanos y el bienestar de las personas. En consonancia con el Reglamento Europeo, refiere en su artículo 2 a los sistemas de inteligencia artificial de riesgo limitado, de riesgos mínimos o nulos, de alto riesgo y de riesgo inaceptable.

Finalmente, resulta destacable el reciente proyecto de ley sobre "Responsabilidad algorítmica y promoción de la robótica, algoritmos verdes e inteligencia artificial de la República Argentina", presentado en 2024 por el diputado Maximiliano Ferraro. Su objetivo es establecer un marco legal a los desarrollos de la inteligencia artificial con el fin de crear certificaciones de buenas prácticas, implementar un registro de riesgos significativos, promover la inteligencia artificial en pequeñas y medianas empresas, como así también fomentar la responsabilidad y transparencia algorítmica de nuevas tecnologías en respeto del bien común, el estado de derecho y la

[8] Iglesias Herrera, Ismael, "La regulación normativa de la inteligencia artificial, el modelo europeo y los proyectos de regulación en el ámbito nacional", Actualidad Jurídica, Derecho Público, número 84, mayo 2024.

protección de la autonomía individual (art. 1). Una especial mención merecen los principios que propone, siguiendo las recomendaciones de la Organización para la Cooperación y el Desarrollo Económico (OCDE) suscriptas por nuestro país en el año 2019 (art. 4).

6. REGULACIÓN ESPECÍFICA EN MATERIA DE RESPONSABILIDAD CIVIL

En lo que atañe específicamente a los daños causados por inteligencia artificial, el desarrollo normativo a nivel mundial es aún incipiente.

La Resolución del Parlamento Europeo del 16 de febrero de 2017[9], propicia sustentar la responsabilidad de los robots o sistemas de IA en un enfoque de gestión del riesgo y plantea la posibilidad de introducir un seguro de daños obligatorio.

En el año 2020, el Parlamento Europeo dicta una nueva Resolución[10] cuyo objetivo es crear una legislación uniforme en materia de IA para los regímenes de responsabilidad europeos. Parte de considerar los problemas que genera la evolución e introducción de sistemas de inteligencia artificial, con la consiguiente dificultad de identificar a los responsables dada la gran cantidad de agentes involucrados.

La normativa propone una responsabilidad basada en el riesgo, y dispone su carácter objetivo frente a los sistemas de IA de alto riesgo.

El fundamento estriba en que los sujetos que van a responder por el riesgo inherente a la actividad productora de los daños causados, ejercen un grado de control suficiente sobre el riesgo creado. Es decir, el operador tiene un grado de control sobre los sistemas de IA mediante diversas instrucciones que puede darle. Por ende, quien desarrolla dicha actividad genera un riesgo para el resto de personas, que amerita que cargue con las consecuencias negativas.

---

[9] Díez Royo, Mario, "Cuestiones de responsabilidad civil en los sistemas de inteligencia artificial en las Propuestas de Directivas Europeas de 28 de septiembre de 2022, https://orcid.org/0009-0002-0566-0406.

[10] Resolución Bruselas, Bélgica, 20 de octubre de 2020, Id SAIJ: LNT0007538.

En cambio, respecto de los sistemas de IA que no son de alto riesgo, asigna un régimen de responsabilidad civil subjetivo, con ciertas particularidades, consagrando la culpa como elemento de imputación.

En Argentina se encuentra vigente el debate acerca de si la normativa general sobre responsabilidad civil es suficiente para abordar los problemas que genera la IA en esa materia, o si por el contrario, es necesario dictar una legislación específica, con principios propios que permitan esclarecer la responsabilidad jurídica de los agentes que emplean sistemas de IA.

El avance y dinamismo inusitado de los sistemas de IA, con su consecuente impacto en todas las esferas del ser humano, exige brindar un marco normativo específico, abierto y flexible, que los regule de manera integral, y concretamente, respecto de la responsabilidad civil por los daños que de ellos deriven.

Sin embargo, y hasta tanto ello tenga lugar, podemos encontrar una respuesta jurídica adecuada en nuestro derecho, a través de la novel legislación relativa a la protección de datos personales (ley n.° 27.699), el régimen protectorio de la ley de defensa del consumidor -sobre todo en materia de productos defectuosos- y los preceptos de responsabilidad civil previstos en el Código Civil y Comercial de la Nación (arts. 1708 y ss., CCCN).

Atento las particularidades características que presentan los sistemas de IA, tales como su opacidad, la vertiginosidad de su desarrollo y la incertidumbre acerca de las consecuencias dañosas que puede generar su uso en un futuro incluso cercano, la función preventiva de la responsabilidad civil consagrada en nuestro ordenamiento sustancial cobra un rol preponderante (art. 1710 y ss, CCCN).

El deber legal de prevenir daños a terceros recae en todos aquellos sujetos que, material o jurídicamente, intervengan en el ciclo de vida de los sistemas de IA. En consecuencia, podrán ser legitimados pasivos de los planteos o acciones entabladas por aquellas personas que acrediten un interés razonable en la prevención del daño.

Frente al daño efectivamente causado por sistemas de IA, en todos aquellos supuestos en donde la afectación se proyecte respecto de los derechos personalísimos que atañen a la dignidad humana, como los vinculados al tratamiento de datos personales sensibles, se propicia una responsabilidad objetiva, con fundamento en el riesgo creado.

La posición expuesta se sustenta en el alto riesgo derivado de los sistemas de IA, que funcionan de forma autónoma, para causar daños o perjuicios a una o más personas de manera aleatoria y que excede lo que cabe esperar razonablemente.

Dentro de esos riesgos, podemos identificar: a) Sesgo o discriminación: la potencia de la IA multiplica exponencialmente cualquier sesgo que presentarán los datos empleados para entrenarla y, para prevenir esto, no solo se analiza la información para asegurarse de que esta es balanceada, justa y libre de elementos discriminatorios, sino que además se implantan incluso medidas de discriminación positiva; b) Explicabilidad: muchas veces resulta muy difícil, entender cómo llega un algoritmo a una determinada decisión. En otras ocasiones, es necesario elegir entre precisión de las decisiones y aplicabilidad de estas, debiendo el desarrollador escoger el mal menor para su caso de uso concreto; c) Transparencia: no solo es importante revelar a los usuarios finales, al inicio y en un lenguaje claro, que están interactuando con un sistema de IA, sino también explicarles cuáles decisiones serán automatizadas y cómo pueden apelar tales decisiones para que sean reevaluadas por un humano; d) Alucinación: es la tendencia de los sistemas de IA generativa de inventar respuestas y/o fundamentos que no están basados en la realidad ni tampoco incluso en la información con que ese algoritmo ha sido entrenado[11].

Conforme se ha desarrollado precedentemente, la legislación comparada pionera en la regulación de la materia bajo análisis, prevé una responsabilidad basada en la culpa para los daños causados por sistemas de IA de bajo riesgo[12], postura que resulta compatible con el impulso del desarrollo y la innovación tecnológica.

Sin embargo, cuando las consecuencias dañosas se proyectan sobre la dignidad humana, resulta indiferente el grado de riesgo del sistema, debiendo buscarse la solución del ordenamiento que sea más acorde a la protección de la víctima que ha sufrido injustamente un daño.

---

[11] Quintana Escudero, Beatriz "Inteligencia Artificial: el riesgo del que no hablamos", SupAbCorp 2024 (agosto), 1; TR LALEY AR/DOC/1889/2024.

[12] Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial, precepto sexto.

De allí que se propicia para toda afectación causada a los derechos personalísimos por sistemas de IA -independientemente del grado de riesgo del mismo- una atribución de responsabilidad de naturaleza objetiva.

Los algoritmos constituyen en cuanto a su diseño, desarrollo y uso, cosas riesgosas o defectuosas que en caso de daños a la persona, gatillan la responsabilidad prevista en el art. 1757 del CCCN. De igual modo, el empleo de esta tecnología se erige en una actividad riesgosa por su naturaleza, por los medios empleados o por las circunstancias de su realización, quedando subsumido en la norma mencionada.

Debe entenderse como sujeto responsable al fabricante, desarrollador, operador, propietario o usuario del sistema, en cuanto pueden encuadrarse en las categorías de dueño y guardián de la cosa riesgosa o viciosa (responsabilidad por el hecho de las cosas); y como sujetos que realizan, se sirven u obtienen un especial provecho de los sistemas de IA, por sí o terceros (responsabilidad por actividad riesgosa o peligrosa). Así, la persona que crea, mantiene, controla y/o explota el sistema de IA, será responsable del daño o perjuicio que cause el dispositivo o la actividad que lleve a cabo el mismo.

En este contexto, deviene imperativa la prescripción que establece que "no son eximentes la autorización administrativa para el uso de la cosa o la realización de la actividad, ni el cumplimiento de las técnicas de prevención" (art. 1757, CCCN).

En los supuestos en que resulten de aplicación las previsiones sobre responsabilidad de defensa del consumidor o por productos defectuosos, debe estarse a la reglamentación prevista en la ley de defensa del consumidor (art. 40, ley n° 24.240).

Cabe remarcar que frente al dinamismo del desarrollo digital, la discusión jurídica debe mantenerse flexible y abierta a innovaciones en la reglamentación en caso de ser necesario para una adecuada protección a los derechos fundamentales, siendo siempre la piedra angular a tal efecto, la dignidad de la persona.

RESPONSABILIDAD POR LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL EN ENTORNOS VIRTUALES: DAÑOS A DERECHOS PERSONALÍSIMOS, DATOS PERSONALES Y ATRIBUTOS DE LA PERSONALIDAD CAUSADOS POR EL INCUMPLIMIENTO DE LA OBLIGACIÓN DE SEGURIDAD DERIVADA DE LOS TRATADOS INTERNACIONALES DE DERECHOS HUMANOS

Por Aldo Marcelo Azar[1]

I. CONCLUSIONES

1. La Inteligencia Artificial (IA) debe conceptualizarse en un sentido amplio como el campo de *sistemas* que desarrollan, emplean o aplican algoritmos, programas, ingeniería de datos, software o tecnología capaces de imitar determinadas funcionalidades de la inteligencia humana, incluidas características como la percepción, el aprendizaje, el razonamiento, la resolución de problemas, la interacción lingüística e incluso la producción de trabajos creativos, con o sin intermediación de máquinas.

2. La responsabilidad civil derivada de la IA por las funcionalidades de sus sistemas que se ejecuten en entornos virtuales se configura por toda contingencia que cause un menoscabo actual o inminente con motivo o en ocasión de las acciones u omisiones ejercidas en Internet, páginas o sitios web, aplicaciones o aplicativos, redes sociales, programas y plataformas digitales.

3. La utilización de la IA en esos entornos, sitios, plataformas, aplicaciones, redes automatiza, acelera y sistematiza un conjunto de fenómenos idóneos para menoscabar: a) los derechos personalísimos tales como la intimidad, la privacidad, el honor, la imagen, la igualdad, la no discriminación, la autodeterminación; b) los atributos de la personalidad tales como el nombre, el patrimonio, y c) los datos personales que

[1] Doctor en Derecho y Ciencias Sociales Universidad Nacional de Córdoba (UNC). Profesor titular de Introducción al Derecho y Derecho Privado II-Obligaciones Civiles y Comerciales en la Facultad de Derecho de la UNC. Investigador de la Secretaría de Ciencia y Tecnología UNC. Profesor titular de Introducción al Derecho Univ. Siglo 21.

contienen la información relativa a esos derechos y atributos tales como las condiciones de salud, los accesos y claves a la correspondencia privada, entre otros.

4. Los Tratados Internacionales de Derechos Humanos (TTDDHH) incorporados por el art. 75 inc. 22 de la Constitución Nacional y los determinados como condición para la aplicación e interpretación de la ley en los arts. 1 y 2 del C Código Civil y Comercial de la Nación (CCCN) consagran y protegen a la seguridad de la persona humana.

5. La seguridad como derecho y garantía de jerarquía constitucional y supranacional derivada de los TTDDHH exige ampliar su comprensión y protección que en la actualidad no se limita a la vida y a la integridad psicofísica, sino que se extiende a todos los derechos personalísimos, los atributos de la personalidad y los datos personales que hacen a la información inherente a los derechos fundamentales de la persona humana.

6. La obligación de seguridad que en el modelo industrial de derecho privado se definió como mantener sana y salva a la persona con motivo u ocasión del cumplimiento contractual, en el actual modelo tecnológico, postindustrial o postmoderno se reconfigura para extenderse a la protección de los derechos personalísimos, atributos de la personalidad, datos e información personal del ser humano. Caracterizada como un deber jurídico específico y de naturaleza secundaria que pesa sobre el deudor cuyo objeto es la protección de la indemnidad del contratante, la obligación de seguridad está orientada al resguardo de su integridad no solo física sino también moral durante el curso ejecución de una relación jurídica.

7. Esa obligación de seguridad concurre con otros posibles factores atributivos de responsabilidad tales como el defecto del producto (virus, bugs, deficiencias en la programación), como el riesgo de la cosa (robots, máquinas, cámaras de vigilancia que aplican IA), como el riesgo de la actividad (en tanto las funcionalidades de la IA contengan un riesgo anormal o intolerable), tanto en el ámbito de las relaciones de derecho privado (art. 1757 CCCN) como de consumo (art. 40 Ley 24240).

8. La obligación de seguridad por los daños a derechos personalísimos, datos personales y atributos de la personalidad es de resultado y por tanto configura un factor objetivo de responsabilidad (arts. 1723 y 774 incs. b y c CCCN).

9. La obligación de seguridad de resultado derivada de la utilización, manipulación o ejecución de la IA en entornos virtuales es agravada dado que no admite como causas ajenas el caso fortuito o fuerza mayor configurado por los contingencias inherentes a los riesgos propios de los sistemas o cosas de IA (art. 1733 inc. e CCCN), ni al hecho del tercero extraño cuando éste los hackea, o accede a la información personal que es guardada, depositada conservada, transferida o actualizada en servidores, aplicaciones, sitios, plataformas en tanto tales conductas no revisten el carácter de caso fortuito en ese tipo de actividades (art.1731 CCCN) .

10. Los asentimientos de los usuarios a utilizar sus datos personales inclusivos de sus gustos, intereses, identidades, orientados, para transferirlos, negociarlos, actualizarlos o vigilarlos no configuran consentimiento de la víctima (art. 1720 CCCN) por los daños a sus derechos personalísimos o atributos de la personalidad derivados de esas actividades de la IA en los entornos virtuales. En efecto, esas conformidades no cumplen con la obligación de información auténtica, íntegra y eficaz respecto a los alcances de ese uso o manipulación, se obtienen por un simple cliqueo carente de las condiciones válidas para un hecho voluntario, constituyen la adhesión a cláusulas predispuestas con las que se exime de responsabilidad por los daños a derechos fundamentales o importan la remisión a otros sitios, programas o cláusulas predispuestas extraños al entorno virtual en el que el usuario está interactuando.

II. FUNDAMENTOS

1. CONCEPTUALIZAICON INICIAL DE LA INTELIGENCIA ARTIFICIAL (IA) Y DELIMITACIÓN DE LOS FENÓMENOS BAJO ANÁLISIS

De conformidad a la UNESCO la IA se define como “un campo que implica máquinas capaces de imitar determinadas funcionalidades de la inteligencia humana, incluidas características como la percepción, el aprendizaje, el razonamiento, la resolución de problemas, la interacción

lingüística e incluso la producción de trabajos creativos"[2]. Ingresan en ese campo así definido cámaras de identificación biométrica, robots, el hardware que utiliza esos recursos, entre otros muchos soportes materiales que facilitan, habilitan o determinan el conjunto de acciones incluidas en ese concepto.

Sin embargo, a los fines del presente trabajo ampliamos la definición precedente para connotar a la IA como los *sistemas* que desarrollan, emplean o aplican algoritmos, programas, ingeniería de datos, software o tecnología cuyas funcionalidades son análogas o equivalentes a la inteligencia humana[3]. En esta comprensión la mediación de máquinas no es determinante, lo cual puede o no acaecer.

Dentro de la totalidad de operaciones y ámbitos en que esos sistemas son susceptibles de operar, limitaremos el análisis de la responsabilidad civil a los daños causados por los sistemas de IA producidos por las acciones o funcionalidades que se ejecuten en entornos virtuales. Ingresan en este ámbito toda contingencia de lesión o menoscabo actual o inminente producido con motivo o en ocasión de las acciones u omisiones ejercidas en Internet, páginas o sitios web, aplicaciones o aplicativos, redes sociales, programas y plataformas digitales.

Asimismo, a los fines de caracterizar el fenómeno bajo estudio, la utilización de la IA en esos entornos virtuales o electrónicos puede abarcar hechos, situaciones o relaciones jurídicas de derecho privado, administrativo, tributario, laboral, de la seguridad social, en todas sus especialidades.

Por último, la actividad desplegada en esos entornos prescinde de la finalidad que se persiga, por lo cual la responsabilidad queda configurada si los sitios, plataformas, redes, aplicaciones tienen por objeto el consumo, el comercio electrónico, el ejercicio del poder de policía por el estado, la interacción o comunicación social entre los usuarios, etc.

---

[2] DE DIEGO, JULIAN A. "Responsabilidad de los robots con la inteligencia artificial y el advenimiento de la personería informática", LA LEY 21.3.2024, 5. Con cita de www.unesco.org Recomendación sobre ética de la inteligencia artificial, Biblioteca Digital.

[3] COLOMBO, MARIA CELESTE, Los algoritmos como potencial agente dañoso, EBOOK-TR 2023 (Colombo), 27. Capítulo II, TR LALEY AR/DOC/766/2023

2. HECHOS PRODUCTORES DE DAÑOS

Los hechos que la IA es idónea para producir daños en entornos virtuales, aplicaciones, programas digitales, redes sociales, sitios web, plataformas de compras son los derivados de los siguientes nuevos fenómenos que se enuncian a modo de ejemplo:

a) la vigilancia, recopilación y comercialización de los datos de los consumidores y usuarios en Internet realizados sin su consentimiento o en ignorancia de tales extremos;

b) la invasión a la privacidad por el seguimiento del usuario y control de su actividad en la red o entornos virtuales;

c) la imposición de esas prácticas a través de la adhesión a cláusulas contractuales en las que el consentimiento del usuario se realiza a través de un click por el solo hecho de navegar en determinados sitios o para la adquisición de productos en los que es obligado, como condición previa de acceso, a dar conformidad a una serie de prácticas invasivas y controladoras que exceden y exorbitan los motivos y las finalidades de la navegación o adquisición de bienes;

d) las aplicaciones, los sitios de comercio electrónico, los buscadores de información, las redes sociales, a los fines de ofrecer precios y productos personalizados al consumidor, estudian el comportamiento de búsqueda de cada usuario, anticipan sus objetivos y ofrecen alternativas al gusto, preferencia o criterios que asume, imputa o infiere respecto a aquel, con lo cual toda la conducta humana es objeto de análisis, sistematización y predicción;

e) el método predictivo señalado permite no solo definir perfiles de comportamientos sino, a partir de ello, prototipos de personalidades en los que todos los aspectos de la intimidad y privacidad son alcanzados: por caso la identidad, orientación, gustos de las personas son etiquetados, sistematizados y estructurados, de modo tal que aspectos personalísimos de la vida privada son tabulados tales como sexo, creencias y experiencias.

Como consecuencia de ello la privacidad en todas sus dimensiones es susceptible de afectarse junto a la información reservada del usuario y consumidor de un sitio web, una aplicación, un programa. De tal modo, la personalidad en todos sus aspectos y los datos de cuentas bancarias, tarjetas de crédito, perfiles de usuarios, atributos de la personalidad (nombre, documentos, domicilio, estado civil, etc.) son objeto de sistematización, conservación en bases, utilización y negociación[4].

La utilización de la IA en esos entornos, sitios, plataformas, aplicaciones, redes profundiza los fenómenos descriptos y define hechos típicos. A modo simplemente enunciativo se verifican los peligros derivados de las acciones u omisiones que se describen a continuación:

a. Identificación biométrica utilizada para localizar o individualizar una persona a los fines de prevenir ilícitos (por caso una amenaza terrorista), al autor o víctima de un delito (por ej. trata de personas, explotación sexual). Los riesgos derivados son la construcción de "sistemas de categorización biométrica por creencias políticas, religiosas, filosóficas o por su raza y orientación sexual", de puntuación "de las personas en función de su comportamiento o características personales", la manipulación del comportamiento humano, o la creación de "bases de datos faciales captando datos de manera indiscriminada a través de internet o de grabaciones audiovisuales" así como el reconocimiento de emociones en los centros de trabajos o escuelas". [5]

b. Tratamiento automatizado de datos personales. La Ley de Protección de Datos Personales no pudo prever, por la fecha de su sanción, el impacto de la IA en la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo,

---

[4] AZAR, ALDO MARCELO. "La obligación de seguridad por indemnidad de datos personales, imagen, intimidad, identidad y privacidad", LA LEY 04/08/2022, 04/08/2022, 1. LALEY AR/DOC/2210/2022. AZAR, Aldo Marcelo - MARTINI, Luciano José, *El valor seguridad en los modelos tecnológicos de derecho privado: la conformación de una nueva obligación de seguridad*, en Direito civil e temas transversais, Renato Dellova (coord.), Schoba, São Paulo, 2020, ps. 35 a 66; y *Obligación de seguridad y responsabilidad por recopilación, guarda, conservación, manipulación y divulgación de datos, imágenes e información personalísimos*, en Instituciones de responsabilidad civil: homenaje al maestro Jorge Santos Ballesteros, tomo II, ps. 91-156, Saúl Uribe García y Alejandro Gaviria Cardona (coords.), Fondo Editorial UNAULA, de la Universidad Autónoma Latinoamericana, Bogotá, 2022.

[5] DE DIEGO, "La responsabilidad de los robots …", ob. y lug. cit.

destrucción y en general el procesamiento de datos personales, así como su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias (art.2 de la ley 25.326). A partir del empleo de la IA la obtención y procesamiento de toda esa información se automatiza, acelera y sistematiza con funciones nuevas.

c. Elaboración de perfiles. Una de las nuevas funciones que la recolección y procesamiento de datos personales adquiere es la elaboración de perfiles humanos que consisten en caracterizar los gustos, intereses, condiciones, características, estados, preferencias de los usuarios a los fines de predecir facetas de su comportamiento, para evaluar aspectos de una persona humana, para analizar rendimiento profesional o laboral, para determinar su situación económica, estado de salud, intereses, fiabilidad de su obrar, ubicación, etnia, género.[6]

d. Comparación y actualización de los perfiles. Una vez obtenido el perfil descripto en el punto anterior, la siguiente función consiste en el seguimiento de los intereses, gustos, calidades de cada usuario para ofrecer bienes, servicios y productos que se adecúen a esa evolución. Esto exige a la vez la actualización constante de cada perfil que permita detectar cambios en los comportamientos de cada usuario para lo cual se ejerce una vigilancia constante de su obrar en los entornos digitales a los fines de ofrecer la publicidad acorde los nuevos intereses, gustos y actitudes. [7]

e. Transferencia y disposición de los perfiles. "La dinámica del tratamiento automatizado de datos personales con inteligencia artificial implica la transferencia constante de datos dentro del país y hacia el extranjero".[8] Con esto se produce la transmisión o cesión de toda esa información personal a terceros con los que el usuario no interactuó ni supo que dispondrían de aquélla. "El hecho de captar datos, someterlos a tratamiento automatizado, actualizarlos, compararlos de manera constante, genera un valor estratégico que transforma los perfiles digitales humanos en un producto, objeto de múltiples transacciones. Por un lado se encuentran las plataformas que llevan adelante el tratamiento automatizado. Por el otro, las empresas interesadas en utilizar dichos perfiles para basar en ellos su

[6] PAPINI, CARINA M.. HELEG, GISELLE. "Proteger perfiles digitales humanos ante el imparable avance de la inteligencia artificial", LA LEY 8.3.2024, 18.

[7] Idem anterior.

[8] Idem anterior.

lógica de negocio o conocer todo tipo de comportamientos, gustos, intereses o preferencias. El producto son los perfiles digitales pertenecientes a los mismos usuarios humanos".[9]

3. LA AFECTACIÓN DE LOS DERECHOS PERSONALÍSIMOS Y DE LOS ATRIBUTOS DE LA PERSONALIDAD

Los fenómenos descriptos en el punto anterior determinan daños materiales y morales que se sustentan en la aptitud que tienen para lesionar los aspectos más centrales de la privacidad e intimidad de una persona por el uso no autorizado de sus datos o información personal.[10] En efecto se advierte cada vez con mayor intensidad que los entornos virtuales (Internet, sitios web, aplicaciones, redes sociales, etc) son una fuente generadora de datos privados susceptible de acumulación y comercialización. Ejemplo de ello son los datos que las empresas privadas registran de sus empleados o que obran almacenados en archivos del Estado; que efectúan los intermediarios de créditos, las empresas de líneas aéreas, los registros impositivos, censos, de naturaleza médica, de información personal financiera; que recopilan las compañías de seguro y de telecomunicaciones. Similar situación se advierte en el incremento del número y la variedad de relaciones jurídicas celebradas o ejecutadas en redes sociales como Facebook, Twitter o Instagram; en aplicaciones utilizadas en los dispositivos móviles que ofrecen servicios de intermediación relacionados con la búsqueda de información (Google), transporte (Uber), cadetería (Glovo) o entrega de productos y alimentos (Pedidos Ya); tarjetas de crédito, contratos bancarios electrónicos, como así también los sitios de Internet en general, que se sirven de datos personales de los usuarios, con grave e irreversible quebrantamiento de su derecho de privacidad

Las imágenes y voz de una persona obtenidas de sus fotografías, videos, audios y demás registros audiovisuales; su salud definido por las dolencias que consigna o informa en una aplicación del Estado o de su seguro médico, obra social o medicina prepaga dentro de las cuales se hallan aquellas protegidas (caso de los infectados por VIH o enfermos de SIDA); sus opiniones relativas a creencias religiosas o políticas vertidas en

---

[9] Idem anterior.

[10] DE LORENZO, MIGUEL FEDERICO, *Derechos personalísimos y determinismo tecnológico (a propósito de la tutela de los datos personales), p*ublicado en: EBOOK-TR 2024 (Tobías-Sambrizzi), p. 783

comentarios de redes sociales; su identidad sexual registrada en aplicaciones, programas o sitios web en los que interactúa con fines de interactuar o entablar un vínculo sexoafectivo, la localización del usuario son algunos de los aspectos registrados, sistematizados, comparados, vigilados y transferidos al conformarse su perfil digital.

La información relativa a cuentas bancarias, tarjetas de crédito, claves de acceso a plataformas en las cuales opera, contrata, adquiere y vende bienes y servicios ingresan al campo de datos recopilados, conservados, guardados y susceptibles de ser afectados por hackeos. De ese modo el patrimonio del usuario o al menos un aspecto de él queda alcanzado y afectado por los riesgos ya descriptos.

Como resultado de todo ello, los derechos personalísimos a la intimidad, privacidad, identidad en todas sus manifestaciones, a la no discriminación, y los atributos de la personalidad tales como el nombre, el domicilio, el patrimonio son los intereses y bienes extrapatrimoniales susceptibles de ser lesionados y dañados por la IA en los entornos virtuales.

4. FACTORES DE ATRIBUCIÓN DE RESPONSABILIDAD

Las soluciones propugnadas para solucionar los problemas de prevención y resarcimiento de daños causados por la IA aplicada en los entornos virtuales (sitios de internet, plataformas digitales, redes sociales, aplicaciones, etc.) vienen reconociendo los siguientes factores atributivos de responsabilidad.

Un sector mayoritario se pronuncia por la configuración de una responsabilidad de corte objetivo cuyos sustentos son, alternativa o conjuntamente, el riesgo de la cosa si la IA opera con la intermediación de máquinas11, la actividad riesgosa para todo lo que es sistema, algoritmo, programas o tecnología que utiliza la IA12, el riesgo por el producto

---

[11] DE DIEGO, "La responsabilidad de los robots …" ob. y lug. cit.

[12] COLOMBO MARIA CELESTE, *La responsabilidad civil derivada del uso de algoritmos en el derecho de consumo* EBOOK-TR 2023 (Colombo) , 43, TR LALEY AR/DOC/767/2023; PICASSO NETRI, LISANDRO *Responsabilidad de las entidades bancarias por estafas informáticas*, Publicado en: EBOOK-TR 2024 (Gómez Leo-Dasso) , 1019 , Cita: TR LALEY AR/DOC/747/2024

elaborado si el daño se produce en el marco de una relación de consumo13, el vicio de la cosa si el algoritmo o sistema presenta algún defecto14, y el incumplimiento de una obligación de seguridad[15].

Un sector minoritario diferencia supuestos de responsabilidades subjetivas y objetivas. Con relación a las plataformas digitales, sin haber enfocado la cuestión a partir de la incidencia de la IA, se considera la asunción de una obligación de medios con un factor de corte subjetivo cuando dichas plataformas cumplen de anuncios, sin un deber de vigilar o supervisar la conducta de las partes que contratan por fuera de ellas. En los casos en que la plataforma brinda una prestación de servicios conexos en la contratación electrónica, coadyuvando a la celebración del contrato formalizado a través de ella o cumpliendo una incidencia ineludible, la atribución asumida es de corte objetivo16. Otra perspectiva que centra la cuestión en la IA, diferencia según los riesgos del uso de la misma. Si el riesgo es bajo o mínimo, la responsabilidad es subjetiva; si el riesgo es alto o inaceptable, será objetiva. Entran en este último encuadre todos los sistemas cuyos usos se consideran inaceptables por ser violatorios de los derechos fundamentales[17].

5. LA CONFIGURACIÓN DE UNA NUEVA Y ESPECIAL OBLIGACIÓN DE SEGURIDAD.

a) La obligación de seguridad en el modelo industrial de derecho privado.

La restitución, preservación o mantenimiento del contratante, sano y salvo, hasta la finalización del contrato conforman el objeto de las

---

[13] COLOMBO, *La responsabilidad civil …* ob. cit. MELO, VERÓNICA E. "Responsabilidad por daños e inteligencia artificial: ¿vino nuevo en odres viejos?", RCyS 2021-III , 3.

[14] COLOMBO, *La responsabilidad civil …* ob. y lug. cit.

[15] IMIRIZALDU, HORACIO DANIEL, "Inteligencia artificial. los riesgos de la recopilación de datos biométricos", SJA 07/06/2024 , 1, COLOMBO, ob. cit.

[16] AICEGA, MARIA VALENTINA. *Alcances del deber de responder de las plataformas digitales. quid de sus grados de intervención,* EBOOK-TR 2024 (Gómez Leo-Dasso) , 1039 Cita: TR LALEY AR/DOC/750/2024

[17] Resolución del Parlamento Europeo del 20.10.2020. Citado por COLOMBO, *La responsabilidad …* ob. y lug. cit.

obligaciones denominadas de seguridad o, más genéricamente, de protección. La gestación, construcción, enunciación, desarrollo y evolución de esta obligación en el derecho privado no ha sido lineal ni pacífica.

En 1911 la Cour de Cassation francesa falla en la causa "Zbidi Hamida c. Compagnie Générale Transatlantique" en la que consigna "la ejecución del contrato de transporte comporta, en efecto, para el transportador, la obligación de conducir al viajero sano y salvo a destino"[18]. En esos términos introduce la obligación de seguridad en el ámbito de la responsabilidad contractual y, con ella, a los intereses extrapatrimoniales en la prestación, tales como la vida, la integridad corporal y psíquica, los que se definen como el resultado que debe garantizarse[19].

b) El resurgimiento de las obligaciones de seguridad en el modelo tecnológico y posmoderno vigente: los Tratados Internacionales de Derechos Humanos.

En el modelo industrial —que se gestó desde las tres últimas décadas del siglo XIX hasta los últimos decenios del siglo XX— se intenta una primera ampliación del contenido de la obligación de seguridad, pues originariamente circunscripta a la vida, salud e integridad psicofísica de una de las partes de la relación se extendió a la protección de sus otros bienes[20].

En el actual modelo tecnológico, globalizado, postindustrial, posmoderno, los ataques a la persona, antes circunscriptos a la protección de la vida y de la salud del contratante, han mutado y se ampliaron a la

---

[18] Cour de Cassation, 21/11/1911.

[19] BELLISSENT, Jean, *Contribution à la distinction des obligations de moyens et de résultat*, LGDJ, Paris, 2000, p. 316 y ss.

[20] Como *seguridad de los bienes:* D´AMICO, Giovanni, *La responsabilità ex recepto e la distinzione tra obbligazioni di mezzi e di risultato*, Scientifiche Italiane, Napoli, 1999, p. 88, n.88 y p. 89. Como *seguridad de la persona y de los bienes: PIZARRO, Responsabilidad civil por riesgo ..., ob. cit., t. III, p. 257. BUSTAMANTE ALSINA, Jorge, Teoría general de la responsabilidad civil, Abeledo-Perrot, Buenos Aires, 1987, 8ª ed., p. 387. VÁZQUEZ FERREYRA, Roberto, "La obligación de seguridad y la responsabilidad contractual", RDPC t.17, p. 79. AGOGLIA, María - BORAGINA, Juan - MEZA, Jorge, "Responsabilidad contractual de los profesionales", JA-III-730. CABANILLAS SÁNCHEZ, Antonio Las obligaciones de actividad y de resultado, Bosch, Barcelona, 1993, p. 78. PASCUAL ESTEVILL, Luis, La responsabilidad contractual, Bosch, Barcelona, 1992, t. I, p. 72. BELLISSENT, Contribution ..., ob. cit., ps. 259, 266.*

personalidad comprensiva de su intimidad, de su privacidad y de la información atinente a ellas.

Las fuentes que determinan el surgimiento de esta especial obligación de seguridad son los Tratados Internacionales de Derechos Humanos a la luz de los cuales corresponde aplicarse e interpretarse la ley (arts 1 y 2 CCCN).

Los Tratados Internacionales de Derechos Humanos consagran el valor y la garantía de la seguridad como uno de los derechos fundamentales de la persona. A modo enunciativo, la seguridad se erige en un derecho humano esencial en la Declaración Americana de los Derechos y Deberes del Hombre (art. I) conjuntamente con los derechos personalísimos a la honra, a la reputación personal y privacidad (art. V); en la Declaración Universal de los Derechos Humanos (art. 3) conjuntamente con los derechos a la no discriminación (art. 1); en la Convención Americana sobre Derechos Humanos (art. 7.1) conjuntamente con la prohibición de discriminación (art. 1.1) y el derecho a la honra y dignidad (art. 11), entre otros.

Ante ello, la obligación de seguridad en el actual paradigma neoconstitucional se reconfigura para extenderse a la protección de los derechos personalísimos, atributos de la personalidad, datos e información personal del ser humano. Caracterizada como un deber jurídico específico y de naturaleza secundaria que pesa sobre el deudor cuyo objeto es la protección de la indemnidad del contratante, la obligación de seguridad está orientada al resguardo de su integridad no solo física sino moral durante el curso ejecución de una relación jurídica. Como se señaló, su primer y más enérgico interés fue la protección de la vida y la salud de la contraparte entendidos en su más amplia acepción. Su centro de gravedad está, por así decirlo, en la cuestión relativa a la protección de intereses distintos al de la prestación principal. El proceso de evolución del valor seguridad continuó con el reconocimiento de prestaciones consistentes en la conservación, mantenimiento, reparación, guarda custodia y seguridad de los bienes.

Hoy en el marco de relaciones jurídicas gestadas por la IA en entornos virtuales como Internet el deber de seguridad adquiere una nueva dirección, donde la protección de la salud, la integridad física, pasa a segundo plano con relación al interés de privacidad que tiene el acreedor en estos nuevos entornos interacción.

La seguridad se amplía para connotar otros aspectos de la personalidad y se extiende para abarcar la protección de la intimidad y

confidencialidad en las relaciones jurídicas originadas en un marco de relaciones nacidas, desarrolladas y cumplidas en un marco de la realidad virtual operada por la IA.

Uno de los rasgos especialmente característicos de estas últimas relaciones jurídicas es la creciente tendencia hacia los problemas relacionados con la vulneración de la privacidad de los usuarios de aplicaciones, redes, sitios de internet, plataformas, sean consumidores o no, por el uso no autorizado de sus datos o información personal. En efecto se advierte cada vez con mayor intensidad que la tecnología utilizada por la IA es una fuente generadora de datos privados susceptible de acumulación y comercialización.

Concebida de tal modo la cuestión, se inicia la gestación de un modelo de obligación de seguridad que responde a un nuevo paradigma tecnológico, postindustrial y globalizado donde el fenómeno jurídico obligacional cuenta con ciertos perfiles propios característicos, cuyo común denominador es la utilización de entornos virtuales, en los cuales Internet es al momento actual la vía en la que se concentra toda la actividad, y en la que la IA es el agente principal de gestión.

6. LA RESPONSABILIDAD POR DAÑOS CAUSADOS POR LA IA EN ENTORNOS VIRTUALES.

Los daños causados por la utilización de la IA en entornos virtuales admite múltiples causas que determinan diversos factores atributivos de responsabilidad. COLOMBO sintetiza esos supuestos en tres aspectos: "a) responsabilidad civil derivada de actividades riesgosas, b) responsabilidad por daños causados por productos defectuosos; y c) responsabilidad derivada del incumplimiento de la obligación de seguridad."[21]

De esos tres supuestos, cabe formular las siguientes consideraciones.

La configuración de una actividad riesgosa está controvertida según el mayor o menor riesgo de los sistemas. La aceptación de una responsabilidad subjetiva en el caso de riesgos bajos, aceptables o mínimos controvierte la aceptación de una actividad riesgosa en los términos y con los lineamientos del art. 1757 CCCN.

---

[21] COLOMBO, *La responsabilidad civil …"*, ob. y lug. cit.

Con respecto a la posibilidad de encuadrar la responsabilidad por producto defectuoso (art. 40 ley 24240) o vicio de la cosa (art. 1757 CCCN) se parte del presupuesto de una falla, bug, insuficiencia del sistema. Está fuera de discusión esa atribución de responsabilidad pero la misma es marginal o determinada por una prueba prácticamente imposible de producir por el damnificado de la IA en esos entornos virtuales.

Toda controversia o impugnación cede ante la conformación de una obligación de seguridad y de resultado (art. 1723, 774 inc.b CCCN) que determina la responsabilidad de los diseñadores, desarrolladores, aplicadores [22], ingenieros, programadores, fabricantes, inversores, vendedores[23], proveedores, empresas que utilizan la inteligencia artificial a lo largo y a lo ancho de toda la cadena de valor24 de modo concurrente si el daño se causa en el ámbito de una situación o relación de derecho privado (art. 850 CCCN) o solidario si se produce con motivo u ocasión de una relación de consumo (art. 40 Ley 24240).

La obligación de seguridad es de resultado por cuanto el titular del servicio, aplicación, sitio, red y de la IA aplicado o utilizada para la gestión en el entorno virtual son quienes asumen la preservación del usuario o consumidor en cuanto obtiene, manipula, conserva y dispone de los datos personales en un proceso causal del cual es el único agente que introduce y controla el riesgo de inmisión.

El resultado de esa prestación es negativo: consiste en no violar la privacidad del usuario o consumidor por las técnicas de recopilación, almacenamiento y tratamiento de datos personales. Ese resultado es una consecuencia directa e inmediata de sus propios procesos tecnológicos, de su intervención y de la conservación de aquéllos. Su situación no es diferente a la de la entidad bancaria que brinda el servicio de cajas de seguridad y se responsabiliza por la custodia de los efectos confiados. En este caso, el titular del programa, plataforma, sitio, aplicación virtual y de la IA en ellos aplicada obtiene los datos, imágenes, valores y accesos a la intimidad del usuario y los guarda en sus propias bases de datos para luego utilizarlos o

---

[22] SANTARELLI, FULVIO G, "Una inteligencia artificial responsable. propuestas de encuadramiento y método para una regulación de la inteligencia artificial responsable" LA LEY 09/08/2023 , 1 • LA LEY 2023-D , 338

[23] DE DIEGO, "La responsabilidad de los robots …", ob. y lug. cit.

[24] COLOMBO, *La responsabilidad civil …,* ob. y lug. cit.

comerciar con ellos ante terceros. Si el cliente del banco deposita sus bienes en una caja de seguridad y el banco se obliga a una seguridad en que el hecho del tercero ajeno y el caso fortuito inherente a la actividad de conservación no exime de responsabilidad, con mucho mayor motivo se funda y amplía la seguridad impuesta a quien conserva, mantiene, custodia, manipula y dispone de información personalísima de terceros, incluso sin su consentimiento, en una base de datos propia. El resultado impuesto define una responsabilidad de corte objetivo pues sólo admitiría la eximición por la culpa exclusiva de la víctima o por un caso fortuito o fuerza mayor extraños a la operatoria de internet. La culpa es absolutamente irrelevante a los efectos de fundamentar la atribución de responsabilidad.

Por otra parte, cabe destacar que la conducta que tiene que desplegar el titular del sitio, plataforma, aplicación en la que se utiliza la IA consiste en mantener indemne al usuario y aquélla se coloca como una causa inmediata con respecto a ese efecto, proyectando sus efectos a la calificación del vínculo como una obligación de resultado.

Ante argumentos relativos a un permiso concedido por el usuario para la utilización de su información personal, la progresiva proliferación de maquilladas licencias que los consumidores otorgarían al amparo de términos y condiciones aceptados por un simple click o mediante la mera utilización del sitio deben tenerse por no convenidas. La solución puede ser propiciada a través de los diversos conceptos relacionados con: i) las notas particulares que tiene el proceso de formación deficiente del consentimiento por parte del consumidor en estas relaciones de consumo, y ii) el cumplimiento defectuoso de la obligación de información para todo otro usuario. No se configura consentimiento del damnificado cuando la información relativa a la utilización del entorno en el que opera la IA no se brinda sino que se impone como una adhesión a cláusulas predispuestas por las que se otorga un derecho a disponer de los datos que afectan a derechos personalísimos del usuario o consumidor.

A igual resultado se llega cuando los titulares de sitios obtienen ese consentimiento a través de un hipervínculo adonde se remite el contenido o simplemente mediante un click del mouse en “aceptar”. La información así concebida se torna, por lo general, ineficaz. En esos ámbitos no existen actos de comunicación negocial mediante un simple click en “aceptar” o un hipervínculo al que los consumidores nunca acceden, no les interesa revisar, no leen, y tampoco cuentan con posibilidades concretas de discutir su no incorporación. En efecto, debido a la particular estructura sobre la cual se

asientan los nuevos modelos de negocios en entornos virtuales e Internet, el consumidor o usuario carece de información suficiente como para lograr un consentimiento pleno. Y éste no puede conformarse si la admisión de la lesión a sus intereses extrapatrimoniales es puesta como condición para poder navegar o utilizar el programa, aplicación, sitio en que opera la IA.

En este nuevo marco social, cultural y jurídico, la reformulación de la obligación de seguridad que proteja esos bienes e intereses no patrimoniales e inherentes a la personalidad de los sujetos se impone y se justifica como una prestación de resultado que determina una responsabilidad objetiva en cabeza del titular del servicio, plataforma, aplicación, programa o entorno virtual que utiliza la IA y dispone de esos datos como guardianes de los mismos y por lo tanto se constituyen en garantes de la privacidad, confianza, identidad personal e intimidad de quien se los ha provisto.

Esta obligación de resultado es agravada por cuanto no basta la mera acreditación de una causa ajena para la eximición de responsabilidad. En efecto, las características de la actividad imponen a quien obtiene, manipula, conserva, transmite los datos, imágenes o información personalísima la misma responsabilidad que para quienes asumen la seguridad de bienes o efectos personales depositados en una caja de seguridad, sea de una entidad[25] bancaria o de una especialista en la guarda de valores. Al igual que en estos últimos casos, quien detenta los datos o información de un usuario que se los ha confiado o de quien se han obtenido, con o sin su pleno consentimiento, responde por los ataques o violaciones a la seguridad que terceros extraños pudieran realizar de sus bases de datos. Otro tanto ocurre con el eventual caso fortuito o fuerza mayor que para ser eximentes válidos deben ser ajenos al riesgo inherente a la actividad de la red social, aplicación, soportes de internet o bases de datos en los que se almacenan la información o las imágenes que hacen a los derechos personalísimos de los usuarios. Por

[25] AZAR, Aldo Marcelo - MARTINI, Luciano José, "El valor seguridad en los modelos tecnológicos de derecho privado: la conformación de una nueva obligación de seguridad", en Direito civil e temas transversais, Renato Dellova (coord.), Schoba, São Paulo, 2020, ps. 35 a 66; y "Obligación de seguridad y responsabilidad por recopilación, guarda, conservación, manipulación y divulgación de datos, imágenes e información personalísimos", en Instituciones de responsabilidad civil: homenaje al maestro Jorge Santos Ballesteros, tomo II, ps. 91-156, Saúl Uribe García y Alejandro Gaviria Cardona (coords.), Fondo Editorial UNAULA, de la Universidad Autónoma Latinoamericana, Bogotá, 2022.

ello, sólo el hecho exclusivo de la víctima y el caso fortuito o fuerza mayor extraños al riesgo de la actividad son idóneos para liberar al civilmente responsable por los ataques, difusión o comercialización de los datos, imágenes e información personalísima del usuario de internet.

EL FACTOR DE ATRIBUCIÓN EN LA RESPONSABILIDAD POR DAÑOS CAUSADOS POR INTELIGENCIA ARTIFICIAL

Por María Florencia Blanco Pighi[1] y Matías Machado[2]

I. CONCLUSIONES

1. Al analizar los supuestos de responsabilidad por actuación de IA podemos afirmar que hay casos en los que el factor de atribución es claro, como ocurre con los automotores autónomos (arts. 1769, 1757 y 1758 del CCCN y la Ley Nacional de Tránsito). El factor de atribución es objetivo y los legitimados pasivos son identificados por el Código. En el caso de los buscadores de internet por daños causados por la implementación de sus algoritmos de indexación el factor de atribución aplicable es subjetivo (fallos CSJN). En los demás supuestos se deberá determinar en el caso concreto si el mecanismo utilizado puede ser englobado bajo el concepto de cosa o actividad riesgosa, de acuerdo a los parámetros mencionados en esta ponencia. Además, en los casos en los que exista una relación de consumo, tendrán legitimación pasiva todos los miembros de la cadena de producción (ley 24.240). En los restantes supuestos se deberá analizar si responden los titulares de IA que proporcionen servicio de soporte o técnico, o los usuarios. Finalmente, consideramos que sería útil consignar estándares normativos concretos que arrojen claridad en el tema.

---

[1] Abogada (UNC). Profesora en Ciencias Jurídicas (UNC). Maestranda en Derecho Civil Patrimonial (UNC). Profesora Auxiliar dedicación semi exclusiva de Política y Derecho Educacional y Pedagogía General (Profesorado en Cs. Jurídicas, Fac. Derecho. UNC). Jefa de trabajos prácticos de Derecho Privado VIII (UCC). Investigadora UNC. UCC.

[2] Abogado (UNC), Magister en derecho civil patrimonial (UNC), Profesor Ayudante "A" con dedicación simple (C.119) en la Cátedra "A" de la asignatura Derecho Privado VII de la carrera de Abogacía (UNC).

Aval: Dr. José Fernando Márquez. Docente titular de la cátedra "B" en la asignatura Derecho Privado VII (Daños) en la Facultad de Derecho de la Universidad Nacional de Córdoba.

II. FUNDAMENTOS

1. INTRODUCCIÓN

En la presente ponencia procederemos a dar tratamiento a la temática del factor de atribución aplicable en los daños causados por sistemas de inteligencia artificial, cuya utilización se ha acrecentado en los últimos tiempos, lo que terminará provocando que nos encontremos frente a nuevos supuestos en los cuales su uso podrá generar algún tipo de perjuicio, de naturaleza patrimonial o extrapatrimonial.

En primera medida, se realizará un análisis general de esta figura, y luego se examinará cuál es el fundamento que debe utilizarse para determinar si se debe responder en estos casos, al establecer cuál es el factor de atribución que le resulta aplicable. A estos fines, se observarán las escasas legislaciones existentes en la materia y los antecedentes jurisprudenciales de nuestro país.

2. INTELIGENCIA ARTIFICIAL – DEFINICIÓN Y CATEGORÍAS

La inteligencia artificial (en adelante IA) ha sido definida como la disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico[3].

Se ha dicho que *"la IA se ha consolidado como la gran promesa del futuro, -aunque podríamos decir que del presente-, que trae consigo la posibilidad de remplazar al humano en sus tareas"*[4].

En el libro blanco de la inteligencia artificial se establece que el término IA se aplica a los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción —con cierto grado de autonomía— con el fin de alcanzar objetivos específicos. Los sistemas basados en la IA pueden consistir simplemente en un programa informático (p. ej. asistentes de voz, programas de análisis de imágenes,

---

[3] https://dle.rae.es/inteligencia#2DxmhCT consultado el 01/05/2024

[4] FOSSACECA (h.), Carlos A. MOREYRA, Pilar; *Aproximaciones a la responsabilidad civil por la utilización de inteligencia artificial y derecho de los robots. Una mirada jurídica.* Publicado en: RCyS 2020-VIII , 20. Cita: TR LALEY AR/DOC/2254/2020.

motores de búsqueda, sistemas de reconocimiento facial y de voz), pero la IA también puede estar incorporada en dispositivos de hardware (por ej. robots avanzados, automóviles autónomos, drones o aplicaciones del internet de las cosas).

Por otro lado, refiere a un concepto más depurado, al identificarla con programas informáticos (y, posiblemente, también equipos informáticos) diseñados por seres humanos que, dado un objetivo complejo, actúan en la dimensión física o digital mediante la percepción de su entorno mediante la adquisición de datos, la interpretación de los datos estructurados o no estructurados, el razonamiento sobre el conocimiento o el tratamiento de la información, fruto de estos datos y la decisión de las mejores acciones que se llevarán a cabo para alcanzar el objetivo fijado[5].

Además, se ha distinguido entre IA débil e IA fuerte. El objetivo de la primera, es la resolución de problemas concretos de manera "inteligente" y busca el desarrollo de programas que resuelvan problemas concretos y acotados, actuando como si fueran humanos. Cuando nos referimos a la segunda, hablamos de máquinas o sistemas que tengan todas las habilidades mentales de los seres humanos, o incluso que superen la inteligencia humana (superinteligencia), aunado a la conciencia, sensibilidad, autoconocimiento y sabiduría6. Existen numerosos mecanismos de inteligencia artificial débil o estrecha a los que el público puede acceder, como los sistemas de recomendación de canciones o videos o los algoritmos de clasificación de páginas web.

Recientemente, la Unión Europea[7] (en adelante UE) ha distinguido legalmente entre "IA de propósito general", por ejemplo, el ChatGPT, para la que exige transparencia en todos los modelos (se requiere a las empresas que elaboren documentación técnica, el cumplimiento de la ley de derechos

---

[5] Comisión europea "*Libro blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza*", COMUNICACIÓN BRUSELAS, BELGICA, 19 de Febrero de 2020, consultado en Id SAIJ: LNT0007437

[6] RODRIGUEZ, Ricardo y MARTÍNEZ, María Vanina en DANESI, Cecilia. 2021. *Inteligencia artificial, tecnologías emergentes y derecho 2* [En Línea]. (1ª Edición). Argentina: Hammurabi. Consultado el 01/05/2024.

[7] https://www.lanacion.com.ar/tecnologia/una-ley-pionera-para-una-tecnologia-con-muchos-interrogantes-las-claves-de-la-regulacion-de-la-nid11122023/?gad_source=1&gclid=CjwKCAjwouexBhAuEiwAtW_Zx5C5f46MKmKJwxd2SPusKz6Jtqfkm64A1YvZ9Hi98h-0wzwBG-Va-BoCRvQQAvD_BwE

de autor de la UE y la difusión de resúmenes detallados sobre el contenido utilizado para la formación) y la "IA de alto impacto o de alto riesgo", en las que se imponen obligaciones más estrictas (las empresas tendrán que realizar evaluaciones de modelos, evaluar y mitigar riesgos sistémicos, realizar pruebas constantes, informar a la Comisión sobre incidentes graves, garantizar la ciberseguridad e informar sobre su eficiencia energética, pudiendo existir sanciones ante el incumplimiento). Así, esta normativa8 (que entrará completamente en vigor en 2026) busca prohibir los usos de la IA que violen los derechos fundamentales y los valores de la UE, establecer reglas claras para los casos de uso de alto riesgo y promover la innovación sin barreras para todos los casos de uso de bajo riesgo.

Si bien ningún otro territorio del mundo tiene una ley que abarque tantos aspectos como la reglamentación europea, en octubre de 2023 el presidente de Estados Unidos firmó un decreto que obliga a las empresas tecnológicas a notificar al gobierno cualquier avance que suponga un "riesgo grave para la seguridad nacional".

La determinación del fundamento axiológico para atribuir responsabilidad en estos supuestos dependerá del tipo de inteligencia artificial frente al cual nos encontremos y los mecanismos que se utilicen en el caso concreto.

3. LOS FACTORES DE ATRIBUCIÓN

Cuando hablamos de factores de atribución nos referimos a las razones que justifican la responsabilidad, que evidencian como justa y constituyen el fundamento o la explicación axiológica de la obligación de resarcir el perjuicio[9].

Estos pueden ser clasificados en factores de atribución subjetivos y objetivos. En el caso de los primeros el fundamento del deber de responder reside en la existencia de culpabilidad en sentido amplio (culpa o dolo). Se encuentran comprendidos en el art. 1724 del Código Civil y Comercial de

---

8 https://digital-strategy.ec.europa.eu/es/policies/european-approach-artificial-intelligence

9 ZAVALA DE GONZÁLEZ, Matilde, *Actuaciones por daños. Prevenir. Indemnizar. Sancionar*, ed. Hammurabi, Bs. As., 2004, p.201

la Nación (en adelante CCCN) que los distingue y establece una definición de culpa.

Los factores objetivos, son aquellos en los cuales existe una razón diferente para atribuir responsabilidad, totalmente ajena a la idea de culpabilidad, como puede ser el riesgo creado, la garantía, la falta de servicio o la equidad. De hecho, el art. 1722 CCCN establece que el factor de atribución es objetivo cuando la culpa del agente es irrelevante a los efectos de atribuir responsabilidad y que, en tales casos, el responsable se libera demostrando la causa ajena, excepto disposición legal en contrario.

En el caso de los daños causados por IA consideramos que el análisis debe centrarse en la necesidad de determinar si nos encontramos frente factores de atribución subjetivos o si, por el contrario, nos encontramos frente a un supuesto de responsabilidad objetiva, fundada en el riesgo creado.

Es decir, que se deberá determinar si, en estos casos, resultan aplicables los arts. 1757 y 1758 del CCCN que regulan la responsabilidad por daños causados por el vicio o riesgo de la cosa o por actividades riesgosas.

4. LOS FACTORES DE ATRIBUCIÓN Y LA INTELIGENCIA ARTIFICIAL

Seguidamente, nos centraremos en examinar de manera concreta qué factores de atribución resultan aplicables a la IA.

Ante todo, debemos destacar que existe un supuesto en el cual consideramos que no existe lugar a dudas que el factor de atribución es objetivo. Se trata del caso de los accidentes de tránsito provocados por vehículos autónomos, que son conducidos por IA.

La razón para sostener esta postura – de lege lata- es lo dispuesto en el art. 1769 del CCCN en el cual se efectúa de manera clara un renvío a los arts. 1757 y 1758 del CCCN en los casos de daños provocados por la circulación de vehículos. Al no realizar esta norma una distinción entre rodados conducidos por personas humanas y aquellos que se trasladan de manera autónoma, consideramos que estos últimos se encuentran englobados dentro de la normativa referenciada, lo cual implica que el fundamento para responder en estos casos sea el riesgo creado. De igual manera, quedarían comprendidos en la definición de automóvil y vehículo automotor del art. 5 de la Ley 24.449 (ley de tránsito nacional) los vehículos

autónomos. Con lo que no existen dudas en torno a la aplicación de este régimen en nuestro país.

Con respecto a los restantes supuestos, se deberá especificar en el caso concreto si nos encontramos frente a una situación que pueda ser englobada en los arts. 1757 y 1758, lo que implicaría la existencia de riesgo creado. Para ello, la normativa citada establece distintos criterios para determinar la configuración de estos supuestos y se refiere a el riesgo por su naturaleza, los medios empleados y las circunstancias de su realización.

El concepto de "cosa riesgosa" se sustenta en un criterio "estadístico". Si el riesgo consiste en la potencialidad dañosa de la cosa, entonces, son tales las que producen daños frecuentemente, regularmente, de acuerdo con lo que suele suceder según el orden natural de los acontecimientos (criterio de la causalidad adecuada). También habría que añadir al catálogo aquellas cosas que, aunque no causan daños habitualmente, pueden producir perjuicios de gran magnitud[10]. De la misma forma, se ha sostenido que el riesgo de la actividad puede ser detectado por un criterio cuantitativo o estadístico, a la ponderación de estándares fijados por el legislador y atendiendo razonablemente a las reglas de la experiencia[11] . La existencia del riesgo debe ser valorada de acuerdo a los estándares fijados por la teoría de la relación de causalidad adecuada.

El supuesto bajo análisis, deberá ser examinado de acuerdo a estos parámetros. Es por ello, que no resultará posible brindar una respuesta genérica para precisar cuál es el factor de atribución aplicable en todas las situaciones en las cuales haya sido provocado un daño por parte de la IA. Esto implica que se deberá analizar cada supuesto específico en el que se aplique este mecanismo, para determinar, caso por caso, si nos encontramos frente a una situación de responsabilidad subjetiva u objetiva.

Sin embargo, se pueden efectuar algunas precisiones, para así encuadrar determinadas situaciones dentro, o fuera del ámbito del riesgo creado.

---

[10] PICASSO, Sebastián y SAENZ, Luis R. J. *Tratado de Derecho de Daños*, Ed. La Ley, Bs. As, 2019, T.II, P. 130

[11] PIZARRO, Ramón D. y VALLESPINOS, Carlos G. *Tratado de Responsabilidad Civil*, Rubinzal – Culzoni editores, Santa Fe, 2018. P. 312 T.II

En efecto, la Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de IA (2020/2014(INL), establece algunos indicadores claros para determinar cuándo nos encontramos frente a un sistema de inteligencia artificial de alto riesgo.

Así, establece en su art. 3 inc. c: *"«alto riesgo»: el potencial significativo en un sistema de IA que funciona de forma autónoma para causar daños o perjuicios a una o más personas de manera aleatoria y que excede lo que cabe esperar razonablemente; la magnitud del potencial depende de la relación entre la gravedad del posible daño o perjuicio, el grado de autonomía de la toma de decisiones, la probabilidad de que el riesgo se materialice y el modo y el contexto en que se utiliza el sistema de IA;"*. Seguidamente, en su art. 4 impone la aplicación de un factor de atribución objetivo a los operadores de un sistema de IA de alto riesgo por cualquier daño o perjuicio causado por una actividad física o virtual, un dispositivo o un proceso gobernado por dicho sistema de IA. Asimismo, aclara que se hará constar en el anexo pertinente un listado de sistemas de inteligencia artificial de alto riesgo.

Por otro lado, en su art. 8 dispone que, quien no figure en el anexo del Reglamento, estará sujeto a responsabilidad subjetiva respecto de todo daño o perjuicio causado por una actividad física o virtual, un dispositivo o un proceso gobernados por el sistema de IA.

Ahora bien, cabe aclarar que en el reglamento aprobado el 14 de mayo de 2024 por el Parlamento de la Unión Europea eliminó las disposiciones referidas al factor de atribución aplicable para los operadores de inteligencia artificial.

Sin embargo, este Reglamento mantuvo una caracterización de los sistemas de alto riesgo y aclaró que serían considerados como tales aquellos contenidos en su anexo III. Allí contempla – entre otros – a los sistemas de identificación biométrica, a aquellos destinados a ser utilizados como componentes de seguridad en la gestión y el funcionamiento de las infraestructuras digitales críticas, del tráfico rodado o del suministro de agua, gas, calefacción o electricidad, a algunos vinculados con la educación y formación profesional, a Acceso a servicios privados esenciales y a servicios y prestaciones públicos esenciales y disfrute de estos servicios y prestaciones, y a aquellos referidos a la Administración de justicia y procesos democráticos.

Algunos autores, han señalado que *"en el caso de los factores de imputación subjetivos, conceptos como culpa, dolo negligencia, impericia o imprudencia parecen ser inaplicables a una máquina que, si bien ha logrado tomar decisiones de manera autónoma, no por ello debería ser considerada humana (...) en la hipótesis de aplicar los criterios de culpa y dolo a la IA, se partiría del presupuesto de que los robots gozan de la capacidad no solo de actuar sino de responder, algo que por el momento resulta inaudito, atendiendo a su falta de personalidad/patrimonio para cubrir el perjuicio ocasionado. En consecuencia, resultaría que la responsabilidad deberá siempre recaer en una persona humana o jurídica, titular del software, por ejemplo"*[12].

Es así que, consideramos que se podrá atribuir responsabilidad al usuario de la IA, como también al titular o creador de esta última, que brinda algún tipo de soporte, asesoramiento técnico o servicio de actualización. Se deberá analizar, en el caso concreto, si resulta posible atribuir responsabilidad a uno de ellos o a ambos. En este sentido, consideramos útiles los conceptos de operador inicial[13] y operador final[14] que brinda la Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de IA (2020/2014(INL.

En nuestro ordenamiento, resulta claro que se puede atribuir responsabilidad a toda la cadena de comercialización de un bien o servicio vinculado con mecanismos de inteligencia artificial, siempre que el daño sea provocado a un consumidor[15] por parte del proveedor, en razón del riesgo o vicio del servicio o actividad.

---

[12] FOSSACECA (h.), Carlos A. MOREYRA, Pilar; *Aproximaciones a la responsabilidad civil por la utilización de inteligencia artificial y derecho de los robots. Una mirada jurídica*. Publicado en: RCyS 2020-VIII , 20. Cita: TR LALEY AR/DOC/2254/2020

[13] Es definido como *"...toda persona física o jurídica que define, de forma continuada, las características de la tecnología y proporciona datos y un servicio de apoyo final de base esencial y, por tanto, ejerce también grado de control sobre un riesgo asociado a la operación y el funcionamiento del sistema de IA"*

[14] Es aquel considerado como "*...toda persona física o jurídica que ejerce un grado de control sobre un riesgo asociado a la operación y el funcionamiento del sistema de IA y se beneficia de su funcionamiento"*

[15] Definido en el art. 1 de la ley 24.240.

En los restantes casos, en los cuales el damnificado no sea un consumidor, se deberá encuadrar al proveedor - o al usuario - dentro de algunos de los supuestos de legitimación pasiva previstos en el art. 1758 del CCCN, a fin de atribuirle responsabilidad.

Por otra parte, existirán determinados casos, en los cuales el factor de atribución será subjetivo y se deberá demostrar la existencia de dolo o culpa del usuario o el titular del sistema de IA. Consideramos que, en el caso de los segundos, será necesario acreditar la existencia de algún tipo de control o servicio de soporte del bien o servicio para endilgarle responsabilidad.

Cabe aclarar que existen supuestos en los cuales, de acuerdo a la jurisprudencia de nuestro Máximo Tribunal, el factor de atribución necesariamente será subjetivo. Nos referimos a los casos en los que se ha resuelto que solo existe responsabilidad de los buscadores de internet, en las situaciones en las que no adopten una conducta diligente luego de haber sido debidamente notificados de la existencia de contenido lesivo que es indexado a través de sus algoritmos[16].

Como se puede observar, existen casos donde resulta claro que el factor de atribución aplicable es subjetivo; mientras que en otros supuestos (vrbg. vehículos autónomos), no hay dudas de que es objetivo.

Sin embargo, existen numerosas situaciones en las cuales el análisis tendrá que ser realizado de acuerdo a las circunstancias y mecanismos utilizados en el caso concreto, así como también de acuerdo al tipo de sistema de IA frente al cual nos encontramos, para determinar si estamos frente a una cosa o actividad riesgosa - conf. parámetros mencionados en los párrafos precedentes - con el objeto de aplicar un factor de atribución objetivo o si, por el contrario, se debe exigir al sindicado como responsable actuar con los estándares de diligencia que emergen de las reglas establecidas en los arts. 1721 y 1724 del CCCN.

Más allá de lo expuesto, consideramos que resultaría de utilidad que se consignen estándares normativos concretos, que permitan determinar con

[16] CSJN, "R., M. B. c. Google Inc. s/ daños y perjuicios" 28/10/2014 Cita online: LALEY AR/JUR/50173/2014 y "G., C. V. c. Google Inc. s/ daños y perjuicios 12/09/2017 Cita Online: AR/JUR/60631/2017

mayor claridad en qué casos la implementación de IA será riesgosa, para diferenciarlo de los supuestos en los cuales sólo responderán en virtud de un factor de atribución subjetivo.

5. CONCLUSIONES

En suma, del razonamiento efectuado se pueden extraer las siguientes conclusiones:

- Existen casos en los cuales resulta claro el factor de atribución aplicable en relación a los daños provocados por IA.

- En el supuesto de los automotores autónomos - en virtud de lo dispuesto en los arts. 1769, 1757 y 1758 del CCCN y la Ley Nacional de Tránsito- el factor de atribución es objetivo.

- En el caso de los daños causados por la implementación de algoritmos de indexación de los buscadores de internet el factor de atribución aplicable es subjetivo, conforme los estándares fijados por la Corte Suprema de Justicia de la Nación.

- Al analizar otras situaciones, en las cuales la inteligencia artificial haya intervenido en la producción de un daño se deberá determinar en el caso concreto si el mecanismo utilizado puede ser englobado bajo el concepto de cosa o actividad riesgosa, de acuerdo a los parámetros mencionados en esta ponencia.

- Consideramos que resulta claro que cuando estemos ante un vehículo autónomo serán legitimados pasivos el dueño o guardián (Art. 1757 y 1758 CCCN). Cuando quien opere con IA sea un consumidor estará legitimada pasivamente toda la cadena de producción (conforme lo normado por la Ley 24.240 y sus modificatorias) y, en los casos en los que no estemos ante supuestos de relaciones de consumo, serán legitimados pasivos el titular de la IA, quien proporcione servicio de soporte o técnico (en el caso de la responsabilidad subjetiva, a título de dolo o culpa) y quienes operen, como dueños, guardianes o simples usuarios que podrán responder de acuerdo al factor de atribución que corresponda .

- Resultaría de utilidad la que se consignen estándares normativos concretos, que permitan determinar con mayor claridad en qué casos la implementación de inteligencia artificial será riesgosa, para diferenciarlo de los supuestos en los cuales sólo responderán en virtud de un factor de atribución subjetivo.

DAÑOS CAUSADOS POR VEHÍCULOS DE CONDUCCIÓN AUTOMATIZADA Y/O AUTÓNOMA EN EL DERECHO ARGENTINO

Por Florencia Bollatti[1]

I. CONCLUSIONES

1. De lege data: Los vehículos automatizados, en todos sus niveles, pueden ser subsumidos en la definición prevista en la Ley Nacional (art. 5, inc. x) de "vehículo automotor".

2. De lege ferenda: Se destaca la conveniencia de distinguir desde el aspecto regulatorio, entre la noción "tradicional" de vehículo automotor y vehículo automatizado o autónomo, conforme los niveles de automatización aceptados internacionalmente, principalmente, a los efectos de la autorización de software y sistemas de IA que permiten la asistencia al conductor.

3. Se propone la siguiente definición de vehículo automatizado: "Un vehículo automatizado es un robot que cuenta con sistemas de IA y conectividad digital (entre vehículos y con la infraestructura vial) que permiten, con distintos grados (del 0 al 5), la conducción del vehículo con una intervención asistida (nivel 0 a 2, inclusive), secundaria y/u ocasional del conductor humano (nivel 3) o, directamente, sin ésta (niveles 4 y 5)."

4. De lege data: Los vehículos automatizados, en todos sus niveles, quedan incluidos dentro del ámbito material de aplicación de la "Responsabilidad derivada de la intervención de cosas y de ciertas actividades" contemplada en la Sección 7ª del Capítulo 1 del CCC, por remisión del art. 1769, CCC.

5. De lege data: Los proveedores y/o fabricantes de los sistemas de IA implicados en el manejo de un vehículo automatizado no son guardianes de los vehículos y, por ende, no resultan legitimados pasivos

---

[1] Abogada (UNC, 2018). Premio Egresada Sobresaliente. Escribana (Universidad Siglo XXI, 2020). Maestranda en Derecho y Argumentación (UNC, 2020 -). Maestranda con Beca Académica en "Derecho de Daños" (Universitat de Girona, 2023 -). Asistente de Magistrado en la Cámara de Apelaciones en lo Civil y Comercial de Tercera Nominación de la ciudad de Córdoba. Adscripta a la Cátedra de Derecho Privado VII (Derecho de Daños), Facultad de Derecho, UNC. Ponencia con aval del Prof. Titular Derecho Privado VII (Facultad de Derecho, UNC), Dr. José Fernando Márquez.

en las acciones de responsabilidad por accidentes de tránsito, incluso aunque el accidente se haya debido a una "decisión" tomada por el vehículo sin intervención directa del conductor humano.

6. De lege data: La responsabilidad de aquellos que participan en el diseño, fabricación o implementación de los sistemas de IA, en tanto productos, ya tiene cabida en el marco del derecho de consumo, por lo que debe descartarse cualquier solución que pretenda transformar los accidentes de tránsito dónde interviene un vehículo autónomo en supuestos de responsabilidad por productos defectuosos (cfr. Art. 40, Ley N° 24240).

7. De lege ferenda: En los vehículos automatizados nivel 0 a 2 inclusive (con sistemas de asistencia a la conducción o ADAS), la aplicación del régimen de responsabilidad civil no presenta grandes matices respecto al vehículo "clásico", pues la conducción debe estar bajo el control permanente y la responsabilidad total del conductor.

8. Sin embargo, el sistema de responsabilidad civil necesariamente deberá adaptarse para contemplar los supuestos en que no habrá -necesariamente- una persona sentada en el asiento del conductor (niveles de autonomía 4 y 5), sino terceros transportados (pasajeros, no necesariamente propietarios o guardianes del vehículo).

9. De lege ferenda: En el marco de lo anterior, resulta especialmente importante definir el factor de atribución del conductor, esto es, si el conductor del vehículo automotor automatizado responderá subjetivamente (cfr. Arts. 1749, 1721, 1724 y 1725 CCC) u objetivamente (cfr. Arts. 1757 y 1758 CCC).

10. Se plantea un eventual y especial problema de valoración de la conducta del agente con relación a la diligencia exigible en el dominio y control del vehículo, que involucra habilidades especiales y adicionales a las del control de un vehículo tradicional (como alfabetización digital, manejo de sistemas de IA, conocimiento específico del nivel de automatización del vehículo, capacidad de respuesta frente a la imprevisibilidad, etc.), que escapan al "conductor promedio".

11. De lege ferenda: Los requisitos para obtener el carnet de conducir deberán ser adaptados de acuerdo a las habilidades específicas que se requieren (y las que ya no) en los distintos niveles de automatización. Resulta aconsejable exigir que los usuarios de vehículos con sistemas de IA incorporados acrediten administrativamente que cuentan con los conocimientos mínimos indispensables en el manejo de este tipo de tecnologías.

12. De lege data: El vicio o defecto del vehículo automatizado o no resulta relevante para exonerar de responsabilidad al dueño o al guardián, pues el caso fortuito (cfr. Art. 1730, CCC) debe ser totalmente ajeno al riesgo o vicio de la cosa, por lo que traer al fabricante o al responsable de despliegue del sistema de IA involucrado no guarda sentido con la especificidad planteada por el legislador para los accidentes de circulación (art. 1769, CCC).

13. De lege data: La valoración de la negligencia o impericia en el manejo de estos sistemas de asistencia a la conducción (cfr. Art. 1724, CCC) requiere una necesaria correlación y modulación con el deber de información al consumidor que pesa sobre el proveedor de estos bienes (cfr. Art. 4 LDC, 1100 CCC y 42 CN) de suministrar en forma cierta, clara y detallada todo lo relacionado con sus características esenciales.

II. FUNDAMENTOS

1. NOCIONES ESENCIALES DE LA CONDUCCIÓN AUTOMATIZADA Y AUTÓNOMA

a) Robótica, Autonomía e Inteligencia Artificial (IA)

Lo primordial e inminente respecto al surgimiento y paulatina incorporación masiva de los vehículos automatizados es resolver qué normativa resultará aplicable en nuestro país, en el ámbito de la responsabilidad civil, a los accidentes de circulación que los involucren, pues ello incidirá tanto en la conducta de los potenciales usuarios como en materia de seguros e, incluso, control y regulación administrativa.

Para ello, debe tenerse en cuenta en primer lugar que un vehículo automatizado es un robot con inteligencia artificial, conforme las cuatro características de un robot inteligente que ha señalado la Comisión Europea: 1. capacidad de adquirir autonomía mediante sensores y/o mediante el intercambio de datos con su entorno (interconectividad) y el análisis de dichos datos; 2. capacidad de aprender a través de la experiencia y la

interacción; 3. forma del soporte físico del robot; 4 capacidad de adaptar su comportamiento y acciones al entorno[2].

De momento, alcanza con entender que la autonomía –en IA- implica dos aspectos: la capacidad de auto dirigirse y la capacidad de autosuficiencia. La primera implica la independencia de un agente de su ambiente físico o grupo social, mientras que la segunda alude a la capacidad de autogenerar metas.[3] El alcance de estas capacidades se relaciona con los distintos niveles de automatización de los vehículos.

En términos generales, puede establecerse que autónomo, según las ciencias técnicas, es un vehículo equipado con un sistema de automatización de la conducción.

Por su parte, el sistema de automatización es un sistema de IA (según la definición que propicia el Reglamento de Inteligencia Artificial aprobado por el Parlamento Europeo de la UE[4] en el art. 3.1.) "capaz" de conducir un vehículo sin la intervención de un conductor, o con una intervención mínima de aquél.

b) Distinción entre conducción automatizada, autónoma y conectada

La automatización no es necesariamente un estado binario, sino que admite una serie de grados o niveles, por lo que el vehículo podrá tener más autonomía o menos autonomía[5]: existen diferentes niveles de

---

[2] Corvalán, J. G., Danesi, C. C., & Carro, M. V. (2023). Responsabilidad civil de la inteligencia artificial. En J. G. Corvalán, *Tratado de Inteligencia Artificial y Derecho: tomo II* (2a ed., págs. 315-398). Ciudad Autónoma de Buenos Aires: La Ley. Págs. 317, 318.

[3] Corvalán, J. G., Danesi, C. C., & Carro, M. V. (2023). Responsabilidad civil de la inteligencia artificial. En J. G. Corvalán, *Tratado de Inteligencia Artificial y Derecho: tomo II* (2a ed., págs. 315-398). Ciudad Autónoma de Buenos Aires: La Ley. Pág. 319.

[4] REGLAMENTO (UE) 2024 DEL PARLAMENTO EUROPEO Y DEL CONSEJO por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), obtenido de https://data.consilium.europa.eu/doc/document/PE-24-2024-INIT/es/pdf.

[5] Zornoza Molinos, A. (Julio de 2020). Tesis doctoral: *Vehículos automatizados y Derecho. La influencia de la conducción automatizada en la responsabilidad civil*

automatización (0 a 5) y sólo los más altos son realmente autónomos, llegando a sustituir al conductor humano.

La clasificación más difundida de los niveles de automatización que se maneja actualmente, es la elaborada originariamente en el año 2014 (y modificada luego en 2016 y 2018) por la Sociedad de Ingenieros de Automoción Internacional (SAE, por su acrónimo en inglés *"Society of Automotive Engineers"*[6]) y plasmada en un documento titulado *"Recommended Practice J3016. Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles"* [7].

Los automóviles conectados son vehículos digitalizados, con conexión a Internet, sistemas avanzados de información y entretenimiento y aplicaciones que permiten a los vehículos "hablar" el uno al otro, intercambiando datos básicos de seguridad como la velocidad y posición, servicios de localización y guiado basados en las condiciones del tráfico en tiempo real y enlaces que facilitan el diagnóstico de vehículos y reparaciones a distancia.

Hay dos tipos de conectividad: (i) entre vehículos (*vehicle to vehicle* o V2V), que permite la comunicación entre ellos, sobre velocidad y dirección, o incluso alerta de la presencia de vehículos de emergencia; (ii) la conectividad vehículo a infraestructura vial (*vehicle to infrastructure o V2I*), para recibir notificaciones directamente de los semáforos u otras señales, notificaciones temporales de ubicación peligrosa.[8]

c) Conclusión: definición propuesta de vehículo automatizado

En base a las nociones que se presentan, se propone la siguiente definición de vehículo automatizado: "Un vehículo automatizado es un robot que cuenta con sistemas de IA y conectividad digital (entre vehículos y con la infraestructura vial) que permiten, con distintos grados (del 0 al 5), la

automovilística y en el seguro obligatorio de automóviles. Madrid, España: Universidad Carlos III de Madrid, pág. 37.

[6] Obtenido de su sitio web oficial, https://www.sae.org/.

[7] Disponible en: https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic.

[8] Navarro-Michel, M. (marzo de 2020). La aplicación de la normativa sobre accidentes de tráfico a los causados por vehículos automatizados y autónomos. *Cuadernos de Derecho Transnacional*, 12(1), 941-961. DOI: https://doi.org/10.20318/cdt.2020.523.

conducción del vehículo con una intervención asistida (nivel 0 a 2, inclusive), secundaria y/u ocasional del conductor humano (nivel 3) o, directamente, sin ésta (niveles 4 y 5).”

2. LA APLICACIÓN DEL RÉGIMEN DE RESPONSABILIDAD CIVIL POR ACCIDENTES DE CIRCULACIÓN DEL CÓDIGO CIVIL Y COMERCIAL A LOS DAÑOS CAUSADOS POR VEHÍCULOS AUTOMATIZADOS Y/O AUTÓNOMOS

a) Ámbito material de aplicación y definiciones legales

A pesar de que se suelen usar indistintamente todos estos términos como sinónimos, tanto del texto del Decreto Ley Nº 6582/58 como de la Ley Nacional de Tránsito N° 24.449 surge la distinción entre vehículos automotores (los que tienen motor y tracción propia o se “autopropulsan”), y los que no lo son.

En definitiva, los automóviles constituyen una subespecie de la especie llamada automotores, que a la vez integra el género denominado vehículos, que son “todos los aparatos que se mueven sobre el suelo para transportar personas o cosas.”[9]

De esta regulación se evidencia que los vehículos automatizados, en todos sus niveles, pueden ser subsumidos sin dificultad en la definición prevista en la LNT de “vehículo automotor” (art. 5, inc. x).

Las definiciones legales de la normativa específica no estatuyen a la conducción o intervención humana, en este sentido, como una condición jurídica relevante y necesaria para la clasificación, poniendo el acento únicamente en la posibilidad del vehículo de propulsarse a través de un motor. En otras palabras, la posibilidad de auto propulsarse es condición necesaria y suficiente para ser considerado “vehículo automotor” en los términos de la LNT.

Ello permite incluirlos entonces fácilmente dentro del ámbito material de aplicación de la normativa del CCC que regula la “Responsabilidad derivada de la intervención de cosas y de ciertas actividades” contemplada en la Sección 7ª del Capítulo 1 del CCC, sin necesidad de acudir a justificaciones relacionadas, por ejemplo, al “mayor

[9] Cfr. Kiper, C. (2018). *Accidentes de automotores: doctrina, jurisprudencia. Tomo I.* (1° Ed. Revisada ed.). Santa Fe, Santa Fe, Argentina: Rubinzal Culzoni. Pág. 11.

riesgo" que estos vehículos pueden importar de momento para la circulación en la vía pública.

Los vehículos automotores "tradicionales" ya son considerados cosas riesgosas ex lege, con lo cual la inclusión de los vehículos automatizados o autónomos dentro de esta categoría hace que los accidentes que con o por ellos se provoquen se subsuman en la regla dispuesta por el art. 1769 CCC.

De todas formas, resulta aconsejable, distinguir desde el aspecto regulatorio, entre la noción "tradicional" de vehículo automóvil y vehículo automatizado o autónomo, conforme los niveles de automatización aceptados internacionalmente.

En este sentido, una modificación como la prevista en el proyecto originario de Ley Ómnibus[10], que pretendía incluir en la LNT a los vehículos "autodirigidos" como un supuesto especial de vehículo en el art. 5 (art. 627 del Proyecto de Ley), no resulta del todo clara en cuanto a su extensión, pues refería a "todo vehículo automotor que cuenta con un sistema de conducción que no necesita de la intervención humana."

Sin perjuicio de que tal vaguedad no afecta a la extensión material de la LNT y el CCC a los restantes vehículos automatizados, la inclusión de una distinción de los grados de automatización con referencia a estándares internacionales como el de la SAE sí resulta deseable, en términos de técnica legislativa, a los efectos de la autorización del software que permite la asistencia al conductor, que ya desde el Nivel 3 (automatización condicionada) pueden dirigir el vehículo sin que la persona accione los pedales, el freno o el volante.

Este salto cualitativo amerita para los vehículos de este nivel en adelante una mayor y/o más meticulosa autorización, reglamentación, y consecuente control, sea en la propia LNT o en la reglamentación que se dicte en consecuencia, tanto del software que utilizan como de las condiciones en que se introducen al tráfico, como se está haciendo en el resto del mundo.

---

[10] MEN-2023-7-APN-PTE, del 27/12/2023, disponible para su visualización completa en sitio web oficial de la Honorable Cámara de Diputados de la Nación, https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2023/PDF2023/TP2023/0025-PE-2023.pdf.

3. FACTOR DE ATRIBUCIÓN O IMPUTACIÓN DEL RÉGIMEN DE RESPONSABILIDAD CIVIL POR EL HECHO DE LAS COSAS Y ACTIVIDADES RIESGOSAS

a) Principio de imputabilidad objetiva a título de riesgo creado

La consagración de una responsabilidad de tipo objetiva (cfr. Arts. 1757 y 1722, CCC) y concurrente tanto para el propietario del vehículo como para quien resulta su guardián (cfr. Art. 1758 CCC), asociada al riesgo creado por tener, utilizar o servirse de la cosa riesgosa, y la presunción de causalidad que a ella se asocia (cfr. Art. 1736, CCC), permitirá condenar sin problemas a los titulares registrales y/o guardianes de automóviles automatizados o autónomos.

b) Legitimados pasivos

El propietario (sea una persona física o jurídica, sea con fines particulares o comerciales) será el responsable civil por excelencia en estos casos, a título de riesgo, sin importar su intervención material o la autorización administrativa para el uso de la cosa o la realización de la actividad (cfr. Art. 1757, segundo párrafo, CCC).

La noción de guardián se ve, en cambio, complejizada y ampliada en cuanto a la casuística que se puede presentar en los supuestos de vehículos automatizados.

Si guardián es, alternativamente, "quien ejerce, por sí o por terceros, el uso, la dirección y el control de la cosa, o quien obtiene un provecho de ella" (art. 1758, CCC), cabe preguntarse si proveedores de los sistemas de IA involucrados –indirectamente- en la dirección y el control de los vehículos automatizados pueden ser considerados guardianes y, por tanto, responsables objetivamente de los accidentes de circulación que se ocasionen con o por los vehículos automatizados.

La respuesta negativa se impone. La ley debe ser interpretada no solo de acuerdo a su literalidad, sino también atendiendo a su finalidad, en forma coherente con el resto del ordenamiento (cfr. Art. 2, CCC). En consecuencia, dado que en nuestro sistema legal la actividad de aquellos que participan en el diseño, fabricación o implementación de los sistemas de IA, en tanto productos, ya tienen cabida en el marco del derecho de consumo, debe descartarse cualquier solución que pretenda transformar los accidentes de tránsito dónde interviene un vehículo autónomo en supuestos de

responsabilidad por productos defectuosos (cfr. Art. 40, Ley N° 24240, en adelante, LDC), incluso cuando su causación –en un sentido eficiente- se corresponda directamente con una respuesta de la máquina a un entorno vial determinado.

Lo propio puede decirse respecto a la posibilidad de atribuir responsabilidad al fabricante por el vicio o defecto del producto en el marco de un accidente de tránsito.

Estas soluciones no solo que complejizarían y elevarían los costos de los litigios por accidentes de tránsito para probar el defecto de fabricación, diseño o información del producto, sino que incrementaría altamente los costos de transacción implicados. Además, hacen sentido únicamente en el marco de regímenes que no consagran una responsabilidad de tipo objetiva para los legitimados pasivos en juicios de accidente de tránsito.

Debe tenerse presente, especialmente, que el vicio o defecto del vehículo –automatizado o no- no resulta relevante para exonerar de responsabilidad al dueño o al guardián, pues el caso fortuito (cfr. Art. 1730, CCC) debe ser totalmente ajeno al riesgo o vicio de la cosa, por lo que traer al fabricante o al responsable de despliegue del sistema de IA involucrado no guarda sentido con la especificidad planteada por el legislador para los accidentes de circulación (art. 1769, CCC).

Ello, sin perjuicio de las acciones que pudiera intentar el titular registral –si puede considerárselo, según el caso, consumidor- en contra del "productor, el fabricante, el importador, el distribuidor, el proveedor, el vendedor y quien haya puesto su marca en la cosa o servicio" (art. 40, LDC) por los daños que le haya ocasionado el vicio o defecto de la cosa.

Por otro lado, puede plantearse un problema –en rigor, no novedoso- dado que todavía no hay un criterio uniforme con relación a si se considera al conductor "guardián" de los vehículos "tradicionales" (cfr. Art. 1758, CCC), sobre todo en los casos en que el conductor no es el propietario del vehículo y no obtiene un provecho de éste (como el caso de los choferes).

En Argentina, reputada doctrina y jurisprudencia sostiene que en el sistema de responsabilidad civil vigente puede mediar acumulación de factores de atribución de responsabilidad objetiva y subjetiva, en tanto pueden concurrir la responsabilidad subjetiva del autor material del daño (como el conductor del automotor) junto a la responsabilidad objetiva por el riego de la cosa del dueño y/o el guardián del automóvil, o de quien se sirve,

obtiene provecho o realiza la actividad riesgosa (como la actividad organizada para la prestación del servicio de remis)[11].

c) Problemas de atribución de responsabilidad según niveles de automatización

En los vehículos automatizados nivel 0 a 2 inclusive (con sistemas de asistencia a la conducción), la aplicación del régimen de responsabilidad civil no presenta grandes matices respecto al vehículo "clásico", pues la conducción debe estar bajo el control permanente y la responsabilidad total del conductor.

El salto cualitativo más importante se produce entre el nivel 2, en que el conductor humano realiza algunas de las funciones dinámicas de conducción, y el nivel 3, en el que el vehículo realiza todas esas funciones. El papel del conductor se torna más pasivo, pasa a ser un conductor "de reserva" y puede llegar a desaparecer para convertirse en un pasajero en los siguientes niveles[12].

En los casos de autonomía y autonomía plena, la conducción no necesita ya control permanente del usuario. En el nivel 4, el sistema realiza todas las tareas de la conducción en entornos controlados y determinados, aunque el sistema puede requerir la atención del conductor en cualquier momento. Lo relevante es que el funcionamiento del vehículo no está necesariamente condicionado a que el conductor responda, de modo que es capaz de detenerse de un modo seguro si el conductor no atiende a la llamada de atención. Esto incluye a los llamados "taxis sin conductor" y a vehículos que, por ejemplo, pueden no traer pedales o volante.

En el nivel 5, el sistema realiza todas las tareas de la conducción en cualquier terreno, bajo cualquier circunstancia y sin ningún tipo de limitación.

---

[11] Galdós, J. M. (2019). La responsabilidad por riesgo y vicio de las cosas en el Código Civil y Comercial. El art. 1757 y los principios generales. En S. Picasso, & L. R. Sáenz, *Tratado de Derecho de Daños* (Vol. III, págs. 117-150). Ciudad Autónoma de Buenos Aires: La Ley, pág. 147.

[12] Navarro-Michel, M. (Marzo de 2020). La aplicación de la normativa sobre accidentes de tráfico a los causados por vehículos automatizados y autónomos. *Cuadernos de Derecho Transnacional,* 12(1), 941-961. DOI: https://doi.org/10.20318/cdt.2020.5231, pág. 947.

En consecuencia, el sistema de responsabilidad civil necesariamente deberá adaptarse para contemplar estos supuestos en que no habrá -necesariamente- una persona sentada en el asiento del conductor (niveles de autonomía 4 y 5), sino terceros transportados (pasajeros, o el mismo propietario del vehículo). En estos casos la noción de culpa se verá sumamente complejizada, cuanto no eliminada, si el conductor no es el que toma las "decisiones" sino el vehículo, lo que plantea un problema tanto de falta de agencia como de intervención causal del conductor en el accidente.

d) Valoración de la conducta del conductor y habilitación administrativa para conducir

Si la responsabilidad del conductor es subjetiva (cfr. Arts. 1749, 1721, 1724 y 1725 CCC), se plantea un eventual y especial problema de valoración de la conducta del agente: ¿debe exigirse una mayor diligencia, o calificada, al conductor de un vehículo automatizado?

Las pautas actuales de valoración imponen que no debe tomarse en cuenta las condiciones intelectuales y personales de una persona determinada, de forma que la avanzada edad, las deficiencias físicas, intelectuales o cognitivas (siempre que se trate de personas con discernimiento), no tienen influencia alguna en la obligación de resarcir .

Sin embargo, la conducción automatizada requiere ciertas capacidades para enfrentar los avatares de la conducción automatizada (como alfabetización digital, manejo de sistemas de IA, conocimiento específico del nivel de automatización del vehículo, capacidad de respuesta frente a la imprevisibilidad, etc.), que escapan al "conductor promedio".

Ello resulta especialmente relevante en el caso de los vehículos con nivel 3 de automatización, en los que el sistema puede realizar todas las tareas de la conducción, pero siempre en entornos controlados y bajo la expectativa de que el conductor asumirá el control rápidamente cuando se le requiera para ello. Estos vehículos –que son los que más cerca se encuentran de ser introducidos en forma masiva al mercado- incluyen, por ejemplo, sistemas "traffic jam chauffer", una extensión del control de velocidad de crucero que monitorea la velocidad de vehículos circundantes –hasta 60 km/h- y acelera y frena en consecuencia.

En el vehículo autónomo, la ciencia todavía no ha logrado consagrar una previsibilidad cierta ante la complejidad del tránsito. Cuanta más autonomía tenga, mayor será la toma de decisiones, mayor será la

incertidumbre e imprevisibilidad. Los humanos ya no seremos conductores sino usuarios, por lo que para usar un vehículo ya no se debe necesariamente saber conducir, o tener licencia habilitante o no haber consumido alcohol o estupefacientes.

La única opción posible para evitar la proliferación de resoluciones judiciales contradictorias y tratos desiguales ante la ley es la aclaración legislativa del factor de atribución que corresponde al conductor de los vehículos, sea igual para todos, sea distinguiendo entre vehículos tradicionales y autónomos.

e) La autorización administrativa para conducir

Un problema similar se plantea respecto de las personas que no podrían conducir vehículos tradicionales, pero sí dirigir vehículos autónomos, como el caso de las personas con discapacidades motrices.

La solución aquí pasa más por la regulación administrativa de los requisitos para obtener el carnet de conducir, que deberán ser adaptados de acuerdo a las habilidades específicas que se requieren (y las que ya no) en los distintos niveles de automatización.

Actualmente, la LNT exige para obtener la licencia de conducir –aparte de la aprobación de un examen práctico de conducción- un examen médico psicofísico de aptitud física, visual, auditiva y psíquica, y que los conductores sepan leer y, si son profesionales, también escribir. Asimismo, se requiere aprobar un examen teórico de conocimientos sobre conducción, señalamiento y legislación, estadísticas sobre accidentes y modo de prevenirlos.

Siguiendo la tendencia europea, resulta aconsejable exigir ab initio que los usuarios de vehículos con sistemas de IA incorporados acrediten administrativamente que cuentan con los conocimientos mínimos indispensables en el manejo de este tipo de tecnologías.

4. RELACIÓN DE CAUSALIDAD

a) Hecho o culpa del damnificado

Con relación a la valoración de la incidencia causal (cfr. Arts. 1729 y 1726, CCC) de la conducta del damnificado (en el caso, conductor de un vehículo automatizado que resulta reclamante o reconviniente en un juicio

de responsabilidad civil), se plantea el mismo problema de valoración de la conducta exigible al agente.

En particular, cuando se demuestre la incidencia causal parcial o total de la conducta desplegada u omitida por el conductor, que por falta o inadecuada educación tecnológica, no pudo intervenir adecuadamente en la conducción del vehículo automatizado (por ejemplo, no reasumiendo la conducción cuando el vehículo se lo requería, o "confiando" demasiado en las capacidades del vehículo), o no pudo prever, anticipar o impedir la "decisión" que el vehículo tomó, reasumiendo el mando del rodado a tiempo.

La valoración de la negligencia o impericia en el manejo de estos sistemas de asistencia a la conducción (cfr. Art. 1724, CCC) requiere una necesaria correlación y modulación con el deber de información al consumidor que pesa sobre el proveedor de estos bienes (cfr. Art. 4 LDC, 1100 CCC y 42 CN) de suministrar en forma cierta, clara y detallada todo lo relacionado con sus características esenciales. En esto, resulta vital que no se generen expectativas irrazonables respecto a la capacidad y limitaciones en particular de cada vehículo.

Ello también resultaría consecuente con la mayor expectativa de seguridad en cuanto bienes de consumo (cfr. Art. 5, LDC) que se tiene respecto de los vehículos automatizados y la especial confianza que inspira en los usuarios la promesa del vehículo autónomo.

Por otro lado, es cierto que estos vehículos auguran una mayor seguridad y eficiencia en el transporte y, en última instancia, más previsibilidad que los humanos en cuanto conductores (intérpretes y aplicadores de las normas de tránsito y señalización), pero la imprevisibilidad surge precisamente de la complejidad de los algoritmos y de su combinación con la experiencia adquirida; y que precisamente la mejor "decisión" según la diligencia debida de la persona razonable (cfr. Art. 1725, CCC) puede no coincidir con la respuesta matemática.

Resulta conveniente, como propugna el Reglamento de IA (v. Considerando 72), que se exija transparencia a los distintos proveedores y responsables del despliegue de los sistemas de IA involucrados en la conducción de vehículos automatizados, a cumplir sus obligaciones en virtud del presente Reglamento antes de su introducción en el mercado o su puesta en servicio.

Máxime considerando que, en principio, aunque la negligencia se deba a una falta de información adecuada, si el factor de atribución del conductor es objetivo, no será causal de eximición.

APROXIMACIONES Y PROPUESTAS PARA UN TRATAMIENTO HUMANISTA DE LOS DAÑOS DERIVADOS DE LA INTELIGENCIA ARTIFICIAL EN EL DERECHO CIVIL ARGENTINO

Por Daniel J. Bonino[1]

I. CONCLUSIONES

1. De lege lata: La responsabilidad civil derivada de los sistemas de inteligencia artificial (I.A.) debe ser abordada por los operadores jurídicos desde una perspectiva constitucional y convencional (arts. 19, 42, 75 inc. 22 CN art. 1 C.C.C.), teniendo como eje la persona humana (garantía de humanidad), jerarquizando el rol de los principios y el dialogo de fuentes a fin de adoptar soluciones circunstanciadas y equitativas frente al fenómeno resarcitorio tecnológico;

2. La función preventiva de la responsabilidad civil, regulada en los arts. 1710 y ss. del CCC, es un instituto idóneo y eficaz para evitar, hacer cesar o disminuir los daños derivados de la inteligencia artificial;

3. En el marco del deber de prevención y buena fe, resulta imperativo para los proveedores, fabricantes de productos y servicios informar, clara y oportunamente, acerca de la utilización de sistemas de inteligencia artificial en las relaciones jurídicas que se entablan en entornos digitales o analógicos;

4. En el Código Civil y Comercial Argentino, los sistemas de inteligencia artificial, que incluyen robots y algoritmos, están comprendidos en el concepto normativo de cosa (art. 16 CCC) y actividad (Art. 257 CCC), es decir como objeto de derechos, descartando su calificación jurídica como sujetos o centro de imputación de derechos y obligaciones;

5. Ante la ausencia de una regulación específica, los daños derivados de la inteligencia artificial (simples o complejas), por su intrínseca potencialidad dañosa, deben ser resueltos bajo las reglas y

---

[1] Miembro titular. Profesor Asociado de Derecho Privado II (Obligaciones), de la Carrera de Abogacía, de la Facultad de Ciencias Humanas de la Universidad Nacional de Río Cuarto. Maestrando de Derecho Civil en la Facultad de Derecho de la Universidad Austral.

principios de la responsabilidad por actividades y cosas riesgosas (arts. 1757 y 1758, Cód. Civ. y Com.), siendo de aplicación el factor objetivo;

6. Resulta aplicable a los vehículos autónomos el régimen de responsabilidad previsto por el art.1757, 1758 y 1769 del Cód. Civ. y Com. Argentino;

7. El titular registral (dueño) y el sujeto que tenga a su cargo el mantenimiento del sistema inteligente (guardián), responderán en forma concurrente por los daños que ocasione el vehículo autónomo;

8. Los daños derivados de los sistemas de I.A., quedan alcanzados por la norma del art. 40 de la Ley 24240, aplicable al proveedor y a todos los que intervienen en el proceso de su comercialización, que incluye las plataformas, frente al consumidor en entornos digitales;

9. Los daños producidos por profesionales por uso de sistemas de I.A. deben ser analizados bajo las pautas de la responsabilidad objetiva, cuando aquellos derivan de los vicios, sesgos u opacidades de la IA o sistemas algorítmicos, en función de lo establecido por la norma del art. 1768, 2 parr. CCCN;

10. Son de aplicación a los daños derivados de la I.A. las prescripciones de la responsabilidad colectiva y anónima de los arts. 1761 y 1762 CCC;

11. En los procesos de daños (preventivos o resarcitorios) derivados de la inteligencia artificial resulta aplicable la doctrina de las cargas probatorias dinámicas, imponiendo el peso de la prueba a los proveedores, titulares, creadores o guardianes de los sistemas por encontrarse tecnológicamente en mejores condiciones de acercar prueba a la causa, sin importar si es actor o demandado.

12. De lege ferenda: Resulta necesario ajustar la legislación de fondo a los nuevos desafíos que plantea la realidad tecnológica I.A., sobre la base un sistema de principios y valores que permitan adoptar soluciones versátiles que tengan como eje la persona humana, la tutela de sus derechos personalísimos (art. 51 y 52 CCN), y se adapten a los vertiginosos y permanentes cambios producidos por la robótica y los sistemas inteligentes generativos;

13. Las reformas legislativas deberán observar las reglas y directivas éticas provenientes del derecho internacional (soft law), poniendo el acento en la función preventiva y precautoria de la responsabilidad civil, en orden a una adecuada gestión de los riesgos

derivados de la IA, con la finalidad de evitar, hacer cesar o disminuir los daños a los derechos fundamentales de las personas;

14. En orden a un manejo responsable de los sistemas inteligentes y algorítmicos se propicia una legislación diseñada a partir de un enfoque integrado y multidisciplinario que combine conocimientos especializados, transparencia, supervisión humana, cumplimiento normativo y protección de la privacidad, procurando promover los beneficios de la tecnología y minimizar los riesgos;

15. Promover la creación legal de un registro público de sistemas de inteligencia artificial, simples y complejos, que permitan a las personas tener conocimiento de las titularidades como las mutaciones reales pertinentes.

16. En el marco de la función resarcitoria, establecer pautas y reglas específicas para discernir los presupuestos de la responsabilidad de los sistemas de I.A., especialmente en lo que atañe la relación causal, autoría, factor de atribución, eximentes extensión del resarcimiento, contemplando mecanismos sustitutivos, como seguros obligatorios que aseguren a las víctimas una adecuada y eficaz reparación del daño injusto.

17. Prever la incorporación de una función sancionatoria, contemplando sanciones punitivas para disuadir la utilización o comercialización de sistemas inteligentes artificiales sesgados que, mediante discriminaciones injustas afecten los derechos, la dignidad como la privacidad de las personas.

RESPONSABILIDAD CIVIL EN EL USO DE DATOS PERSONALES POR LA IA

Manuel Gonzalo Burgueño Ibarguren[1]

I. CONCLUSIONES

1. La normativa argentina de protección de datos es aplicable a la IA y, si bien permite la operatoria de estas, también asigna derechos a los titulares de los datos.

2. Los proveedores y quienes despliegan una IA deben asumir una actividad preventiva de daños en el uso de los datos personales, conforme el art. 1710 del CCC.

3. Se garantiza al titular de los datos, como formas de prevención de daños: el acceso, rectificación y eliminación de datos, lo que debe hacerse de forma diligente y por un simple reclamo online. Son viables las acciones de habeas data y acción preventiva de daños, si existe previsibilidad o actualidad de algún perjuicio causado por una conducta antijurídica.

4. Es posible la responsabilidad civil en casos de violación de la seguridad o confidencialidad de los datos. Estos deberes son de resultado y la responsabilidad objetiva. Estimamos que la opacidad de la IA y el riesgo de la actividad debe permitir una amplia legitimación pasiva por aplicación del art. 1757 del CCC y art. 40 LDC, si hay relación de consumo.

5. También puede haber responsabilidad resarcitoria cuando la IA es directamente dañosa o de alto riesgo según el destino para el que fue creada, ampliando la responsabilidad a todo el grupo de personas físicas y jurídicas que desarrollan una actividad peligrosa de grupo, siendo un supuesto de responsabilidad colectiva.

---

[1] Lic. en administración (IESE). Abogado (UNPSJB). Magíster en derecho privado (UNR), Master en Economía y derecho del consumo online (Univ. de Castilla y la Mancha). Especialista en derechos de daños (UBA). Especialista en derecho de daños (UNL). Cursante en Universidad de Salamanca, Universidad de París II Panthéon Assas, Universidad Complutense de Madrid. Doctorando (UNR). Profesor de derecho de las obligaciones (JTP) y de derecho digital (a cargo de la cátedra) en la Facultad de Derecho de la Universidad Nacional de la Patagonia (Comodoro Rivadavia).

6. Puede existir relación de consumo por el uso de IA y proceder la aplicación de daños punitivos si se configuran sus requisitos.

II. FUNDAMENTOS

1. INTRODUCCIÓN

El derecho de daños, con sus múltiples funciones, debe regular a las consecuencias dañosas del el uso antijurídico de datos personales por parte de los operadores de IA[2], conforme el marco jurídico de protección establecido en el art. 43 de la Constitución Nacional, el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, el Protocolo Adicional al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las autoridades de control y a los flujos transfronterizos de datos[3], Protocolo Modificatorio del Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal[4], la Ley 25.326 y Resolución 161/2023 de la Agencia de Acceso a la Información Pública.

2. PROBLEMA FÁCTICO

El auge y desarrollo moderno de la inteligencia artificial se debe al uso de algoritmos y sobre todo de datos. Es más, el enfoque de la inteligencia artificial basado en datos y la enorme disponibilidad de datos son responsables del apogeo de la IA de aprendizaje automático (*machine learning*)[5]. Por ello, la accesibilidad, pertinencia y calidad de los datos es

---

[2] Proveedor (quien introduce un sistema o modelo de IA en el mercado), fabricante del producto (quien crea cosas que funcionan con IA), responsable del despliegue (un usuario de IA bajo propia autoridad, como la administración pública o una empresa salvo uso personal y no profesional), representante autorizado, importador o distribuidor de IA. Art. 3º, Reglamento de Inteligencia Artificial del Parlamento Europeo y del Consejo, 13 de marzo de 2024.

[3] Aprobado por ley 27483 del 02/01/19.

[4] Aprobado por la ley 27699 del 30/11/2022.

[5] Boucher, Philip Boucher; Artificial intelligence:How does it work, why does it matter, and what can we do about it?, European Parliamentary Research Service,

fundamental para la creación, entrenamiento, aprendizaje, prueba, mejora y evolución de la IA[6]; porque funciona en base al procesamiento de datos, a través de redes neuronales artificiales, que permite imitar algunas facultades humanas, analizar el entorno, tomar acciones con autonomía para cumplir objetivos[7]. Por ello, a los fines del desarrollo de la IA se debe garantizar el acceso igualitario a conjuntos de datos de alta calidad y su transferencia entre empresas y con el estado[8].

No obstante la importancia que tienen los datos en general para los sistemas y modelos de IA, puede haber un conflicto de intereses cuando se trata de datos personales y la captación, registro, gestión y procesamiento, a los fines del uso, es desconocido por las personas que podrían ser afectadas en sus derechos a la imagen, intimidad, vida privada y familiar y confidencialidad de las comunicaciones[9].

En efecto, el uso de los datos es tan central en la IA como el de los algoritmos y, especialmente, debe tenerse en cuenta los conceptos de *big data* y *data mining*, que ponen de manifiesto la existencia de ingentes cantidades de datos reunidos de fuentes muy diversas y que son procesados de forma automática, para encontrar patrones, errores y detectar los datos útiles -que muchas veces son producidos y otorgados para otra finalidad y, al permanecer accesibles, son recopilados y empleados para la IA (*data in*

---

https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf.

[6] "Es preciso instaurar prácticas adecuadas de gestión y gobernanza de datos para lograr que los conjuntos de datos para el entrenamiento, la validación y la prueba sean de alta calidad. Los conjuntos de datos para el entrenamiento, la validación y la prueba, incluidas las etiquetas, deben ser pertinentes, lo suficientemente representativos y, en la mayor medida posible, estar libres de errores y ser completos en vista de la finalidad prevista del sistema". Considerando (67), Reglamento de Inteligencia Artificial del Parlamento Europeo y del Consejo, 13 de marzo de 2024.

[7] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels, 25.4.2018, COM(2018) 237 final.

[8] Considerando (68), Reglamento de Inteligencia Artificial del Parlamento Europeo y del Consejo, 13 de marzo de 2024.

[9] Sin perjuicio de los derechos de propiedad intelectual que pueden ser conculcados en el uso de algoritmos, modelos, datos y software preexistentes, que no correspondan a licencia libre y código abierto, y mediante el entrenamiento con datos de sonido, imagen, texto, video etc. protegidos por derechos de autor.

the wild)-. Además, debe tenerse presente que los usuarios de IA también proporcionan datos cada vez que le dan indicaciones o pedidos (*prompts).*

Justamente, dentro del universo de datos, importan en este trabajo los datos personales extraídos sin expreso consentimiento ni imperativo legal que habilite el uso por parte de la IA. En ese conjunto de datos es donde puede existir el conflicto de intereses y es donde la acción de *habeas data* y las funciones de la responsabilidad civil deben actuar con su milenaria experiencia para resolver el conflicto e imponer obligaciones concretas para prevenir daños, indemnizar perjuicios o punir hechos socialmente reprochables[10].

Efectivamente, no se trata de un problema hipotético o exclusivamente ético[11]; puesto que el tema ha dado lugar a litigios ante la Corte del Distrito Norte del Estado de California, donde ya se han presentado cuatro acciones de clase contra las principales empresas informáticas del mundo: tres contra OpenAi y Microsoft -una desistida por los actores el 15 de septiembre de 2023, otra rechazada por el tribunal con posibilidad de enmendar la demanda el 23 de mayo de 2024 y la última se desistió por la

[10] Por otro lado, las respuestas que brinda la IA en base a los datos recabados pueden entrañar algún sesgo discriminatorio, que podría dar lugar a responsabilidad civil, pero estimamos que es otro tipo de problema jurídico vinculado a los conjuntos de datos que se emplean en la IA.

[11] Desde la perspectiva de la Ética, se proponen requisitos para la confiabilidad de los sistemas de IA. En cuanto a la problemática del uso de datos, se considera que corresponde una adecuada gestión de datos para prevenir daños a la privacidad, garantizar la protección de la intimidad y de los datos a lo largo de todo el ciclo de vida de un sistema, garantizar la calidad e integridad de datos y regular el acceso a los datos personales mediante protocolos que tiendan a garantizar la confidencialidad. Grupo de expertos de alto nivel sobre inteligencia artificial, Directrices éticas para una IA fiable, junio de 2018, https://digital-strategy.ec.europa.eu/es/library/ethics-guidelines-trustworthy-ai

parte demandante el 30 de mayo de 2024-[12] y la restante contra Google[13] que continúa activa[14].

Básicamente, se atribuye a las empresas creadoras de IA haber extraído datos personales de sitios web en internet (*web scraping*), sin conocimiento ni consentimiento directo de las personas que los proporcionan, para incorporarlos a sus productos. La metodología de rastrillaje de datos se habría realizado en secreto, sin previo aviso al público y sin darle la opción de no participar a los individuos y sin registrarse como corredor de datos conforme las leyes de California y Vermont. Por ello, se imputa la realización de una actividad ilegítima que, a la postre, proporciona ganancias comerciales.

Otro caso que demuestra la tangibilidad del conflicto de intereses, radica en el uso de miles de fotografías obtenidas de perfiles de webs de citas para entrenar y probar diversas II.AA, que puede determinar la sexualidad de esas personas con mayor grado de eficacia que los humanos[15]. Esto desde ya, además de representar una amenaza a la privacidad y un medio de runión de datos sensibles, en algunos países puede instar la persecución criminal por estar la homosexualidad penada.

---

[12]https://clarksonlawfirm.com/wp-content/uploads/2023/06/0001.-2023.06.28-OpenAI-Complaint.pdf.

https://fingfx.thomsonreuters.com/gfx/legaldocs/xmpjlnldzpr/OPENAI%20PRIVACY%20LAWSUIT%20complaint.pdf

https://fingfx.thomsonreuters.com/gfx/legaldocs/zgvonmynbpd/OPENAI%20PRIVACY%20LAWSUIT%20dismissal.pdf

https://s3.amazonaws.com/jnswire/jns-media/8e/6d/15489761/NORCAL_AS_v_OpenAI.pdf

https://www.pacermonitor.com/public/case/52505332/AS_v_OpenAI_LP_et_al

[13]https://fingfx.thomsonreuters.com/gfx/legaldocs/xmpjlnldzpr/OPENAI%20PRIVACY%20LAWSUIT%20complaint.pdf

[14] https://www.courtlistener.com/docket/67599029/l-v-alphabet-inc/

[15] Leuner, Jhon; A Replication Study: Machine Learning Models Are Capable of Predicting Sexual Orientation From Facial Images, University of Pretoria, 2018, https://arxiv.org/pdf/1902.10739

En suma, por la existencia de conflictos reales en materia de datos empleados por IA[16], corresponde reflexionar qué puede hacerse en nuestro país con la normativa vigente y que se debería hacer para proteger a las personas sin obstaculizar el desarrollo de la IA que puede traer ventajas para la humanidad e inversiones para Argentina.

3. MARCO JURÍDICO ARGENTINO SOBRE DATOS PERSONALES

El primer dilema jurídico que se debe resolver es si resulta aplicable el régimen argentino de protección de datos, organizado en base a los registros creados para dar informes de datos; lo que no se ajusta a la realidad de la IA, que se sirve del *big data* y realiza un rastrillaje en la red, puede no obtener datos de forma directa del público en la etapa de creación, entrenamiento y prueba y, por supuesto, no opera como un registro creado para proporcionar informes de datos personales y tampoco como un motor de búsqueda en internet, que favorece el hallazgo de información que sí puede contener datos personales o dar publicidad a datos que significan el menoscabo de derechos de la persona titular.

Al respecto, estimados que los derechos constitucionales en juego, como el honor, la confidencialidad y la intimidad hacen analogicamente aplicable la normativa de protección de datos, a todo tipo de tecnologías, por el principio de neutralidad tecnológica[17], incluida la IA.

Entonces, entendiendo que sí es aplicable la normativa de protección de datos, se puede afirmar que, en general, sí es factible jurídicamente la obtención y tratamiento de datos personales por un sujeto que crea una IA y el acceso y uso de los datos es legítimo en nuestro país, si los datos son ciertos, pertinentes, precisos, proporcionados, adecuados, actualizados y no excesivos en relación con un ámbito o fin legítimo (expreso y específico)

---

[16] Gal, Uri; ChatGPT is a data privacy nightmare. If you've ever posted online, you ought to be concerned, 8/2/23, https://theconversation.com/chatgpt-is-a-data-privacy-nightmare-if-youve-ever-posted-online-you-ought-to-be-concerned-199283

[17] Según el art. 5 de la Propuesta de Anteproyecto de Ley de Datos Personales, en virtud del principio de neutralidad tecnológica, las normas de protección de datos se "aplican a cualquier tratamiento de datos personales, con independencia de las técnicas, procesos o tecnologías –actuales o futuras- que se utilicen para dicho efecto". https://www.argentina.gob.ar/sites/default/files/2022/09/propuesta_de_anteproyecto_de_ley_vf.pdf

para el que se hubieran obtenido, y si se desarrolla el tratamiento de forma justa, transparente[18] y considerando todos los intereses en juego.

Por otro lado, no siempre se debe contar con consentimiento informado del titular de los datos o con habilitación legal para recabarlos: como ocurre con los datos alojados en fuentes públicas e irrestrictas, los que se obtienen para ejercicio de funciones públicas o en cumplimiento de deberes legales y los datos inherentes a relaciones contractuales, científicas o profesionales del titular de los datos; así como la información financiera e información básica de la persona[19]. El tratamiento de datos genéticos, penales y penitenciarios, biométricos y datos sensibles (sobre raza, etnia, opinión política, gremial, religión, vida sexual y salud) sí es posible, con finalidades estadísticas o científicas; cuando no puedan ser identificados sus titulares y si la ley establece las salvaguardas adecuadas y brinda protección y seguridad al titular de los datos contra los riesgos propios de la actividad (acceso no autorizado a los datos, destrucción, pérdida, uso por terceros, modificación y divulgación); riesgos que deben ser previstos, prevenidos y minimizados[20].

Además, se admite la transferencia transfronteriza de datos con los países con los que existen convenios, lo que inhibe la posibilidad de prohibir y de exigir autorización previa, y también con otros países que garanticen estándares similares de protección y de procedimientos.

En todo caso, se debe garantizar al titular de los datos seguridad y confidencialidad[21], el acceso y confirmación del empleo de datos personales, información sobre el origen y tiempo de conservación. Además, se debe

---

[18] La transparencia requiere de información sobre el encargado de tratamiento de los datos (identidad y domicilio), los fundamentos legales y finalidad del tratamiento de datos, categorías de datos usados, destinatarios de los datos personales y formas de ejercer derechos del titular de los datos. Art. 8.1 del Convenio 108+, Ley Ley 27699. En los incs. 2 y 3 del art. 8 se establecen las excepciones a ese deber de informar, cuando ya se lo haya hecho previamente y el titular de los datos cuente con la información, cuando no se haya recabado los datos de los titulares, el tratamiento fuese establecido por ley, hubiese imposibilidad o esfuerzos desmedidos, aspectos aplicables a los proveedores y responsables de despliegue de IA. También se establecen deberes de información para quien recaba los datos del titular, conforme el art. 6 de la ley 25.326.

[19] Art. 5 de la ley 25.326

[20] Arts. 5, 6, 8 y 10 del Convenio según texto modificatorio aprobado por ley 27.699.

[21] Arts. 8 y 9 de la ley 25.326.

garantizar la rectificación de los datos sin costos y la eliminación si se incumplen las normativas legales. El titular de los datos puede expresar oposición fundada al tratamiento de datos que lo involucran, pero el titular del tratamiento puede utilizarlos si demuestra la existencia de fundamentos legítimos superiores al interés del reclamante[22].

En conclusión, se puede emplear, bajo la ley argentina, datos personales en el entrenamiento y prueba de la IA, si hay consentimiento del titular o habilitación legal (por ejemplo cuando hay interés científico), incluso si son datos sensibles, si existe una finalidad que lo justifique y son medios racionales para su alcance, cuentan con fundamentos legítimos y proceden con confiabilidad y seguridad al tratamiento de los datos. El ejercicio regular de estos derechos no da lugar a responsabilidad civil, siendo primordial la finalidad perseguida por el sistema de IA que se utilice, la utilidad social y el servicio que esté destinado a prestar, sin importar si hay o no fin de lucro, aspecto que no es de interés en el marco de la protección de datos.

No obstante, la utilización ilegítima de datos personales a espalda de la legislación, el desconocimiento de los derechos de acceso, rectificación y supresión, o la violación de los deberes de seguridad y de confidencialidad pueden significar la antijuridicidad a los fines de las tres funciones de la responsabilidad civil, lo que tiene que ser puesto en valor dentro de los demás componentes del sistema de responsbilidad.

4. APLICACIÓN DE LAS REGLAS DE LA RESPONSABILIDAD CIVIL A LA IA POR USO DE DATOS

Es importante destacar que la IA es, por así decirlo, un circuito cerrado, que pone a disposición del usuario un algoritmo y todos sus datos para dar una respuesta a un problema. Pero, sacando los problemas vigentes en materia de *copyright,* no proporciona ni publica datos personales, ni siquiera son los mecanismos más eficaces para proporcionar información exacta y se sirve de datos que ya han sido proporcionados por el titular, no los obtiene de él de forma directa en la etapa de entrenamiento y prueba -

[22] Por ejemplo, seguridad; defensa nacional; intereses económicos y financieros del estado; proteger la imparcialidad e independencia del Poder Judicial; prevención, investigación y procesamiento de delitos; intereses científicos o históricos; propósitos estadísticos y archivo en interés general. Art. 11 del Convenio según texto modificatorio aprobado por ley 27.699.

aunque sí podría hacerlo conforme a nuestro derecho, en algún caso-. Por ello, su actuación difiere de aquella que corresponde a otras herramientas que ya han sido abordadas en nuestra jurisprudencia, como los registros de datos y motores de búsqueda, circunstancia que perduran hasta la etapa de puesta en servicio y uso de la IA, aunque en esta etapa sí puede obtenerse datos personales de los usuarios que expresan instrucciones para la IA y la utilizan.

De todos modos, en cualquier etapa de la IA los datos empleados no quedan expuestos, pero, aún así, la protección de la persona requiere de los sujetos asociados al desarrollo, despliegue o uso de IA del cumplimiento del art. 1710 del CCC para prevenir daños, adoptando conductas diligentes y de buena fe que minimicen riesgos: siendo importantes tareas como anonimizar, encriptar y disociar lo relevante de los datos de las personas titulares y limitar los datos a la función propia de la IA para posteriormente eliminarlos de ser innecesarios.

Por otro lado, es importante, como parte de la función preventiva de la responsabilidad en general, permitir el acceso, la rectificación y remoción de datos incorrectos mediante un mero trámite privado, online y con respuesta en tiempo razonable. Pero, la oposición al uso de datos personales por el titular, queda sujeta a la inexistencia de un mejor interés o derecho para la persona detrás de la IA. Y, en todo caso, queda disponible y accesible la acción de habeas data o incluso una acción preventiva si se avizora razonablemente la causación de perjuicios concretos por la tenencia y empleo de datos solo de forma antijurídica, considerando el aval que asigna nuestro derecho a la actividad; puesto que la acción preventiva no debe entorpecer actividades legítimas.

En cuanto a la responsabilidad civil resarcitoria por el empleo de datos personales -sin perjuicio de qué puede existir por otros conflictos, como los relativos a los derechos de propiedad intelectual-, parece circunscrita a cuestiones de seguridad y de confidencialidad quebrantadas en cualquier etapa del desarrollo y funcionamiento de la IA. También parece posible la responsabilidad de los proveedores y responsables de despliegue por vulneración del derecho de acceso, rectificación, remoción de datos incorrectos y por empleo de datos personales frente a la oposición fundada del titular sin la existencia de un interés superior acreditable en favor de los sujetos ligados a una IA. En estos casos, no aparece una actividad dañosa justificable en base al ejercicio regular de un derecho, más bien todo lo contrario.

En estos supuestos, se estima que los deberes indicados son obligaciones de resultado (art. 774 y 1723 del C.C.C), por lo que la responsabilidad civil resarcitoria es objetiva. La opacidad del sistema de IA es incompatible con un sistema de responsabilidad por culpa; ya que sería una exigencia diabólica en nuestros tribunales que carecen de peritos suficientemente distribuidos en todo el país. Y, una inversión de la carga de la prueba, no es compatible con las obligaciones de resultado.

Por otro lado, teniendo en cuenta riesgo propio de la actividad, su masividad, el domicilio extranjero de las empresas y el potencial dañoso, creemos que se debe allanar el camino de los damnificados mediante legitimaciones pasivas amplias y deben responder los proveedores, quien despliega y aprovecha a la IA y quien está a cargo de su mantenimiento y seguridad informática -arts. 1757 y 40 LDC de corresponder-.

Cabe destacar que es especialmente pasible de responsabilidad civil aquella IA que es creada para fines que, de por sí, son dañosos o de alto riesgo: como las IA que pueden crear imágenes falsas de personas desnudas que han causado severos perjuicios a adolescentes[23] y gente famosa[24]. En este caso, responden personas físicas y jurídicas bajo las reglas de la responsabilidad de los grupos de riesgos, siendo un supuesto de responsabilidad colectiva por el carácter masivo de las lesiones de derechos de terceros, daños previsibles y consustanciales con las función de la IA (art. 1762 C.C.C.).

En la etapa de desarrollo de la IA y durante su explotación, no procede la aplicación de daños punitivos por el uso de datos personales ni la aplicación de la LDC, si no existe una relación de consumo entre el titular

---

[23] https://www.infobae.com/estados-unidos/2024/06/03/las-imagenes-falsas-de-desnudos-creadas-con-ia-se-han-convertido-en-la-peor-pesadilla-para-los-adolescentes-en-eeuu/

https://www.lanacion.cl/alumnos-del-colegio-saint-george-crearon-imagenes-de-companeras-desnudas-usando-ia-y-las-viralizaron/

https://elpais.com/espana/2023-09-18/la-policia-investiga-el-desnudo-integral-de-varias-menores-en-extremadura-con-inteligencia-artificial-me-dio-un-vuelco-el-corazon.html#

[24] https://www.lemonde.fr/pixels/article/2024/01/30/fausses-photos-pornographiques-de-taylor-swift-l-ia-et-les-recoins-sombres-d-internet_6213910_4408996.html

de los datos y las entidades que crean, desarrollan, introducen o despliegan una IA al momento de la creación, entrenamiento, prueba y uso. Con mayor razón, cuando no son las entidades las que solicitan los datos al titular y los obtienen de forma legítima. Por supuesto, dependiendo del destino que le de un sujeto a la IA, podría haber relación de consumo una vez que opera la IA en el mercado y está disponible para quienes pueden emplearla para fines personales.

Una vez introducida en el mercado la IA sí puede haber relación de consumo, e importan los datos que puede obtener la IA por el uso. En este último caso, corresponden los mismos derechos al titular de los datos y sí pueden caber daños punitivos de haber conductas antijurídicas graves, junto con la responsabilidad civil preventiva y resarcitoria en hipótesis semejantes a las desarrolladas.

SISTEMAS DE INTELIGENCIA ARTIFICIAL, DATOS Y PREVENCIÓN DEL DAÑO (TRANSPARENCIA Y EXPLICABILIDAD)

Por Carlos I. Bustos[1]

I. CONCLUSIONES

1. Desde noviembre de 2022 los modelos basados en IA generativa (que consiste en modelos de aprendizaje automático, para crear patrones y relaciones de conjunto de datos de contenido) se masificaron, dado que posibilitan utilizar todos los datos que se tiene disponibles sobre el usuario (por ejemplo, los provenientes de un big data set) y conforme un algoritmo[2] (de IA) va a elegir la mejor opción (con ahorro de tiempo y dinero) para satisfacer las necesidades[3]. La propuesta de estas empresas para el consumidor es fabulosa, pues maximiza los estándares de efectividad y eficiencia, de allí que la mayoría de los usuarios aceptamos los resultados sin conocer -del todo- los mecanismos empleados por estos procesos, cediendo la razonable comprensión del medio utilizado –y sus potenciales consecuencias- por la practicidad de los resultados[4].

2. En la presente ponencia, pongo a consideración que, junto con estos evidentes beneficios, la IA generativa puede amenazar la privacidad de los usuarios, generar desinformación o falsa información, con alguna opacidad en la forma en que el sistema procesa y usa los datos. Describo algunos elementos e instrumentos que permitirían un enfoque preventivo, basado en los riesgos, considerando el consentimiento informado, la

---

[1]Profesor Titular Experto de la materia Derecho de Daños UES 21. Magistrado Juz 32 Civil y Comercial de la ciudad de Córdoba. Especialista en Derecho Procesal UNC. Magister en Derecho y Argumentación UNC . Escribano

[2] Rudimentariamente, algoritmo puede definirse como como un conjunto ordenado de operaciones sistemáticas que permite hallar soluciones a ciertos tipos de problemas

[3] Los modelos de lenguaje natural más poderosos que existen, son GPT-4 de OpenAI y Gemini de Google DeepMind, funcionan con texto, imágenes y audio.

[4] No existe, por ejemplo, una clara conciencia de pérdida o afectación de derechos tales como la intimidad, el uso de datos personales, el secreto de las comunicaciones, etc. Es que el uso de estas tecnologías, también permitiría que escuchen conversaciones, captar las fotografías tomadas con la cámara del equipo, el libre acceso a sus contactos, registran las búsquedas realizadas en Internet, los desplazamientos y rutas, gustos, frecuencia de compras y un sinnúmero de situaciones similares.

explicabilidad y la transparencia de las tecnologías emergentes. Propongo integrar al concepto de consentimiento informado, los principios de transparencia y explicabilidad.

II. FUNDAMENTOS

1. LA ERA DE LOS DATOS Y LA TECNOLOGÍA DIGITAL

Para iniciar el análisis del tema, resulta necesario considerar –al menos sintéticamente- la operatoria coyuntural de los negocios que llevan adelante las grandes empresas –denominadas "data brokers"[5] representadas por Google, Apple, Facebook, Amazon– que desarrollan u operan con tecnología pensada para el almacenamiento, procesamiento y tratamiento de datos personales de los usuarios de las aplicaciones, redes o plataformas digitales que administran. Estos datos, les permite elaborar perfiles, predecir conductas e incidir en el comportamiento de las personas[6]. Esa recolección masiva de datos se lo denomina "big data" (BD). Para realizar el procesamiento de datos de manera rápida y efectiva, utilizan sistemas de inteligencia artificial, que automatizan el proceso de análisis, revelando por ejemplo patrones o tendencias, que les permite realizar analítica predictiva. Tanto uno como otro dependen de los datos: la Inteligencia Artificial requiere conjuntos de datos grandes para su entrenamiento, y el "big data" es la fuente de estos conjuntos de datos. En esencia, el BD proporciona la materia prima, y la IA procesa e interpreta ese material para generar ideas y acciones inteligentes[7].

Para trazar una breve descripción de lo que implica la IA, el Grupo de Expertos en IA de la Organización para la Cooperación y el Desarrollo

---

[5] Albornoz, María Mercedes "El titular de datos personales, parte débil en tiempos de auge de la Inteligencia Artificial. ¿Cómo fortalecer su posición?" Revista Del Instituto de Ciencias Jurídicas de Puebla, México. Nueva Época Vol. 15, No. 48. Julio - Diciembre De 2021. pags. 209-242

[6] Por ejemplo, el conocido y condenable suceso por el cual la firma "Cambridge Analytica" tomó datos de millones de usuarios de Facebook" sin su consentimiento, principalmente para utilizarlos con un fin de propaganda política.

[7] Cristina Ortega "Big data e inteligencia artificial": ¿Cómo trabajan juntos? Extraído de https://www.questionpro.com/blog/es/big-data-e-inteligencia-artificial/#:~:text=La%20Inteligencia%20Artificial%20(IA)%20desempe%C3%B1a,y%20reducci%C3%B3n%20de%20errores%20humanos.

Económicos (OCDE)[8] elaboró una descripción de un sistema de IA, que permite identificarla como aquel basado en máquinas, que es capaz de influir en el entorno produciendo un resultado (predicciones[9], recomendaciones o decisiones) para un conjunto determinado de objetivos. Utiliza datos e insumos basados en máquinas y/o humanos para i) percibir entornos reales y/o virtuales; ii) abstraer estas percepciones en modelos a través del análisis de manera automatizada (por ejemplo, con aprendizaje automático), o manualmente; y iii) usar la inferencia del modelo para formular opciones para los resultados. Asimismo, el Reglamento, en proceso de aprobación, para la Unión Europea (Ley de Inteligencia Artificial o AI Act) define al "sistema de IA" como un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales[10].

En este contexto, los expertos en marketing digital han desplegado tecnologías de gran alcance para la recogida de datos, la elaboración de perfiles y la selección de objetivos en línea. Se hace habitual convivir con la creación de "perfiles virtuales" de las personas, a partir de la información o datos personales existente (al navegar por internet, uso del GPS, enviar un correo electrónico, etc.). Además, se adoptan decisiones con respecto a ellas a partir del tratamiento automatizado de sus datos mediante diversas herramientas tecnológicas. En este sentido, las personas pueden verse afectadas con las decisiones que se tomen a su respecto a partir del uso y tratamiento de datos personales en procesos de inteligencia artificial (religión, sexo biológico, etc.), como por ejemplo solicitud de crédito, fiabilidad, ubicación o movimientos del usuario, como también las

[8] Disponible en https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[9] El término predicción es ambiguo y puede significar conceptos diferentes en distintos textos, softwares, etc. e implicar explicación, esperanza condicional, pronóstico, etc.

[10] Art. 3 literal 1) Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts {SEC(2021) 167 final}–{SWD(2021) 84 final}– {SWD(2021) 85 final}. Disponible en https://artificialintelligenceact.eu/the-act/.

decisiones basadas en datos no personales pero basado en situaciones personales (calidad o cantidad de bienes o servicios) que también pueden producir un efecto jurídico o similar significativo sobre el interesado; por consiguiente, requerirían igualmente una explicación técnica.

2. EL USO CONSENTIDO Y GRATUITO DE APLICACIONES/PLATAFORMAS DIGITALES.

Más allá de la sintética descripción expuesta, nuestra cotidianeidad permite evidenciar – como un hecho notorio- que el uso de estos sistemas condiciona nuestros hábitos, generando nuevas necesidades, sin tomar plena conciencia de ello.

A modo de ejemplo, en la práctica tribunalicia la mayoría de litigantes y personas que juzgan, recibieron con beneplácito la idea de implementar "notificaciones digitales" (e-cedulas), "registración de audiencias" o incluso receptar el denominado "expediente digital", al que se accede mediante la utilización de un sistema operativo que permita a los usuarios visualizar y revisar las actuaciones de manera digital o electrónica: la migración del mundo analógico de los átomos, hacia el mundo digital de los bits[11]. No debe pasar desapercibido que, junto con los beneficios de la digitalización del expediente, en correlato, se obliga al uso de aplicaciones (i.e. obtener una dirección de correo electrónico), visitar sitios web, crear un usuario y contraseña, todas estas cuestiones que implica contactarse con los "data brokers" (Google, Microsoft etc.), lo que genera todo un "ecosistema digital".

En principio, nada para objetar pues se trata de productos y servicios: i) confiables y seguros, dado que se requieren permisos (consentimiento) del usuario para acceder a ciertos datos[12] y ii) su uso es generalmente gratuito. Sin embargo, ambas afirmaciones no son del todo correctas, pues se fundan en una mirada incompleta e ingenua de las condiciones en que se presta el consentimiento y la gratuidad del servicio.

---

[11] De Resende Chaves Júnior (2015) *"El Expediente en Red y La Nueva Teoría General del Proceso";* Biblioteca Digital Gratuita de E-Justicia Latinoamérica; disponible en http://wp.me/p4n5ZR-6n

[12] Esto puede corroborarse ingresando a https://support.google.com/mail/answer/10434152?hl=es-419

Como bien se afirma, las plataformas digitales no aparentan peligro ni limitación sobre el consentimiento, sino que al contrario "conscientes del condicionamiento que imponen, nos consultan previamente sobre nuestra conformidad para acceder a nuestros datos personales"[13]. Si bien es correcto que existen reglas sobre el tratamiento de datos y las condiciones en que el consentimiento de otorga, con frases como "tu privacidad nos importa"; "si consientes su instalación pulsa aceptar Cookies"; pero lo real es que el usuario no puede negarse a consentir pues sin hacer clic no puede acceder al servicio (que siguiendo con el ejemplo seria algo tan necesario como acceder a las e-cedulas). Aceptar con un clic clausulas tales como "Nosotros y terceros seleccionados utilizamos cookies o tecnologías similares con fines técnicos y, con su consentimiento, para otras finalidades", implica repensar que extensión se otorga al consentimiento para "la instalación de cookies" y como debe ser informado, pues se condiciona la posibilidad de continuar navegando, seguir un enlace, desplazarse por la página o cualquier otro método que requiera que el usuario proceda activamente.

Considerando que los sistemas gestionados mediante IA (plataformas digitales, sitios web, aplicaciones, etc.) son indispensables, en cuanto necesarias para poder participar activamente en la sociedad (i.e. enviar una cedula), ya no hay posibilidad de excluirnos de forma voluntaria de la recopilación de datos, que subyace como condición. Más aún, el sujeto moderno, tecnológicamente condicionado, al aceptar mediante un simple clic ingresa al servicio y entrega como contraprestación sus propios datos personales.

Estas tecnologías, en particular el desarrollo de la IA, ha convertido a los datos personales en activos valiosos, a tal punto de considerarse "commodities" con alta demanda[14]. En tal sentido, los datos tienen un valor económico que es reconocido abiertamente por las prestadoras de bienes y servicios en Internet. La cuestión problemática es que al aceptar el uso de estas tecnologías, es posible que también aceptemos el acceso a información tan sensible como el origen racial o étnico del usuario, sus opiniones políticas, convicciones religiosas, filosóficas o de otro tipo. Cuando las

[13] De Lorenzo "La tutela del derecho personalísimo a los datos personales (La actualidad del debate entre Alfredo Orgaz y Santos Cifuentes)" en "Márquez J. F. "Revista de Estudios de Centro" Volumen 1, Nro. 2, paginas 7/20

[14] Ontiveros Emilio (Director) "Economía de los Datos. Riqueza 4.0" Ariel, Barcelona 2017

personas navegan en Internet, exploran redes sociales o usan aplicaciones generalmente comparten datos personales como nombre y apellido, DNI, geolocalización, domicilio, número de teléfono o correo electrónico. A veces, incluso sin saberlo, pueden poner a disposición de las empresas y entidades que las administran información sobre gustos o intereses que permiten identificar directa o indirectamente a su titular, así como uno o varios elementos característicos de su identidad física, fisiológica, genética, biométrica, psíquica, económica, cultural, social, etc tal como se plasma en las recomendaciones internas.[15]

En Estados Unidos, ante la irrupción de ChatGPT y otras aplicaciones de IA generativa, conscientes de los problemas que puede generar esta tecnología, se manifiesta que la inteligencia artificial está facilitando la extracción, reidentificación, vinculación, inferencia y acción en base a información sensible sobre las identidades, ubicaciones, hábitos y deseos de las personas. Las capacidades de la inteligencia artificial en estas áreas pueden aumentar el riesgo de que los datos personales puedan ser explotados y expuestos[16].

3. LA CLASIFICACIÓN DE SISTEMAS DE IA SEGÚN LOS RIESGOS

Lo expuesto permite colegir que, si bien el usuario puede poner a disposición de estas empresas (data brokers) información sobre gustos o intereses de manera voluntaria, conforme la clásica concepción de estos bienes dentro de la autonomía privada; debemos pensar si tal consentimiento deja de ser un acto de autorización unilateral revocable (art.55 del Código Civil y Comercial CCC), sino el objeto de una contraprestación según la cual se permite el acceso a ciertos datos conforme las reglas de los bienes del mercado (artículo 959 CCC), dado que algunas empresas, como por ejemplo Google, pueden crear un perfil completo de cada usuario en función de la información de diferentes productos tales como búsqueda, mapas, correo electrónico y su red social.

---

[15] Disponibles en https://www.argentina.gob.ar/noticias/recomendaciones-de-la-aaip-para-proteger-datos-personales-en-internet

[16] Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. Disponible en https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

En estos términos, el desarrollo alcanzado por Internet y, particularmente, por la IA, desafía el alcance y la validez del consentimiento informado[17], pues los datos personales de los usuarios de bienes y servicios de base tecnológica, constituyen un "valor en si mismos" demuestra que los usuarios no son "free-riders" de las empresas; el pago por el acceso a los servicios ofrecidos no es en moneda, sino en datos. De allí que la modalidad de manifestar la voluntad mediante un "clic" de aceptación a los términos y condiciones de las páginas, las plataformas, las redes sociales, las apps, y en general, la totalidad de los servicios disponibles en medios tecnológicos o virtuales es esencialmente problemática y naturalmente riesgosa en lo que hace a la recopilación y uso de datos.

Es por ello que las propuestas normativas existentes, se diseñan en base a una aproximación de riesgos.

Así por ejemplo, para la Unión Europea (Reglamento de la Inteligencia Artificial) las aplicaciones de IA se clasifican en cuatro niveles de riesgo: inaceptable, alto, medio o limitado y mínimo). Las primeras generan riesgos inadmisibles por contravenir los valores de la Unión Europea, en particular, al facilitar la vulneración de derechos fundamentales, por ejemplo aquellos sistemas que utilizan técnicas subliminales que pueden conducir a la manipulación o los sistemas que pretenden aprovecharse de la especial vulnerabilidad de personas o aquellos que incluyen los sistemas de puntaje social estatal. Las de riesgo alto o elevado son aquellas que por las características o actividad es previsible que existan riesgos significativos[18], son por ejemplo máquinas o robots operados autónomamente con sistemas de inteligencia artificial, que incluye juguetes; dispositivos médicos; aviación civil; vehículos automotores; identificación biométrica; operación y gestión de infraestructuras criticas; aplicación en el sector de la educación; empleo y recursos humanos; acceso a servicios esenciales públicos o privados —incluye riesgos de crédito de personas naturales— seguridad pública; control de fronteras y migraciones; administración de la justicia. De riesgo medio o limitado, son ciertas aplicaciones que interactúan con

[17] Cotino Hueso, Lorenzo, "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", Dilemata. Revista Internacional de Éticas Aplicadas, Año 9, No. 24, mayo 2017, p. 145. [Disponible para su descarga a partir de: https://www.dilemata.net/revista/index.php/dilemata/article/ view/412000104

[18] Informe de la relatora especial a la Asamblea General de Naciones Unidades: disponible en https://www.idhc.org/arxius/noticies/N2324238.pdf

personas y que se emplean para detectar emociones o realizar asociaciones mediante categorías basadas en datos biométricos —como es característico de los robots conversacionales o de los sensores para la predicción y prevención de procesos críticos—, o que son susceptibles de generar o manipular contenido, como en el caso de los llamados "deep fakes" que vinculan la imagen y voz de una persona con un mensaje que esta nunca llego a transmitir. Los sistemas de inteligencia artificial que no se hallan comprendidos en ninguna de las tres categorías anteriores, se consideran de riesgo mínimo o nulo, por ejemplo, aquellas que recomiendan películas al usuario.

La IA generativa (i.e. ChatGTP) se encontraría entre el riesgo medio y alto dependiendo del uso específico y del contexto en el que se implementen[19]. En este trabajo me concentro en los de riesgo medio, es está constituido por el riesgo a la "desinformación", es decir cuando la IA generativa puede producir contenido que parezca creíble pero que sea incorrecto o engañoso. Esto puede afectar la toma de decisiones de los usuarios y la difusión de información falsa, sea porque los datos se interpretaron erróneamente o bien porque no se expresa que el contenido fue elaborado por una IA, porque carece de supervisión humana o que puede contener datos erróneos o peligrosos (slop o bazofIA[20])

Una de las formas de prevenir el daño que puede causar esta IA generativa es el análisis de explicabilidad, como herramienta útil para mitigar los riesgos que puede provocar la utilización indebida de datos, sea por falsos o incorrectos.

4. EL ANÁLISIS DE TRANSPARENCIA Y EXPLICABILIDAD

Tal como vengo afirmando, los datos personales de los usuarios tienen un valor económico para las prestadoras de bienes y servicios digitales. Al aceptar el uso de estas tecnologías, es posible que el usuario

[19] Dentro de estos últimos esta ubicada contextos críticos como diagnósticos médicos, decisiones legales, o educación, los errores o sesgos en la generación de contenido pueden tener consecuencias graves para los individuos afectados, el uso indebido de datos personales para entrenar o generar contenido puede infringir la privacidad de los usuarios y plantear riesgos de seguridad

[20] Como se advierte en https://www.theguardian.com/technology/article/2024/may/19/spam-junk-slop-the-latest-wave-of-ai-behind-the-zombie-internet

también acepte el acceso a información relacionada con los datos demográficos del usuario, edad, sexo, ocupación, tan sensible el uso de sistemas con IA generativa implica que el usuario debe necesariamente permitir. También afirmé, que el consentimiento en los términos clásicos aparece como insuficiente en relación a los distintos tipos de datos de entrenamiento de la IA. Las razones es que estos datos sean utilizados de manera diferente al consentimiento inicialmente prestado. Por ejemplo lo que se utiliza son los banners de cookies los que no son específicos o claros. En este sentido, es ilustrativa una sentencia del Tribunal del Justicia de la Unión Europea (TJUE) de fecha 01/10/2019, donde se trató la política de "cookies" y el modo de obtener el consentimiento para instalar y utilizar la inmensa mayoría de las páginas web actuales. En el fallo se exige que el consentimiento se debe prestar de forma expresa, que debe facilitarse su "gestión" y que el rechazo no puede impedir navegar por la página de que se trate.

Es que los sistemas de IA orientados al usuario pueden ser potencialmente susceptibles a la manipulación y dar lugar a los usuarios faciliten información que no esperaban aportar, mediante conexiones sofisticadas, permitiendo la elaboración de perfiles a los que inicialmente el usuario no accedió. Por ejemplo, es cada vez más frecuente que los anunciantes "Premium" insistan en una prueba de consentimiento para recoger datos de los usuarios antes de asociarse con desarrolladores de aplicaciones.

De allí que resulta necesario pensar si resulta necesario adaptar la idea de "consentimiento", acompañándola por una serie de principios para una gestión responsable de la IA (Principles for responsible stewardship of trustworthy AI) tal como el principio de transparencia y explicabilidad (explainability).

La transparencia tiene como objetivo proporcionar información adecuada a los respectivos destinatarios para permitir su comprensión y fomentar la confianza[21]. Lo que subyace en el principio es facilitar información clara con respecto de las capacidades y limitaciones del sistema de IA, los objetivos del sistema, las condiciones en las que se espera que funcione según lo previsto y el nivel de exactitud esperado en la consecución

[21] UNESCO, Recomendación sobre la ética de la inteligencia artificial https://www.unesco.org/es/articles/recomendacion-sobre-la-etica-de-la-inteligencia-artificial

del objetivo mencionado. Según los casos, se debe informar claramente al usuario cuándo esta interactuando con un sistema de IA y no con un ser humano.

Estrechamente vinculado a lo anterior esta la explicabilidad que incluye la mención clara de los elementos pertinentes para la existencia de un sistema de IA: los datos, el sistema y los modelos de "negocio" en el caso de que el interesado esté sometido a decisiones automatizadas o a la elaboración de perfiles, el titular del dato puede entender cómo se produce el tratamiento al que será sometida la información que le concierne, por ejemplo, si se trata de un caso de inteligencia artificial se debe dar información significativa sobre la lógica aplicada y la importancia y las consecuencias previstas (art. 22 RGDP)[22]. Por otra parte, el artículo 63 del mismo reglamento otorga al interesado el derecho a conocer y recibir comunicaciones sobre la lógica que subyace a cualquier tratamiento de datos en relación con la toma de decisiones automatizada.

El detalle de los datos empleados para la toma de decisión, más allá de la categoría, y en particular información sobre los plazos de uso de los datos (su antigüedad). La importancia relativa que cada uno de ellos tiene en la toma de decisión. La calidad de los datos de entrenamiento y el tipo de patrones utilizados. Los perfilados realizados y sus implicaciones. Valores de precisión o error según la métrica adecuada para medir la bondad de la inferencia. La existencia o no de supervisión humana cualificada. La referencia a auditorías, especialmente sobre las posibles desviaciones de los resultados de las inferencias, así como la certificación o certificaciones realizadas sobre el sistema de IA. En el caso de sistemas adaptativos o evolutivos, la última auditoría realizada. En el caso de que el sistema IA contenga información de terceros identificables, la prohibición de tratar esa información sin legitimación y de las consecuencias de realizarlo[23]. Permite que las personas afectadas por el resultado de un sistema de IA entiendan cómo se llegó a él. Esto implica proporcionar información fácil de entender a las personas afectadas por el resultado de un sistema de IA que les permita

[22] Según el artículo 22 del RGDP todo interesado tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. *En Argentina la Resolución 4/2019 dictada por la AAPI (Ley 25.326)*

[23] Ver https://legalinstruments.oecd.org/en/

cuestionar el resultado en particular, en la medida de lo posible, los factores y la lógica que condujeron a un resultado[24].

5. LA FUNCIÓN PREVENTIVA INTEGRADA POR CONSENTIMIENTO, TRANSPARENCIA Y EXPLICABILIDAD.

En nuestro sistema cuenta con normas genéricas, que hacen posible la aplicación de las nociones preventivas (arts. 1710 a 1713 del CCC) para mitigar o minimizar los posibles daños de los sistemas de IA.

Entre las diversas estrategias, propongo apelar, en clave preventiva, a las nociones de consentimiento informado, transparencia y explicabilidad que, aunque diferentes y que bien pueden solaparse, merecen un tratamiento conjunto.

Como bien se sabe el "consentimiento informado" es una de las principales herramientas habilitadas por el ordenamiento jurídico para el ejercicio de los derechos fundamentales en la era digital y en el ámbito europeo se plantea como una de las formas de hacer realidad el "derecho a la autodeterminación informativa"[25]. Es un proceso mediante el cual un individuo es debidamente informado sobre los aspectos relevantes de una actividad o tratamiento de datos y, con base en esa información, decide libremente si desea aceptar o rechazar participar en dicha actividad o tratamiento. El propósito del consentimiento informado es asegurar que las personas tengan control sobre sus datos personales y sean plenamente conscientes de cómo, por qué y para qué se utilizan esos datos[26]. Se vincula al derecho a una Información completa, clara, precisa y comprensible sobre el propósito del tratamiento, los datos que se recopilarán, cómo se utilizarán, los riesgos involucrados y sus derechos; que debe ser otorgado libremente,

---

[24] Argentina: Subsecretaría de Tecnologías de la Información, Disposición nro. 2/2023, de fecha 01/06/2023

[25] Tribunal Constitucional español causa 254/1993. La Corte Constitucional Federal alemana se pronunció en 1983 acerca de la autodeterminación informativa y consideró que el libre desarrollo de la personalidad requiere que el individuo goce de protección contra la recolección, el almacenamiento, el uso y la transmisión ilimitados de datos personales. Sentencia del 15 de diciembre de 1983 Disponible en: https://www.bundesverfassungsgericht.de/e/rs19831215_1bvr020983.html

[26] La Corte Interamericana de Derechos Humanos ha dicho que el consentimiento informado se basa en el respeto a su autonomía y su libertad para tomar decisiones de acuerdo a su plan de existencia, la autonomía es un elemento indisoluble de la dignidad de la persona (caso "I. V. vs. Bolivia, noviembre 2016)

sin coerción ni engaño, por persona con plena capacidad para entender la información y tomar una decisión informada, incluso la posibilidad de revocarlo, y la persona debe ser informada de este derecho (arts.5 y 11 de la Ley N° 25.326). El ordenamiento refleja la libertad individual, y la autonomía de la voluntad, admitiendo la facultad de disponer de ciertos atributos de la personalidad, con los límites impuestos por la propia ley, la moral y las buenas costumbres (Artículo 55 CCC). Para la Unión Europea (Ley de Inteligencia Artificial o AI Act) el "consentimiento informado" es la expresión libre, específica, inequívoca y voluntaria por parte de un sujeto de su voluntad de participar en una determinada prueba en condiciones reales tras haber sido informado de todos los aspectos de la prueba que sean pertinentes para su decisión de participar.[27]En Latinoamérica, encontramos los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales adoptados por el Comité Jurídico Interamericano (CJI) y aprobados por la Asamblea General de la OEA en 2021[28], donde se advierte también la combinación de estos principios para la especificación de las categorías de Datos Personales a ser tratados, las finalidades para las cuales se traten, así como los destinatarios o categorías de destinatarios a quienes se divulgarán y la explicación accesible y comprensible para el usuario medio, no solo para expertos en tecnología. El Reglamento General de Protección de Datos (GDPR) de la Unión Europea[29], en el artículo 22 establece que los individuos tienen derecho a no ser objeto de una decisión basada únicamente en el procesamiento automatizado, y los artículos 13 a 15 otorgan el derecho a recibir información significativa sobre la lógica involucrada en dichos procesos. Es necesario remarcar el binomio "derecho deber de transparencia e información al interesado" (arts. 5.1.a y 14.5.b del Reglamento General de Protección de Datos) frente a usos insospechados o desconocidos en el momento de la obtención del consentimiento; la minimización de datos porque va en contra de muchos sistemas que se basan

[27] Reglamento consejo Europeo art. 3 https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_ES.pdf

[28] https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

[29] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

precisamente en mezclar grandes cantidades de información y otros datos que no tienen esa consideración.

No en todos los casos se debe hablar de los tres conceptos en forma conjunta, pues muchas veces con las normas jurídicas tradicionales (consentimiento, publicidad engañosa) es posible exigir conductas o medidas preventivas del daño, así por ejemplo una plataforma digital (Netflix, Amazon) puede ofrecer al usuario una prueba gratis que automáticamente se convierte en una suscripción paga al final el periodo de prueba sin que este haya sido advertido previamente; en el supuesto aplicando las normas clásicas de consentimiento informado se advierte una violación notoria de las normas, en el mismo ejemplo la plataforma puede diseñar la interfaz para que el botón para cancelar sea difícil o pasos complicados, aquí también es posible apelar a las normas clásicas para resolver la cuestión.

Pero por ejemplo, las plataformas de transporte privado de pasajeros (Uber o Cabify), gestionadas con IA podrían fijar precios o tarifas más elevados para aquellos usuarios con teléfonos con batería baja o ubicados en zonas peligrosas de la ciudad, ya que ellos pueden estar más desesperados en tomar el servicio. Esta decisión, esta basada en la información sobre la carga de la batería o la geolocalización no puede identificar a un usuario específico y además el usuario puede ver afectado su libre consentimiento, dado que al otorgar su consentimiento para la instalación de la aplicación; pero no para que le fijen tarifas según la lectura de la carga de la batería o la geolocalización, no le fue explicado y el interesado tiene derecho a conocer la lógica que subyace a cualquier tratamiento de datos en relación con la toma de decisiones automatizada[30].

Otro supuesto que permite advertir la importancia de la explicabilidad es la utilización de plataformas para la reserva de vuelo y hoteles (Despegar), quienes rastrean las cookies de navegación del usuario para elaborar patrones de búsquedas; si la búsqueda es reiterada, interpreta que existe especial interés en un determinado destino u hotel y aumentar el precio. En estos casos se detecta lo que la doctrina llama “patrones

[30] Mascitti Matías “La función preventiva de los daños causados por la robótica y los sistemas autónomos” Direitos Fundamentais & Justiça | Belo Horizonte, ano 16, número especial, p. 15-54, outubro 2022. Disponible: https://dfj.emnuvens.com.br/dfj/article/download/1319/1063

oscuros"31; por consiguiente, ello no equivale a una indicación específica, informada e inequívoca de la voluntad del interesado respecto al tratamiento de sus datos. Esto otorga potencialmente al interesado el derecho a una explicación de la tecnología. De hecho en 2000 Amazon cobro a los clientes precios diferentes por los mismos títulos de DVD[32]

Con el manejo de datos sensibles, como el género, se torna aún más evidente la necesidad adoptar estos principios, si por ejemplo un sistema de contratación automatizado está entrenado con datos, donde, históricamente, se han contratado más hombres que mujeres para ciertos roles, la IA podría priorizar los postulantes hombres, el uso indebido de datos puede llevar a decisiones discriminatorias sin el consentimiento explícito de ser evaluado bajo estos sesgos.[33]Aquí se alza la explicación como una garantía en caso de tales decisiones.

En consecuencia, generar estrategias y políticas públicas que conlleven conocimiento de los riesgos de daños causados por los sistemas de IA en el manejo de datos, la forma de prestar el consentimiento, la transparencia y aplicabilidad en la toma de decisiones la disminución de esos perjuicios; por ejemplo, para prevenir la discriminación o evitar un uso indebido de los datos personales.

6. CONCLUSIÓN

Para desarrollar los sistemas de IA se recolectan, almacenan, analizan y procesan enorme cantidad de información, usada para generar

---

[31] Existen seis tipos de patrones oscuros: sobrecarga, omisión, agitación, obstaculización, inconstante y dejada en la oscuridad https://www.edpb.europa.eu/edpb_en

[32] Serrano, E.; Such, JM.; Botia, JA.; García Fornes, AM. (2014). Strategies for avoiding preference profiling in agent-based e-commerce environments. Applied Intelligence. 40(1):127-142. doi:10.1007/s10489-013-0448-2

[33] Amazon diseñó una herramienta de contratación que revisaba currículums de los solicitantes de empleo con el objetivo de mecanizar la búsqueda de los mejores talentos, pero el sistema no calificaba a los candidatos de una manera neutral al género. Esto se debió a que los modelos informáticos de Amazon fueron capacitados para examinar a los solicitantes mediante la observación de patrones en los currículums enviados a la empresa durante un período de 10 años y la mayoría provenía de postulantes hombres https://www.reuters.com/article/amazon-com-contratacion-ia-idESKCN1MO0M4/

diversos resultados, acciones o comportamientos por parte de los sistemas o de los usuarios de estas.

Son innegables los beneficios de la IA en cuanto a la eficacia de tiempos y costos; pero no debe perderse de vista que implican desafíos, peligros o amenazas que son intrínsecos a la inteligencia artificial. A título enunciativo, por ejemplo, dichos riesgos pueden incluir aspectos como la falta de ética comercial en el desarrollo o uso de la inteligencia artificial, la toma de decisiones sesgadas, no transparentes o incorrectas.

Es necesario considerar los niveles de riesgo que implican estos sistemas, conforme el uso especifico y el contexto en que se implementen, de allí que resulta necesario la identificación de riesgos de manera preventiva para luego mitigarlos. Las prácticas deben ser gestionadas preventivamente de acuerdo con las regulaciones de protección de datos y con un enfoque en la transparencia y el consentimiento del usuario, permitiendo entender como se utilizan los datos mediante la explicabilidad.

RESPONSABILIDADE CIVIL E A UTILIZAÇÃO DE ROBÔS DE ASSISTÊNCIA Á SAÚDE E ANÁLISE DO DIAGNÓSTICO COM INTELIGÊNCIA ARTIFICIAL NA AMÉRICA LATINA: QUEM DEVE SER RESPONSABILIZADO EM CASO DE DANO À SAÚDE?

Por Gracemerce Camboim Jatobá e Silva[1]

I. CONCLUSIONES

1. À luz da breve análise realizada, podemos afirmar que estamos diante de uma nova realidade no qual a medicina depende de ferramentas de tecnologia da informação em saúde projetadas para fornecer aos médicos e a outros profissionais suporte à decisão clínica, ou seja, assistência nas tarefas de tomada de decisão para o tratamento dos pacientes, fornecendo um diagnóstico mais preciso e as melhores escolhas de tratamento.

2. Como visto, a responsabilidade decorrente do uso da IA no setor da saúde pode ser enquadrada em regras de negligência, no entanto, o uso de ferramentas de tecnologia da informação em saúde poderão interromper drasticamente o relacionamento típico entre médico e paciente, circunstâncias estas que causam problemas de causalidade, dificultando ao paciente prejudicado estabelecer um nexo de causal entre o dano e a conduta ilícita.

3. Portanto, no Brasil e na América Latina, caso os operadores do direito sigam interpretando os danos à saúde sob regras de negligência médica, cuja responsabilidade é subjetiva, o conceito de negligência médica terá que ser reformulado.

4. Concluiu-se também que a simples aplicabilidade das normas de protocolos médicos traz o perigo de alocações injusta de responsabilidades, considerando o fato de que a IA revela-se uma realidade muito mais complexa do que os parâmetros médicos tradicionais.

---

[1] Advogada, Professora substituta externa na Universidade de Brasília, Mestre em Comércio Exterior e Relações Internacionais pela UFPE, Doutoranda em Direito pela Universidade de Brasília/UNB.

5. No entanto, a abordagem da responsabilidade civil enfrentaria a desvantagem do fato de que, se não houver um órgãos responsáveis pela avaliação dessas ferramentas de tecnologia da informação em saúde, como enfatizado por Jerry Fishenden, os fabricantes de tecnologia deixarão de rotular seu software como IA para escapar da regulamentação.[2]

6. Uma responsabilidade compartilhada, a priori, compartilhar a responsabilidade entre todas as partes interessadas envolvidas no desenvolvimento, fabricação e uso da tecnologia - devem ser considerados, a fim de evitar que a vítima (paciente prejudicado) com o fardo de demonstrar e provar o erro médico e um nexo de causalidade entre o erro e o dano.

7. De acordo com a necessidade de criar um princípio legal de responsabilidade compartilhada, o papel do auto-cumprimento não deve ser desconsiderado, doravante, as partes interessadas envolvidas nesse processo devem seguir os códigos de conduta e ética na medicina.

8. Nos Estados Unidos foi estabelecido um Código de Conduta no qual foram estabelecidos sete princípios e que poderão servir como norte as interpretações no Brasil e na América Latina, quais sejam:

(i) Consciência: Proprietários, designers, construtores, usuários, e outras partes interessadas dos sistemas analíticos devem estar cientes dos possíveis vieses envolvidos na seu design, implementação e uso e os possíveis danos que podem causar a indivíduos e a sociedade;

(ii) Acesso e reparação: os reguladores devem incentivar a adoção de mecanismos que permitem questionar e reparar indivíduos e grupos que são afetados por decisões informadas por algoritmos;

(iii) Responsabilidade: as instituições devem ser responsabilizadas pelas decisões tomadas pelos algoritmos que elas usam, mesmo que não seja viável explicar em detalhes como os algoritmos produzem seus resultados;

(iv) Explicação: Sistemas e Instituições que usam a tomada de decisão algorítmica devem ser incentivadas a produzir explicações em relação aos procedimentos seguidos pelo algoritmo e às decisões

[2] UK'S PARLIAMENT, Select Committee on artificial intelligence collated written evidence volume - House of Lords(UK) - Statement of Cooley (UK) LLP (written evidence AIC0217) available on https://www.parliament.uk/documents/lords-committees/Artificial-Intelligence/AI-Written-Evidence-Volume.pdf acesso em 20.07.2020

específicas que irão utilizar, principalmente em contextos de políticas públicas;

(v) Origem dos dados: A descrição detalhada de como os dados foram coletados deve ser mantida pelo fabricantes destas tecnologia, acompanhados de uma exploração dos vieses potenciais induzidos por o processo humano ou algorítmico de coleta de dados;

(vi) Auditabilidade: modelos, algoritmos, dados, e as decisões devem ser registradas para que possam ser auditadas nos casos em que haja suspeita de dano;

(vii) Validação e teste: as instituições devem usar métodos rigorosos para validar seus modelos e documentar esses métodos e resultados. Em particular, deverão avaliar e determinar se os modelos geram danos discriminatórios.

9. Esses princípios abordam alguns dos principais obstáculos à compensação por danos no escopo do uso de ferramentas de tecnologia da informação na saúde.

10. Os princípios de conscientização e proveniência de dados visam fornecer uma orientação quanto a coleta dos dados iniciais sob os quais o sistema funcionará e permitirá que os pacientes coletem evidências sobre a falha do software que levou a um diagnóstico ou opção de tratamento quando a falha for resultado de um erro ou viés de dados.

11. Por outro lado, os princípios de prestação de contas e explicação abordam a caixa preta da tecnologia, promovendo práticas de transparência a serem adotadas entre aqueles que desenvolvem tecnologias dessa natureza. Sob esses princípios, instituições que usam algoritmos para fins clínicos de tomada de decisão deve produzir explicações sobre como os algoritmos trabalho, mesmo que - devido à obscuridade e opacidade do algoritmo - não seja possível fornecer uma explicação detalhada e completa.

12. Esse entendimento é de grande importância, uma vez que a falta de conhecimento sobre como funcionam os algoritmos utilizados para diagnóstico e tratamento médico, pode ser considerado como uma causa de exclusão de responsabilidades.

13. As auditorias são necessárias para alcançar uma alocação de responsabilidades mais claras e precisas para definir as responsabilidades e facilitar as chances das vítimas de obter a compensação pelos danos causados após um diagnóstico e prescrição errada de um tratamento.

14. Em suma, existe um consenso entre a comunidade tecnológica, jurídica e médica de que princípios e regras de transparência e

responsabilidade devem ser projetados e aplicados neste escopo a fim de que, mais do que definir a alocação de responsabilidades entre os atores envolvidos, forneça uma mais proteção a todos os pacientes cujo diagnóstico, tratamentos médicos ou decisões médicas de qualquer a natureza é substancialmente decidida pelos algoritmos de aprendizado de máquina.

II. FUNDAMENTOS

1. INTRODUÇÃO

Com a expansão e a chegada da Inteligência Artificia (IA) em larga escala, quem deve ser responsabilizado em caso de dano à saúde? Como atuar quando o assunto envolve a utilização de robôs de assistência à saúde e análise d diagnóstico com inteligência artificial na América Latina?

A IA para fins de diagnóstico médico e escolha de tratamento está se tornando uma ferramenta comum nas mãos de médicos em todo o mundo. Mais do que simplesmente confiar em suas informações pessoais de conhecimento técnico, os médicos agora são assistidos por máquinas, que avaliam os dados clínicos do paciente à luz dos dados os quais o algoritmo foi alimentado, fornecendo diagnóstico mais preciso e opções de tratamento.

Embora os benefícios por trás do uso dessa tecnologia sejam inquestionáveis, também é inquestionável que esse paradigma de saúde represente uma ruptura no relacionamento clássico entre as partes envolvidas na prestação de serviços de saúde. Se, antes, um paciente que sofreu dano no decurso de um diagnóstico ou no tratamento prescrito por um médico, facilmente identificaria o agente contra quem tomar as medidas cabíveis (o médico ou a instituição médica sob o qual o médico prestou os serviços de saúde), hoje, com o uso de ferramentas de IA, esse paradigma de responsabilidade direta ficou obscuro, considerando que, além do médico, existe outra entidade que poderá causar o dano, ou seja, a saída do algoritmo que o médico seguiu.

A realidade descrita traz várias questões relacionadas à alocação de responsabilidades. Ou seja, deve ser discutido se os conceitos tradicionais de negligência médica e o padrão de atendimento se adequam a essa nova realidade.

Nesse sentido, será avaliado se as regras de más práticas devem ser moldadas e adaptadas ou se a intervenção da IA interrompe a relação entre o profissional e o paciente de maneira tão severa que as regras de negligência médica devem ser desconsideradas e as disputas que surgem nesse escopo devem ser enquadradas exclusivamente sob os regimes de responsabilidade do produto.

2. DAS REFLEXÕES E EXPERIÊNCIA DA COMUNIDADE EUROPEIA

O Parlamento Europeu aprovou em 16/02/2017, a resolução número 2015/2103 sob o título "*Regras de Direito Civil sobre Robótica*", como uma possível resposta aos diversos desafios legais e complexos que há pela frente.

Essa resolução expõe a necessidade de salvaguardar e proteger a saúde dos pacientes.

Um dos países europeus que parece estar ciente da necessidade de repensar as regras clássicas de responsabilidade no escopo da IA para soluções na área da saúde é o Reino Unido, no qual conduziu uma análise profunda sobre o assunto, trazendo para o debate todos os envolvidos: acadêmicos, profissionais jurídicos, desenvolvedores e fabricantes de tecnologia, instituições de saúde etc.

No relatório final, menciona-se a necessidade de ação em quatro áreas-chave: a) Responsabilidade legal – a base sobre a qual a responsabilidade legal pode ser estabelecida em relação a uma inteligência artificial tecnologia; b) Questões de causalidade e responsabilidade - a base para determinar qual parte deve ser considerada responsável (ou está preparado para aceitar a responsabilidade) pela inteligência artificial, que não executar como esperado; c) Uso de IA na tentativa de executar ou cumprir com as obrigações legais existentes; e d) Status legal - até que ponto um status legal deve ser concedido a um AI.[3]

Apesar dos esforços da comunidade Europeia em regular o setor, não há legislação específica que lide com responsabilidades decorrentes da utilização da IA para fins de diagnóstico da saúde. Portanto, *a priori*, essas situações serão regidas pelas regras de cada Estado-Membro, de acordo com o especificidades do caso.[4]

Na realidade, as comunidades jurídicas e científicas na Europa ainda estão discutindo se a responsabilidade decorrente do uso da IA deve ser regulamentada ou estar apenas sujeita às leis de cada Estados-Membros têm

---

[3] UK's Parliament, *Select Committee on artificial intelligence collated written evidence volume - House of Lords(UK)* - Statement of Cooley (UK) LLP (written evidence AIC0217) *available on* https://www.parliament.uk/documents/lords-committees/Artificial-Intelligence/AI-Written-Evidence-Volume.pdf

[4] Andoulsi, Isabelle and Wilson, Petra *Understanding Liability in eHealth: Towards Greater Clarity at European Union Leve*" in George, Carlisle; Whitehouse, Diane and Duquenoy, Penny *eHelath: Legal, Ethical and Governance Challenges*, Springer 2013

atualmente em vigor, como privacidade e proteção de dados, proteção, dispositivos médicos, leis de responsabilidade civil ou criminal, entre outras.

Vale ressaltar que produtos e serviços que possuem o escopo de fornecer cuidados com a saúde são, normalmente, elaborados sob rígidas normas de controle de qualidade, considerando o objetivo de garantir que sejam seguros e eficientes, além de resguardar que os dados gerados pelas ferramentas utilizadas sejam precisos e confiáveis.[5]

Nesse sentido, os atores envolvidos no setor da saúde normalmente estão sujeitos a leis rígidas em diversos países no mundo, inclusive no Brasil.

Todavia, os legisladores não podem ignorar o fato de que regulamentações excessivamente rígidas e com regimes desproporcionais de responsabilidades sobre desenvolvedores e fabricantes de tecnologia poderão sufocar a inovação e o desenvolvimento de IA para fins de assistência médica[6], e que regimes de responsabilidades pesadas aos médicos que utilizam a tecnologia poderão comprometer a aceitação dos sistemas de suporte às decisões clínicas pela comunidade médica.

Portanto, a elaboração de um regime de responsabilidade eficiente exige um equilíbrio entre a proteção do consumidor e a rentabilidade industrial[7], o que significa que o desenvolvimento da tecnologia deve ser estimulada sem comprometer a segurança do paciente.

Determinar e alocar claramente a responsabilidade neste domínio é um assunto que deve ser considerando, tendo em vista que a tecnologia da IA está se tornando crucial no campo da medicina.

---

[5] Tsang, Lincoln; Kracov, Daniel A.; Mulryne, Jacqueline; Strom, Louise; Perkins, Nancy; Dickinson, Richard; Wallace, Victoria M. and Jones, Bethan *The Impact of Artificial Intelligence on Medical Innovation in the European Union and United States*, available on https://www.arnoldporter.com/~/media/files/perspectives/publications/2017/08/the-impact-of-artificialinteelligence-on-medical-innovation.pdf

[6] Petit, Nicolas *Law and regulation of artificial intelligence and robots: conceptual framework and normative implications*, available on https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2931339

[7] Lenardon, Joao Paulo de Almeida *The regulation of artificial intelligence* available on http://arno.uvt.nl/show.cgi?fid=142832

Em primeiro lugar, os custos financeiros relacionados aos cuidados de saúde desempenham uma grande participação nas economias dos países em todo o mundo.

Esta é a razão pela qual existe um interesse óbvio na adoção de tecnologias que permitam reduzir os custos recorrentes a ferramentas que economizem o tempo do profissional da saúde ao diagnosticar pacientes ou prescrever tratamentos. Além disso, essas ferramentas de suporte de decisões têm o potencial de reduzir ou totalmente eliminar custos decorrentes de erros de diagnóstico; custos relacionados com a realização de exames médicos adicionais; ou custos relacionados à prescrição de tratamentos que poderiam ter sido poupado se um diagnóstico preciso tivesse sido feito em um estágio anterior da doença.[8]

Tecnologias avançadas na área de diagnóstico médico podem, de fato, permitir que os pacientes recebam planos de tratamentos mais eficientes e que, oportunamente, os levem a melhores taxas de sobrevivência e qualidade de vida.

De fato, os sistemas de suporte à decisões médicas são um exemplo de que as sociedades atuais estão passando de um paradigma clássico de diagnóstico médico para a adoção de soluções de saúde eletrônica, recorrendo a tecnologias da informação através da IA para fins de diagnósticos, circunstância esta que acentuam a necessidade de discutir as possíveis responsabilidades ao caso concreto.

3. RESPONSABILIDADE DECORRENTE DA USO DA INTELIGÊNCIA ARTIFICIAL PARA FINS DE DIAGNÓSTICO MÉDICO E A ESCOLHA DO TRATAMENTO: QUEM DEVE SER RESPONSABILIZADO EM CASO DE DANO À SAÚDE?

Mais do que simplesmente confiar em seu conhecimento técnico sobre a medicina, os médicos da atualidade são assistidos por máquinas (Ex. IBM Watson para o diagnóstico do câncer), que avaliam os dados clínicos

[8] Marr, Bernard The Amazing Ways How Artificial Intelligence And Machine Learning Is Used In Healthcare, available on https://www.forbes.com/sites/bernardmarr/2017/10/09/the-amazing-ways-how-artificial-intelligenceand-machine-learning-is-used-in-healthcare/#71eee5dc1c80 acesso em 20.07.2020

do paciente à luz dos dados aos quais o algoritmo foi alimentado, fornecendo um diagnóstico mais preciso e opções de tratamento mais seguras.[9]

Embora os benefícios por trás do uso dessas tecnologia serem inquestionáveis, também são inquestionáveis que esses paradigmas de saúde representem uma ruptura no relacionamento clássico entre as partes envolvidas na prestação de serviços de saúde.

Se, antes, um paciente que sofreu o dano no decurso de um diagnóstico ou tratamento errôneo facilmente identificaria o agente contra quem tomar as medidas cabíveis (o médico ou a instituição médica sob o qual o médico prestou os serviços de saúde), hoje, com o uso de ferramentas de IA, além do médico há outra entidade que pode causaram o dano, isto é, a saída do algoritmo que o médico seguiu.[10]

Nesse sentido, deve ser avaliado se as regras de imperícia devem ser moldadas e adaptadas a essa nova realidade ou se a intervenção dos sistemas de suporte às decisões clínicas interrompem a relação entre médico e paciente de maneira tão severa que as regras de negligência médica deverão ser desconsideradas e as discursões que surgem nesse ponto deverão ser analisadas exclusivamente sob a responsabilidade do produto.

O conceito de negligência médica é essencial no objeto de definir a responsabilidade decorrente do uso da IA, considerando que é necessário avaliar se os erros médicos no diagnóstico e a escolha do tratamento realizado pelos profissionais ao seguir a saída de um algoritmo deve ser considerado negligência.

Nas palavras de JASON CHUNG, "negligência médica se aplica quando um médico é negligente em não cumprir os padrões profissionais da medicina e, como resultado, fere um paciente o direito a recuperar os danos".[11] Nesse sentido, a fim de fundamentar com êxito uma má prática, o paciente lesionado deve demonstrar: (i) que o médico tinha o dever de cuidar da o paciente; (ii) que o réu não cumpriu com os padrões de atendimento aos quais foi obrigado; (iii) que um dano surgiu do comportamento do réu;

---

[9] VARELLA, Drauzio - https://drauziovarella.uol.com.br/videos/repensando-a-medicina-o-que-e-o-watson/ acesso 13.08.2024

[10] ANDOULSI, Isabelle and Wilson, Petra *op cit.*, p. 165.

[11] COX, Holly *Medical Device Software: Who Is Responsible When Something Goes Wrong?* available on https://ohiotiger.com/medical-device-software-defects/

e (iv) a existência de um nexo de causalidade entre o ato ou a falta de ação e o dano, havendo no caso, a responsabilidade subjetiva por erro médico.

Após a breve análise do conceito de negligência médica, deve ser avaliado se o conceito deverá ser amplo o suficiente para abranger situações em que os danos não resultaram diretamente de uma falha médica no diagnóstico ou na escolha do tratamento, mas no resultado da decisão médica ao seguir a saída dos algoritmos.

De fato, e como destacado por SHAILIN THOMAS, "existem leis de negligência médica para proteger pacientes, e como os algoritmos assumem um papel maior no processo de tomada de decisão médica, eles se tornarão um meio menos viável de policiar as decisões de diagnóstico e tratamento".[12]

Deve ser analisado que, sob as regras de negligência médica, o ônus da prova recai sobre o Reclamante - que, além de provar o dano, terá que provar que o dano surgiu como conseqüência de um descuido da prática médica, portanto, cabe ao paciente provar que o uso da tecnologia (que levou a uma determinada decisão médica) ficou abaixo do padrão de atendimento necessário.

Analisando sob esta ótica, os conceitos de erro médico poderão ser definidos como a falha de um plano de ação a ser concluída conforme o planejado (isto é, erro de execução) ou o uso de um plano errado para alcançar um objetivo (ou seja, erro de planejamento)[13] ganham maior relevância.

Na prática médica tradicional, o principal elemento para verificar se o comportamento do médico foi qualificado como negligente é a previsibilidade.[14]

---

[12] THOMAS, Shailin. 2017. "Democratized Diagnostics: Why Medical Artificial Intelligence Needs Vetting" *Originally published on September 22, 2017, on the Petrie-Flom Center for Health Law Policy, Biotechnology, and Bioethics Bill of Health blog.*

[13] LA PIETRA, L.; Molendini, Calligaris; Quattrin, R.; Brusaferro, S. *Medical errors and clinical risk management: state of the art* available on https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2639900/pdf/0392-100X.25.339.pdf

[14] LEWIS, Charles J. *Medical Negligence*: a practical guide, third Edition, Tolley 1995, p. 159

Em suma, apesar de não ser uma condição *sine qua no*, a previsibilidade dos riscos envolvidos na decisão médica é usada como um indicador de cuidados abaixo do padrão.

Na atualidade, esse requisito é desafiado pelo uso da IA, uma vez que, quando as decisões médicas são tomadas usando algoritmos de caixa preta, o modo de funcionamento da máquina é obscuro e o profissional é incapaz de entender até que ponto ou qual a probabilidade de obter uma saída errada.

No contexto da assistência médica, o uso atual da tecnologia da caixa preta traz preocupações adicionais, considerando que as decisões médicas não devem se basear em meios automatizados que os médicos não conseguem entender e nem os desenvolvedores de software explicar. Pode-se argumentar que a conformidade com o padrão de atendimento requer que o médico aplique a saída da máquina criticamente.

Vale ressaltar que o objetivo da utilização da IA é ampliar e aprimorar o conhecimento existente do médico e, não, substituí-lo. A última palavra deverá sempre pertencer ao médico; portanto, as reivindicações de negligência neste domínio devem seguir o conceito clássico de padrão de atendimento.

Por outro lado, deve-se concluir que o padrão médico de atendimento ao qual os médicos estão obrigados é limitado pelo estado da ciência médica e do conhecimento científico no momento do tratamento, o que significa dizer que se os médicos estão usando tecnologias que incluem algoritmos e meios de funcionamento que nem mesmo os projetistas e desenvolvedores da tecnologia conseguem entender, *a priori* - e a menos que, sob o padrão razoável médico, fosse previsível que o diagnóstico ou tratamento prescrito não atenda ao perfil do paciente – este não será considerado negligente e responsabilizado sob as regras de negligência, por ter seguido o resultado fornecido pelo algoritmo.

Diante essa nova perspectiva, há uma mudança significativa no escopo das ações de negligência, uma vez que a opacidade e imprevisibilidade dos algoritmos de IA desafiam o princípio da

responsabilidade subjetiva, segundo a qual os tribunais só podem compensar os danos decorrentes de lesões previsíveis.[15]

À luz das especificidades, NICHOLSON PRICE alega que, "quando a tecnologia de IA é utilizada no decurso de decisões médicas, na avaliação da conformidade com o padrão de cuidados - a fim de verificar se o médico deve ser responsabilizado - devem ser feitos sob níveis diferentes, de acordo com a gravidade ou o impacto do uso da tecnologia e as condições do paciente."

4. DAS IMPLICAÇÕES EM RESPONSABILIZAR OS MÉDICOS

Dentro este novo paradigma de tomada de decisões médicas baseado na tecnologia de IA, as avaliações médicas aplicáveis se tornam mais profundas e mais complexas.

Se a responsabilidade for transferida do desenvolvedor de tecnologia para o médico especialista que recorre as tecnologias, futuramente restará mais difícil a posição de justificar criticamente o diagnóstico ou curso de ação sugerido pela máquina ou quais os motivos pelo qual o médico desviou da produção da máquina.

Não obstante, padrões excessivamente rigorosos trazem obstáculos de aceitação dentro da comunidade médica.

Dentro deste novo paradigma de tomada de decisões médicas baseado na tecnologia de IA, a avaliação sobre se o médico cumpriu com os padrões de atendimento aplicáveis se tornam mais profundos e mais complexos.

Considerando as implicações mencionadas acima, alguns autores argumentam que, embora a responsabilidade quanto ao uso da IA na área da saúde devem ser alcançados - por meio da validação independente dos resultados algorítmicos e da qualificações dos desenvolvedores - tais responsabilidades não devem recair sobre o médico que utiliza a tecnologia,

---

[15] Stanford University *Artificial intelligence and life in 2030 one hundred year study on artificial intelligence – Report of the 2015 study panel*, September 2016 available on https://ai100.stanford.edu/sites/default/files/ai100report10032016fnl_singles.pdf Acesso 20.07.2020

mas sobre a instituição hospitalar dentro do qual o diagnóstico ou tratamento foi fornecido. [16]

De acordo com NICHOLSON PRICE,[17] embora o usuário ainda possa desempenhar um papel na avaliação do nível de risco quanto a utilização da tecnologia e na detecção de resultados errôneos, as instituições hospitalares devem garantir que os algoritmos - como um todo - sejam de alta qualidade de acordo com características mensuráveis.

Até este momento, o dever de cuidado como uma obrigação que cabe ao médico tem sido discutido, porém as instituições hospitalares também estão vinculadas a esse dever.

Na realidade, as empresas de saúde também possuem o dever de cautela com os pacientes, portanto, podem estar sujeita as reivindicações de responsabilidade.

De fato, os hospitais têm o dever de fornecer instalações adequadas para o atendimento ao paciente, incluindo equipamentos operacionais necessários para os cuidados com o paciente. [18]

Nesse sentido, as instituições médicas podem ser responsabilizadas direta ou indiretamente, em analogia as reivindicações negligentes contra os médicos, também haverá um padrão a ser lembrado, o padrão de um hospital razoável.

Ao abordar essa questão, deve-se referir que os hospitais normalmente não são responsáveis pelo uso de dispositivos defeituosos, no entanto, se for demonstrado que os hospitais foram negligentes na avaliação do software de IA e que havia um falha em garantir que os algoritmos nele incluídos não atendiam a alta qualidade e segurança mínima, os hospitais podem ser responsabilizados no caso de danos à saúde causados por falhas do sistema que levou a um diagnóstico errado ou escolha de um tratamento inadequado.

Nos Estados Unidos essa visão foi endossada por várias doutrinas sob o qual os tribunais têm mantido cada vez mais hospitais responsáveis

---

[16] PRICE, W. Nicholson Medical Malpractice and Black-Box Medicine available on https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2910417 Acesso 23.07.2020

[17]PRICE, W. Nicholson Medical Malpractice and Black-Box Medicine available on https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2910417 Acesso 23.07.2020

[18] Idem.

pelo não cumprimento dos padrões de segurança no escopo da adoção de equipamentos de saúde ou dispositivos de qualquer natureza. Subjacente a essas doutrinas que envolvem responsabilidade corporativa está a idéia que entre um autor inocente e réus negligentes, estes devem arcar com o custo de lesão.[19]

A responsabilidade dos hospitais nas circunstâncias descritas também pode ser fundamentada no fato de que, embora os hospitais não sejam capazes de garantir que todas as decisões clínicas tomadas por seu corpo médico estejam corretas, existe o dever de garantir que os médicos que prestam serviços na instituição sejam razoavelmente proficiente.[20]

Desse dever, duas implicações podem ser descritas. Em primeiro lugar, um paralelo pode ser traçado entre a escolha do corpo médico e a escolha da ferramentas de tecnologia da informação para concluir que os hospitais são realmente responsáveis em relação à seleção dos recursos (humanos ou não humanos) utilizado dentro de suas instalações.

Em segundo lugar, o dever de contratar médicos com proficiência razoável, pode equiparar a existência de um dever de preparar adequadamente os médicos para usarem a tecnologia em suas dependências, portanto, cabe a responsabilidade dos hospitais por erros médicos causados pelo uso inadequado do diagnóstico e ferramenta de AI de tratamento.

5. REFERÊNCIAS BIBLIOGRÁFICAS:

ANDOULSI, Isabelle and Wilson, Petra Understanding Liability in eHealth: Towards Greater Clarity at European Union Leve" in George, Carlisle; Whitehouse, Diane and Duquenoy, Penny eHelath: Legal, Ethical and Governance Challenges, Springer 2013

CHUNG, Jason**.** "What Should We Do About Artificial Intelligence in Health Care?" New York University, 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3113655 acesso 15.07.2024

CORREA. Adriana Espíndola. Reflexão sobre as potencialidades da informação como tutela da autonomia privada no âmbito contratual. Revista

[19] Price, W. Nicholson *op. cit.*

[20] Price, W. Nicholson *op. cit.*

da Faculdade de Direito da Universidade Federal do Paraná, Curitiba, v. 35, p. 121-133, 2001.

CORDEIRO, A. Barreto Menezes. Direito da proteção de dados. Coimbra: Almedina, 2020.

COVENTRY, Linne; BRANLEY, Dawn Beverley Branley. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, [S.l.], v. 103, p. 48-52, jul. 2018.

COX, Holly Medical Device Software: Who Is Responsible When Something Goes Wrong? available on https://ohiotiger.com/medical-device-software-defects/

DALLARI, Analluza Bolivar. Impactos da LGPD na saúde suplementar e a aprovação do parecer sobre MP 869/2018. Consultor Jurídico, 07.05.2019. Disponível em: [www.conjur.com.br/2019-mai-07/analluza-dallari-impactos-lgpd-saude-suplementar]. Acesso em: 10.08.2024.

DATOS MOVING CARE FOWARD. The world's first provider of a field-proven Remote Care Telemedicine that is already in use in Israel and in the USA. Disponível em: [www.datos-health.com/coronavirus/]. Acesso em: 09.04.2020.

DAVIS, Jessica. 30 percent of online health databases expose patient data. Health IT Security, 12 dez. 2018. Disponível em: [https://healthitsecurity.com/news/30-percent-of-online-health-databases-expose-patient-data]. Acesso em: 10.04.2020.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

EUROPEAN COMMISSION. Towards a thriving data-driven economy. Communication from the commission to the European Parliament, the council, the European economic and social Committee and the committee of the regions. Bruxelas, 2014.

EUROPEAN UNION. Market study on telemedicine. Luxemburgo: Publications Office of the European Union, 2018.

FARIA, Paula Lobato de; CORDEIRO, João Valente. Health data privacy and confidentiality rights: Crisis or redemption? Revista Portuguesa de Saúde Pública, Lisboa, v. 32, n. 2, p. 123-133, jul./dez. 2014.

GARCIA, Lara Rocha. Inovação tecnológica e direito à saúde: aspectos jurídicos, econômicos, tecnológicos e de políticas públicas. Curitiba: Juruá, 2017.

GIDDENS, Anthony. Modernity and self-identity: self and society in the late modern age. Cambridge: Polity Press, 1991.

LA PIETRA, L.; Molendini, Calligaris; Quattrin, R.; Brusaferro, S. Medical errors and clinical risk management: state of the art available on https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2639900/pdf/0392-100X.25.339.pdf acesso 10.08.2024

LENARDON, Joao Paulo de Almeida The regulation of artificial intelligence available on http://arno.uvt.nl/show.cgi?fid=142832

MARR, Bernard The Amazing Ways How Artificial Intelligence And Machine Learning Is Used In Healthcare, available on https://www.forbes.com/sites/bernardmarr/2017/10/09/the-amazing-ways-how-artificial-intelligenceand-machine-learning-is-used-in-healthcare/#71eee5dc1c80 acesso em 20.07.2020

PEREIRA, André Gonçalo Dias. O consentimento informado na relação médico-paciente: estudo de direito civil. Coimbra: Coimbra Editora, 2004.

PETIT, Nicolas Law and regulation of artificial intelligence and robots: conceptual framework and normative implications, available on https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2931339

PRICE, W. Nicholson Medical Malpractice and Black-Box Medicine available on https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2910417 Acesso 23.07.2020

SCHWAB, Klaus. A Quarta Revolução Industrial. Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016.

Stanford University Artificial intelligence and life in 2030 one hundred year study on artificial intelligence – Report of the 2015 study panel, September 2016 available on https://ai100.stanford.edu/sites/default/files/ai100report10032016fnl_singles.pdf Acesso 20.07.2024

THOMAS, Shailin. 2017. "Democratized Diagnostics: Why Medical Artificial Intelligence Needs Vetting" Originally published on September

22, 2017, on the Petrie-Flom Center for Health Law Policy, Biotechnology, and Bioethics *Bill of Health* blog.

TSANG, Lincoln; Kracov, Daniel A.; Mulryne, Jacqueline; Strom, Louise; Perkins, Nancy; Dickinson, Richard; Wallace, Victoria M. and Jones, Bethan The Impact of Artificial Intelligence on Medical Innovation in the European Union and United States, available on

https://www.arnoldporter.com/~/media/files/perspectives/publications/2017/08/the-impact-of-artificialinteelligence-on-medical-innovation.pdf acesso 20.07.2020

UK'S PARLIAMENT, Select Committee on artificial intelligence collated written evidence volume - House of Lords(UK) - Statement of Cooley (UK) LLP (written evidence AIC0217) available on https://www.parliament.uk/documents/lords-committees/Artificial-Intelligence/AI-Written-Evidence-Volume.pdf Acesso em 13.08.2024

THOMAS, Shailin. 2017. "Democratized Diagnostics: Why Medical Artificial Intelligence Needs Vetting" Originally published on September 22, 2017, on the Petrie-Flom Center for Health Law Policy, Biotechnology, and Bioethics *Bill of Health* blog.

VARELLA, Dráuzio https://drauziovarella.uol.com.br/videos/repensando-a-medicina-o-que-e-o-watson/ acesso 13.08.2024

RESPONSABILIDAD CIVIL E INTELIGENCIA ARTIFICIAL

Por Silvina María Chaín Molina[1]

I. CONCLUSIONES

1. Legitimación pasiva por uso de bienes con IA. *De lege lata:* Son legitimados pasivos, responsables por los daños producidos por cualquier obra intelectual o material realizada con el uso de la INTELIGENCIA ARTIFICIAL (generativa o máquinas automáticas de cualquier tipo), tanto el autor de las mismas (arts 51 a 55 bis, 71 y 72 ley 11723); como además, en caso de corresponder, todos los intervinientes en la cadena de producción y comercialización en el sistema de la Ley de Defensa del Consumidor (art 2 LDC). Es decir que son legitimados pasivos el autor, desarrollador, fabricante (productores) y los integrantes de la cadena de comercialización (proveedores).

2. Robots. *De lege ferenda:* La responsabilidad del uso de robots (inteligentes o no), se determina conforme a las normas que rigen la responsabilidad por daños producidos con las cosas o actividades, sean peligrosas o no, y por tanto con un criterio de responsabilidad objetiva o subjetiva respectivamente. Si la comercialización de estos robots se encuentra alcanzada por la ley de Defensa del consumidor, se habilita la aplicación de estas normas estatutarias. Las máquinas por más complejo que sea su programación o más se asemeje su servicio al del razonamiento humano, nunca pueden considerarse personas, y siempre debe proveerse una instancia revisora humana.

3. Imagen generada con IA. *De lege lata:* Respecto a la responsabilidad civil por utilización indebida de la imagen mediante el uso de INTELIGENCIA ARTIFICIAL, la misma se encuentra delimitada por los arts 53 CCC (derecho a la imagen del propio interesado, así como el de sus herederos por 20 años, con las excepciones q prevé el artículo); y el art 31 ley 11723 (fotografías). Tanto el daño patrimonial como el daño moral o extrapatrimonial serán resarcidos conforme al régimen propio de cada tipo de daños.

---

[1] Dra en Ciencias Jurídicas por la UNLP. Docente Titular de Derecho Civil II – Obligaciones UCSE – DASS. Autora de "Obligaciones Civiles y Comerciales en el nuevo Código". Ed Advocatus. Córdoba. 2019 (3 tomos: Clasificación de las Obligaciones y Extinción de las Obligaciones).

4. Propiedad intelectual y derecho autoral. *De lege lata:* La utilización de la INTELIGENCIA ARTIFICIAL que infrinja los derechos de autor, hace responsable al usuario, de las sanciones impuestas por la ley 11723, ley 24766 (confidencialidad de los productos), ley 24481 (patentes de invención sólo si fuese aplicable por tener aplicabilidad industrial), 25156 (defensa de la competencia), ley 26338 (delitos informáticos). De lege ferenda: Respecto a los derechos de autor en la actividad académica, o evaluación de los alumnos en el nivel de la Educación Superior, se deben regular los espacios en donde se permite el uso de la IA, estableciendo mecanismo de detección de su uso, o permitiéndolo en determinadas instancias o porcentajes, a fin de garantizar el aprendizaje y evitar la competencia desleal entre los distintos establecimientos educativos.

5. Protección del software. *De lege ferenda:* Se propone la regulación de la protección del software y de los sistemas expertos e inteligentes de manera específica, independientemente de los preceptos contenidos en la ley 11723.

II. FUNDAMENTOS

1. DERECHO E INTELIGENCIA ARTIFICIAL

a) Derecho e informática. Ciencia Informática y de las Comunicaciones. Impacto en la Filosofía del Derecho

Parafraseando a Levene y Chiaravalloti, "a lo largo de la historia, el hombre ha necesitado transmitir y tratar la información de forma continua. Aún están en el recuerdo las señales de humo, los destellos con espejos, y ,ás recientemente los mensajes transmitidos a través de cables utilizando el código Morse, o la propia voz por medio de teléfono" [2]

Ahora bien, el paso dado con la escritura, ya esencial, aceleró enormemente el adelanto en las comunicaciones con la imprenta, con un salto gigantesco ya que permitía a la escritura difundirse con amplitud

[2] LEVENE, Ricardo (nieto) Y CHIARAVALLOTI, Alicia.-DELITOS INFORMATICOS(PRIMERA PARTE)(LA LEY 1998-E, sec.doctrina)

mayor: tanto cualitativa (rapidez de la grafía), como cuantitativamente (por el número de ejemplares a distribuir de una sola vez).

Actualmente sin embargo la agilidad dada a las comunicaciones por uso de la tecnología informática ha deslucido totalmente los antes citados pasos. Daniel Altmark comenta que fue la Academia de Ciencias francesa la que intentó, en 1966, una primera definición, sosteniendo que "informática es la ciencia del tratamiento sistemático y eficaz, realizado especialmente mediante máquinas automatizadas, de la información, contemplada como vehículo del saber humano y de la comunicación de los ámbitos técnico, económico y social"[3].

Evidentemente a pesar de ser conceptos diferentes, en la actualidad la informática y las comunicaciones son convergentes, según esta sencilla explicación: La "información" es una verdad "comunicable" con mayor o menor extensión, conforme a la esencia de cada dato. Evidentemente hay datos cuya divulgación, en cambio, puede ocasionar un daño o bien, constituye un delito.

Entonces surge una pregunta inevitable: ¿Qué es un dato?. El análisis no es fácil. El dato es una verdad en tanto destinada a ser conocida. Es decir, los datos son aseveraciones que constituyen el conocimiento de algo.

Dato viene de la raíz latina datum o dare, que significa "dado". Es la misma verdad sobre algo la que puede ser mirada como "dato", cuando se lo hace bajo el aspecto de objeto formal de las Ciencias Informáticas -de la Información- o Comunicación cuando el dato conocido es a su vez "comunicable", lo que se seguirá de la esencia de tal verdad.

La rapidez de estas operaciones es notoriamente mayor, con un empequeñecimiento igualmente mayor de los equipos aptos para transmitir o interrumpir la energía conductora de los datos o información. De los viejos y enormes computadores -por el mayor tamaño de relès, transistores y válvulas de vacío como transmisores o interruptores de energía- se ha pasado a la diminuta dimensión de los chips capaces a su vez de almacenar incomparablemente mayor cantidad de datos. La Informática en tanto vía

[3] ALTMARK, Daniel: La etapa precontractual en los contratos informáticos. Depalma. 1987 (Informática y Derecho. Tomo 1, pág 6).-

eficiente de comunicar datos, o instrumento necesario de la comunicación eficiente y eficaz., se denomina TELEMATICA o informática comunicable.

Informática (o computadoras), sistemas y cibernética, no son lo mismo, aunque actualmente todos estos términos se intenten vincular inexorablemente a máquinas u ordenadores: informática -vocablo originado en el idioma francés a partir de "information" y "automatique" -que en el lenguaje cotidiano también se lo llama computación- "se usa asimismo para la parte de la electrónica relativa al desarrollo técnico y a la construcción de computadoras" y especialmente la construcción de los programas necesarios para su funcionamiento.

Sistema, en tanto, es el "conjunto de reglas o principios sobre una materia enlazados entre sí" . Por último, cibernética es la disciplina que estudia los sistemas de control y comunicación de animales o máquinas. La cibernética intenta reproducir electrónica o electromecánicamente funciones orgánicas.

b) Inteligencia Artificial (IA). Clasificaciones

b.1- Informática Jurídica: Es la Ciencia de la Informática como herramienta del Derecho. Losano, arrancando de una etapa o clasificación anterior o más abarcativa, divide a la iuscibernética -entendemos y traducimos como cibernética jurídica- en dos corrientes: la modelística -con orientación predominantemente teórica - y la informática jurídica - de corte más empírico -(Guibourg) . Esto es, ubica a la Informática-Jurídica, dentro de la iuscibernética.-

La informática jurídica busca aplicar al derecho la lógica y otras técnicas de "formalización", con vistas al empleo de los medios electrónicos y procura adquirir las técnicas adecuadas para aplicar la acción de los ordenadores al campo jurídico.

La clasificación más utilizada distingue tres subespecies de informática jurídica: la documental, la de gestión y la decisoria.

Rafael A Bielsa, por su parte, sostiene que la clasificación es bipartita: Informática jurídica-documental y de gestión, pero particiona a ésta última en tres niveles: 1) el de la informática operacional; (se ocupa de diligenciar la documentación producida dentro del ámbito de la actividad judicial); 2) el de la informática registral; (retiene y actualiza permanentemente la información histórica); 3) el de la informática decisional; (actúa sobre los modelos abstractos elaborados a partir de la base

de los datos de los registros a fin de poder preveer comportamientos frente a varias posibilidades) .

Todos citan a la lógica como ciencia auxiliar primera, por cuanto la máquina, al ser también capaz de inferir conclusiones -siempre en base a los programas y datos que contenga según dijimos-, lo hace en base a una lógica matemática: como ya se dijo, el lenguaje que a través de la programación se introduce en ellas, sistematizando su funcionamiento, consiste en instrucciones aptas para asimilarlas mediante energía eléctrica, a través del sistema binario que, al igual que los polos positivos y negativos de la energía, está integrado por sólo dos caracteres: 0 y 1. Esto es, que la máquina, no responde a "razonamientos" humanos. El hombre, razona sin tales barreras: el raciocinio del hombre (incluye su voluntad y libertad) que no sólo abarca la dimensión matemática sino además, la física y filosófica o por las causas últimas. Por último, la libertad es ínsita al hombre, que puede variar –por ejemplo, por conveniente, por utilidad e incluso por error o con malicia- un resultado por perfecto que parezca.

Comenta Guibourg, la importancia de comprender que se trata de sistemas informáticos que funcionan electrónicamente mediante el sistema binario de 0 y 1 para decodificar las cargas positivas y negativas propias de la electricidad.

b.2- Sistemas Expertos: Resulta recomendable conocer el funcionamiento tecnológico de las máquinas, tratando de que nos sean comprensibles los software para empresas, bases de datos, bases de datos relacionales, procesadores de textos, hojas de cálculo, contabilidad, computadores e imágenes, procesamiento de imágenes, cuadros mediante números, dibujos animados, gráficos de tres dimensiones, la visión de los computadores, computadores que hablan, computadores dirigidos por la voz, sensores, sensores a distancia, velocidad y aceleración. Como avance de esta tecnología se habla de Inteligencia Artificial, como la capacidad de un sistema informático para reproducir alguna de las funciones de la inteligencia humana

Algunos explican la inteligencia artificial circunscripta a la resolución de problemas como lo haría un experto en la materia, de allí se conocen estos procedimientos "Sistemas Expertos" en los que la máquina lejos de razonar o decidir almacena datos, los asocia en razón de un programa que se le formula al efecto y arroja matemáticamente los resultados a los que arriba, y suponen una representación del conocimiento y un motor inferencial como brevemente se explicara al tratar la Informática

Decisoria. La última tecnología ha incluso puesto su mira, en intentar que las máquinas puedan "aprender" de la realidad por el método del acierto y del error, es decir, a través de la comparación de los distintos caminos intentados por la máquina para resolver un tema. Esto excede el mero método de inferencias de la Inteligencia Artificial del llamado Sistema Experto .

Sin embargo, no son automatizables las decisiones personales, así como tampoco "las interpretaciones de la jurisprudencia y aun, en buena medida, la resolución de aplicar normas sobre inconstitucionalidad, abuso del derecho o lagunas", elementos que tales autores indican como dependientes de otros criterios que se encuentran en la formación moral y profesional del magistrado, atribuyéndoles correspondencia con la programación ignota, que hacen absolutamente aleatorias las decisiones judiciales .

Otra corriente pretende validar -como preferente al parecer-, el juicio de máquina, pues no cae en los "errores humanos". Obviamente habremos de disentir. Al respecto cabe aclarar que entendemos que el conocimiento implica una operación gnoseológica propia del intelecto -facultad superior del hombre-, en tanto apetito apto para descubrir lo real en tanto "verdadero", del mismo modo que la voluntad –otra facultad espiritual del hombre- adhiere a esa misma realidad que en tanto es conocida como verdadera, se le presenta como "buena". Esta es la facultad u operación "crítica" del hombre que no ha de responder a subjetivismos sino a la humildad intelectual que busca "desvelar" lo real. En este proceso intervienen además, la afectividad y emociones humanas, de la que la máquina carece en absoluto. Como puede verse, esta operación no tiene nada que ver con las opciones derivadas del sistema matemático binario propio de la máquina.

Por último, dijéramos que el Derecho, en tanto Ciencia que tiene por objeto material conducta humana -que comparte con la Psicología, moral, sociología- , la estudia desde el punto de vista del deber ser en una relación de alteridad –objeto formal o aspecto desde el que se aborda caracterizada por la libertad que es esencial y connatural a la dignidad del hombre-. Por tanto, resulta aplicable para su estudio un método científico apropiado –inductivo-deductivo-, distinto al de las ciencias naturales o las ciencias exactas, cuyas leyes son de cumplimiento inexorable y no libre. Los sistemas expertos, no pueden definir adecuadamente leyes conductuales, en las que a idénticas circunstancias, puede el hombre reaccionar de diferentes maneras.

Ejemplo de una posible falencia en el método escogido es la aplicación en el Derecho de métodos matemáticos, que, en tanto se pretenda aplicar la ley general al caso particular a través de medios automáticos sin una revisión humana de tal procedimiento, puede resultar una solución obviamente injusta.

b.3- Diversas clasificaciones acerca de la I.A.

De manera muy sucinta, y según el Diccionario de la RAE, la INTELIGENCIA ARTIFICIAL es la "disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico".

Es decir que supone una máquina electrónica que, mediante la ejecución de un software de esta complejidad, consigue generar y entrecruzar datos, o bien los ordena de manera tal que la misma máquina ejecute acciones automáticas, éstas últimas, con mayor o menor independencia de la intervención humana.

Básicamente se denomina IA GENERATIVA a la tecnología del primer tipo (generación de datos, imágenes, información entrecruzada, emulación, emisión de dictámenes decisorios o toma de decisiones, reconocimiento de voz y búsqueda, agentes de juego estratégico, etc); y se denomina IA DE AUTOMATIZACIÓN a las de la segunda clase (máquinas automáticas que imitan las capacidades humanas o machine learning). Existen otras clasificaciones: a) IA supervisada o no supervisada por el ser humano; b) de learning o aprendizaje superficial o profundo (imitación de red neuronal); c) según sea su funcionamiento (mediante reglas, datos superficiales, redes neuronales, algoritmos genéticos y de evolución (IA evolutiva), de procesamiento del lenguaje (Siri, GPT), o mediante razonamiento o toma de decisiones (IA cognitiva).

c) Robótica e inteligencia artificial

En este punto hemos de distinguir a los *autómatas, robots, androides y humanoides*[4]. La enunciación va de los más básicos capaces sólo de operaciones automáticas como una lavadora de autos, a las más sofisticadas, como es el caso de los robots inteligentes, capaces de sentir (recoger datos

[4] COSOLA, Sebastián Justo y SCHMIDT, Walter César: "El Derecho y la Tecnología". La Ley. BsAs. 2021; Tomo II, pág 314.

de la realidad mediante el uso de sensores), pensar (procesar aquellos datos) y actuar (sobre esas bases establecer una respuesta de acción o inacción). Por ejemplo un robot que ayude a una persona ciega a transitar las calles y llegar a destino, mediante un gps, un reconocimiento de semáforos con sensores que capten los colores rojo, amarillo y verde, y que por tanto avance o se detenga para llevarlo sano y salvo a destino (tal vez incluso pueda haber preparado el desayuno antes de que salga de su domicilio). De allí para nosotros la distinción entre las variantes consignadas al inicio del presente párrafo, mezcla criterios clasificatorios pues podríamos decir que las máquinas inteligentes pueden ser autómatas –cuando imitan un comportamiento animado- o inteligentes; y desde otro punto de vista, los robots pueden tener aspecto humanoide o además comportarse imitando al humano como en el caso de los androides.

Los autores consideran necesaria la distinción con el propósito de no restringir el concepto de robot a aquellos con figura humana o humanoides según lo imaginado por Karel Capek e Isaac Asimov, según el mito de Pigmalión.

El interrogante jurídico se cierne en torno a indagar si el robot está programado para ayudar a una persona a tomar una decisión, sustituir su voluntad o servirle de apoyo ante su capacidad restringida? Concluyen los autores indicando que no existe regulación en nuestro Derecho, si bien en la Comunidad Europea, el Parlamento, mediante resolución del 16/2/2017 estableció recomendaciones a la Comisión de Derecho Civil para comenzar a considerar y distinguir robots con capacidad para funciones específicas (autos autónomos), de los que poseen inteligencia artificial con Deep learning, y reconociéndoles a los robots un status particular de persona o personalidad.

Finalmente Cosola y Schmidt, respecto a los robots “inteligentes”, se plantean interrogantes jurídicos tales como: Qué es un fallo de programación? La negativa del robot a cumplir con mi solicitud se considera fallo de programación? Se pueden considerar que los daños producidos por robots inteligentes son de responsabilidad del fabricante, o bien del programador, o del usuario, o finalmente del dueño del robot? Se puede considerar al robot como “persona no humana”? Podríamos hablar de persona jurídica electrónica? Podemos predicar que tiene voluntad jurídica? Seria contrario a la ética considerar al robot como una cosa? Se puede asimilar su situación a la de un esclavo? Se puede ser ético explotando a una entidad inteligente bajo amenaza de “apagado-muerte”?

Actualmente se agregó el concepto de **Cyborg**, que supone un humano que pretende fusionarse con partes mecánicas que incluso mejoran la fisiología meramente humana (fusión cerebro-software-máquina). Se trata de la incorporación de dispositivos a los cuerpos humanos, que a su vez se vinculan con otros que se encuentran fuera del cuerpo humano transmitiendo o recibiendo datos; y por contrapartida, existen robots híbridos compuestos por elementos artificiales y controlados por un elemento orgánico (**Hybrot**).

Por último, los robots inteligentes son aquellos que además pueden tomar decisiones basadas en la lógica e inteligencia artificial, prediciendo necesidades humanas y sin estar sometidos al control de los últimos. En esta línea existen los robots operados manual o remotamente, los que contienen manipuladores automáticos, con trayectoria continua o punto a punto sin captar su entorno, los que sí pueden adquirir datos del entorno. Desde otro punto de vista, los mismos pueden manejarse manualmente, o bien ser programados con secuencias repetitivas invariables o variables –según puedan modificarse o no por un operador-, regeneradores o conducidos externamente, de control numérico y finalmente los robots inteligentes (algunos de los cuales poseen componentes electromecánicos, microscópicos –nanorobots-, xenorobots –transporte de medicamentos en el cuerpo humano con capacidades curativas-, softrobots –programas dentro de otros programas y por lo tanto no se materializan en cuerpos físicos-, y sirviendo de aplicación en los más diversos campos: ambiente, prótesis, salud y calidad de vida, militar (drones), educación, juguetes, entretenimiento, arte. En éste último punto, Cosola – Schmidt expone confusamente que en la exposición de Roboart se premiaron las mejores obras pictóricas realizadas mediante la inteligencia artificial *deep learning*. A partir de ello, cuestionan a quién pertenecen los derechos de autor: al robot, al programador, al dueño, al operador[5].

A cualquier efecto, y principalmente a fin de imputar responsabilidad civil, es que pasa a primer plano la pregunta de otorgar personalidad jurídica al robot.

Compartimos el postulado de que la personalidad es condición del atributo capacidad, y no al revés; toda vez que el actual criterio abierto y dinámico de la capacidad, cuestiona la sustitución de la capacidad de una persona y la reduce al mínimo posible.

---

[5] COSOLA –SCHMIDT, op cit. Vid nota al pie N°9.

Es decir que la persona humana es el centro de atención de la capacidad y de los derechos humanos, atributos sólo de aquellas; la protección de la persona humana frente al daño que pueda derivarse de medios tecnológicos, y desde que las obras creadas por el hombre –incluso cuando adquieran ciertas habilidades de autosustento o manejo, no pueden preferirse frente al único destino de la tutela jurídica, que está reservada al hombre; y que, ante el conflicto entre la persona humana y el robot, imponga preferir siempre al hombre. Cosola propone la denominación de "entes con intenligencia –sea de aprendizaje acotado o aprendizaje profundo-", en el último caso para el supuesto de contar con inteligencia artificial.

d) Conclusiones del Título

Respecto a los robots que cuenten con inteligencia artificial, no puede predicarse de los mismos, que estén dotados de voluntad (capacidad de elegir libremente, sino siempre se trata de una capacidad de decidir sólo entre las opciones programadas.

Los robots no poseen personalidad jurídica distinta de sus dueños o guardianes, por lo que pertenecen a la categoría de cosas. Dependiendo de las actividades de las que sean capaces, serán considerados cosas riesgosas o peligrosas. Se aplicarán en cada caso, las normas relativas a uno u otro supuesto.

2. RESPONSABILIDAD CIVIL POR EL USO DE LA INTELIGENCIA ARTIFICIAL. TUTELA DEL DERECHO DE PROPIEDAD INTELECTUAL Y DERECHO A LA IMAGEN

a) Legitimación pasiva

La INTELIGENCIA ARTIFICIAL (I.A.), pretende aproximarse al proceso de inferencias del razonamiento humano, o también de algoritmos genéticos (IA evolutiva), de procesamiento del lenguaje (IA propia de sistemas como SIRI, ALEXIA y GPT) o procesos que pretenden que la máquina toma de decisiones (IA cognitiva). Son legitimados pasivos responsables por los daños ocasionados con las cosas en los términos del art 1758 CCC, el dueño o guardián. Tratándose ya sea de **obras puramente intelectuales** como las realizadas con el uso de INTELIGENCIA ARTIFICIAL GENERATIVA de contenido, o bien de **cosas o máquinas automáticas** programadas mediante INTELIGENCIA ARTIFICIAL AUTOMATIZADA, en ambos casos involucran la utilización de "símbolos

y reglas" –tecnología simbólica-, redes de datos –máquinas automáticas- o "redes neuronales de entrecruzamiento de datos".

Ahora bien, podemos inferir, que el "dueño" de los datos o información generados con IA, es el autor, es decir el titular del derecho de propiedad intelectual (ley 11723). Sin embargo en caso de máquinas automatizadas o robots, el dueño es además, el titular del derecho real de esa máquina.

También la ley indica como responsable al "guardián". El art 1758 CCC estatuye que se considera tal, a quien ejerce por sí o por terceros, el uso, dirección y control de la cosa, o a quien obtiene un provecho de ella. Es por ello que, como corolario y en ambos casos (IA generativa de datos o máquinas automatizadas o con capacidad decisoria o inferencial), cabe la aplicación de las normas sobre licencias de uso del software, de donde el usuario integra el concepto de guardián.

En todo caso siendo la IA un software, se aplican a su tutela, las breves normas a que refiere la ley 11723 (arts 71 a 83). El sistema se ha considerado complementado por las siguientes leyes ley 24766 (confidencialidad de los productos), ley 24481 (patentes de invención sólo si fuese aplicable por tener aplicabilidad industrial), 25156 (defensa de la competencia), ley 26338 (delitos informáticos).

Careciendo nuestro sistema normativo de regulación específica de la tutela del software, de manera sucinta ha sido receptada la protección del "código fuente" y código objeto" en el art 1 de la ley 11723. En EEUU la protección del software se realiza como parte de la protección de patentes de invención, por no encontrarse requerida la utilidad industrial como sí lo exige nuestro sistema.

Sin embargo, si bien el impacto de la IA es exponencial en relación al riesgo autoral que antaño se diera con la creación de la Imprenta y la difusión de las ideas inicialmente también sin protección autoral, toca ahora profundizar en la especialización del tema mediante normas propias de la materia.

b) Ley de Defensa del Consumidor

Es pertinente la aplicación de la normativa correspondiente a la Defensa del Consumidor respecto a la producción y provisión de bienes con I.A., tanto de la ley específica (ley 24240 y modif 24787, 24999 –art 13 y 40 responsabilidad solidaria de productores, importadores, distribuidores y

vendedores-, 26361, 27077, 27250 e integrada por las leyes 25156 de defensa de la competencia y 22802 de lealtad comercial) como de las disposiciones del Código Civil y Comercial ley 26994, respecto a los contratos del tipo (arts 1092 a 1122 CCC).

c) De la tutela del Derecho a la imagen

Sin ahondar en el tema, excepto por su conexión con el objeto de este estudio, podemos indicar la previsión normativa que surge del art 31 de la ley 11723 (comercio de retrato fotográfico) , y del art 53 CCC (captación o reproducción de la imagen o la voz de una persona.

3. CONCLUSIONES

a) Tutela del software. Necesidad de ley específica para tutelar el uso de la inteligencia artificial.

b) La afectación del derecho a la salvaguarda de la imagen debe ser resarcido conforme a su régimen propio, tratándose de un daño extrapatrimonial sumado al recupero del lucro cesante o daños patrimoniales eventuales.

c) El Estado podría incurrir en responsabilidad civil por la falta de reglamentación del uso de la inteligencia artificial en exámenes en los distintos niveles educativos, siendo necesario que se establezcan condiciones de admisibilidad del uso de la inteligencia artificial en la educación a distancia.

d) La falta de servicio se configuraría por la falta de previsión normativa, y el daño positivo resultante de la competencia desleal en el marco de las evaluaciones a distancia realizadas por alumnos que utilicen ofertas de educación a distancia.

LA ACTIVIDAD DEL USUARIO DE LOS SISTEMAS DE IA COMO EXIMENTE DE RESPONSABILIDAD

Por María Celeste Colombo[1]

I. CONCLUSIONES

1. La actividad del usuario de sistemas de IA puede gravitar como eximente de la responsabilidad civil.

2. Se distingue entre el usuario profesional/*deployers*, y los usuarios finales.

3. La actividad de estos usuarios puede eximir a otros sujetos de responsabilidad ya sea parcial o totalmente si su conducta tiene incidencia causal en la producción del resultado dañoso.

4. En el caso de los usuarios finales, solo se configura en eximente la conducta que haya interferido sustancialmente en las condiciones de funcionamiento del sistema de IA, o bien cuando debidamente advertido (informado) no haya ejecutado una actualización crítica del sistema de IA.

II. FUNDAMENTOS

1. INTRODUCCIÓN

La creciente adopción de la inteligencia artificial[2] en diversas áreas de la sociedad ha generado un amplio debate sobre las implicaciones legales con relación a su uso. En especial, uno de los aspectos más cruciales es la responsabilidad civil derivada de los daños causados por sistemas de IA.

A medida que estas tecnologías se integran en nuestras actividades cotidianas, desde la conducción autónoma, asistentes conversacionales

---

[1] Abogada (UNC). Magister en Derecho Civil Patrimonial (UCA). Jefa de Trabajos Prácticos de la Cátedra de Obligaciones Civiles y Comerciales- Facultad de Derecho- UBA. Aval otorgado por Carla Kott, profesora adjunta de la Universidad Nacional de Buenos Aires.

[2] En adelante utilizaremos el término inteligencia artificial y la sigla IA indistintamente.

(LLMs), dispositivos telemáticos, etc; surge la imperiosa necesidad de establecer quién responde cuando un sistema de IA provoca daños.

Tradicionalmente, la responsabilidad civil se ha estructurado en torno a la figura de la culpa. Se ha escrito en piedra el lema "*no hay responsabilidad sin culpa*".

Actualmente, gran parte de los sistemas de responsabilidad civil tienen este corte subjetivista. En nuestro país, tras la adopción de la teoría del riesgo, hay una marcada predominancia de una responsabilidad objetiva.

Ahora bien, cuando hablamos de IA, determinar quién responde por el daño causado se vuelve una problemática por demás compleja. ¿Debe considerarse responsable al desarrollador del software, al fabricante del hardware, o al usuario que opera la IA?

La dificultad que plantea este dilema se agrava por la capacidad de los sistemas de IA para tomar decisiones autónomas e incluso para aprender de la interacción con su entorno, lo que a menudo los torna en impredecibles para los mismos proveedores, desarrolladores y/o usuarios.

El usuario de un sistema de IA, en muchas situaciones, se enfrenta al desafío de supervisar y controlar una tecnología que no solo puede operar de manera autónoma, sino que su comportamiento es imprevisible y evoluciona conforme su uso.

En la presente ponencia desarrollaremos el concepto de usuario profesional, para luego proceder a distinguirlo del usuario final. Finalmente, intentaremos abordar dos cuestiones: ¿en qué medida debe el usuario ser considerado responsable por el daño causado por la IA bajo su control? Asimismo, ¿la actividad del usuario de los sistemas de IA constituye una eximente de responsabilidad?

2. LA ACTIVIDAD DEL USUARIO EN LOS SISTEMAS DE IA

En un análisis más profundo sobre la responsabilidad de los sistemas de IA, encontramos que diversos sujetos pueden ser considerados legitimados pasivos. En efecto, dos o más actores pueden contribuir al daño

a través de sus acciones y ser considerados responsables, incluso si no es posible identificar la acción específica que causó el daño.[3]

Ahora bien, tradicionalmente cuando los bienes materiales o inmateriales son puestos a disposición del mercado, aun para aquellos bienes con algún elemento digital incorporado, podemos advertir que estamos a ante un objeto estático. Es decir, se trata de un producto que no sufre ningún cambio, permanece igual. Incluso su puesta en circulación deviene en un momento estático[4].

En el mundo 4.0, en cambio, cuando introducimos bienes y/o servicios que incorporan sistemas de IA, el momento de puesta en circulación de este producto digital se convierte en dinámico. Asimismo, los sistemas de IA son entidades en constante evolución, y que poseen la capacidad de tomar decisiones autónomas. Son entes cuyo comportamiento una vez que han ingresado al mercado escapa a la previsibilidad del proveedor, por lo que sufren cambios a lo largo de todo su ciclo de vida. Por otro lado, son objeto de actualizaciones sistemáticas, por lo que la actualización posterior no forma parte del momento temporal en que fue puesto en circulación.

En este contexto, la actividad desplegada por el usuario a lo largo del ciclo de vida del sistema de IA puede ser relevante para la causación del daño.

Así, dadas las características y complejidad de los sistemas de IA, se advierte un nuevo legitimado pasivo hasta ahora ajeno a la cadena de valor: los usuarios de los sistemas de IA.

Cuando hablamos de usuarios de los sistemas de IA hay que distinguir entre aquellos que los despliegan a nivel profesional, de aquellos que hacen un uso personal.

---

[3] Excede el marco de esta ponencia, pero entendemos que podemos incluir en el elenco de legitimados pasivos: a) proveedores/desarrolladores; b) usuarios profesionales/*deployers*; c) importadores; d) distribuidores; representantes autorizados, y fabricantes de productos.

[4] Ej: un auto, un teléfono móvil, un programa de software, etc.

El Reglamento de la Inteligencia Artificial de la Unión Europea[5] hace el distingo, en el art. 3.4 se refiere a los *deployers*, también denominados implementadores, responsables de despliegue[6], o usuarios profesionales[7].

A diferencia de los usuarios finales, los *deployers* son responsables no solo de la implementación técnica del sistema, sino también de las consecuencias legales de su uso. Esto los coloca en una posición similar a la del denominado "controlador de datos" del Reglamento General de Protección de Datos (RGPD), con obligaciones que van más allá del uso cotidiano y que incluyen aspectos como la formación del personal, la transparencia y la cooperación con las autoridades

El RIA[8] les impone la responsabilidad de garantizar que los sistemas de IA de alto riesgo se utilicen de manera segura y conforme a las normativas vigentes. Esto incluye realizar evaluaciones de impacto sobre los derechos fundamentales, asegurar la supervisión humana y mantener registros de las operaciones del sistema. Además, deben informar a las autoridades competentes en caso de incidentes graves relacionados con la seguridad o derechos fundamentales.

Los usuarios profesionales tienen el deber de realizar las evaluaciones de impacto sobre la protección de datos y, en algunos casos, se les exige publicar un resumen de estos hallazgos para garantizar la transparencia.

---

[5] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). Online: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R1689

[6] Responsable de despliegue es la traducción oficial en español hecha por la UE.

[7] A la par de los *deployers* el art. 3.3 ubica a los proveedores y los define como una persona física o jurídica, que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente.

[8] En adelante nos referiremos al Reglamento de Inteligencia Artificial europeo como RIA.

Esto refleja un enfoque proactivo hacia la mitigación de riesgos asociados con el uso de la IA, considerando el potencial que poseen las herramientas de IA para evolucionar y generar nuevos riesgos.

Como se podrá advertir, los responsables del despliegue de sistemas de IA toman un papel activo en la gestión de riesgos y en la garantía de cumplimiento normativo, lo que incluye la posibilidad de suspender del uso del sistema de IA si se detectan riesgos no mitigables.

Asimismo, vinculado con la alfabetización en IA, se debe garantizar que todo el personal que maneja sistemas de IA de alto riesgo para el *deployer* esté suficientemente capacitado y calificado.

En contrapartida tenemos a los usuarios finales. El RIA no conceptualiza a los usuarios finales, pero a partir del art. 3.4 del reglamento de IA podemos establecer una definición.

Se denomina *usuario final* a toda persona física o jurídica que utiliza un sistema de IA bajo su propio control, y en una actividad personal. Es decir, que utiliza el sistema de IA de manera no profesional.

En virtud de lo expuesto, ¿existe alguna relación entre usuarios profesionales y finales?

Entendemos que la vinculación entre *deployers* y usuarios finales se establece en el deber de seguridad que recae sobre los *deployers* − *obligación de seguridad* − para con los usuarios finales con quienes contrata.

Para finalizar, ¿qué obligaciones tiene sobre el usuario final?

En principio, utilizar los sistemas de IA conforme las instrucciones de uso de los desarrolladores y las recomendaciones de los *deployers*. No obstante, se impone un deber de información adecuado respecto del uso y consecuencias negativas de los sistemas de IA.

3. LA ACTIVIDAD DEL USUARIO DEL SISTEMA DE IA COMO EXIMENTE DE RESPONSABILIDAD

Antes de analizar la temática del presente apartado es necesario delinear algunas cuestiones con relación al hecho del damnificado y hecho de un tercero como eximentes de responsabilidad.

a) Hecho del damnificado

Nuestra normativa regula la incidencia del hecho del damnificado en la producción del propio daño. Así, el art. 1729 del CCyC establece que la responsabilidad se excluye o limita según el hecho haya sido causa exclusiva o concausa del daño[9].

La doctrina explica que en estos casos no parece razonable trasladar total o parcialmente las consecuencias a terceros, ya que la propia conducta del damnificado lo convierte en autor material del daño por él sufrido, y lo debe soportar en esa medida.

El hecho del damnificado se verifica cuando hay una incidencia causal en la producción del daño, el hecho de la víctima debe ser causa adecuada o concausa del daño. Asimismo, el requisito de culpabilidad del damnificado no es lo relevante, ni estrictamente necesario, si bien admite excepciones como cuando la ley o contrato dispongan la exigencia de la culpa o dolo de la víctima[10].

Ahora bien, si el hecho del damnificado es exclusivo de la causación de su propio daño exime de responsabilidad al demandado. En cambio, si concurren ambas conductas (víctima y dañador) las consecuencias dañosas se distribuyen conforme el porcentaje de incidencia causal de cada una de ellas en el resultado[11].

---

[9] ZAVALA DE GONZALEZ, Matilde, *La responsabilidad civil en el nuevo Código,* Tomo II- Ediciones Alveroni- Córdoba- 2016- pág. 229

[10] PIZARRO, Daniel, *Tratado de la Responsabilidad Objetiva*, Tomo I- La Ley- Buenos Aires, 2015, págs. 286/298. GAGLIARDO, Mariano, "*Culpa de la víctima: ¿siempre?*"- Publicado en: RCCyC 2021 (febrero), 173, Cita online: TR LALEY AR/DOC/4066/2020

[11] PIZARRO, Daniel, *ob.cit*., págs. 312/314.

b) Hecho de un tercero

"*El nexo causal se interrumpe, total o parcialmente, cuando se demuestra que el daño obedece al hecho de un tercero extraño por quien no se debe responder*"[12].

¿Quién es este tercero?, pues se trata de toda aquella persona extraña, es decir de distinta del demandado y de la víctima, que con su conducta provoca el resultado dañoso.

Para que se configure la eximente de estudio se deben dar una serie de requisitos, a saber: a) *incidencia causal*: se hace necesaria la autoría material en cabeza del tercero que se erige en causa o concausa de la producción del daño. En caso de concurrencia entre hecho de tercero y demandado, ambos deberán responder frente a la víctima; b) *hecho del tercero no imputable al demandado*: hay hecho de un tercero cuando la conducta del demandado es extraña al resultado dañoso; c) *el hecho de un tercero debe reunir los caracteres del casus*, es decir ser imprevisible, inevitable, sobrevenido, extraño al sindicado como responsable. Esta eximente se encuentra regulada en la ley de fondo en el art. 1731[13].

La carga de la prueba tanto en el supuesto del hecho del damnificado como para el hecho de un tercero es de quién la alega (art. 1734 C.CyC).

Ahora bien, resta analizar el *core* de la presente ponencia: la actividad del usuario de sistemas de IA como eximente de responsabilidad.

Junto a una serie de legitimados pasivos entre los que se destacan los desarrolladores y fabricantes, tenemos una categoría especial denominada *deployers*, implemetadores, responsables de despliegue y/o usuarios profesionales.

Lo que caracteriza a esta categoría es la utilización de los sistemas de IA con fines netamente profesionales. Básicamente, son aquellos sujetos que para el ejercicio de su actividad comercial y/o profesional hacen uso de herramientas de IA.

Así, pueden quedar incursos en esta categoría bancos, empresas de seguro, de transporte, empresas que prestan servicios tecnológicos, plataformas de e-commerce, incluso profesionales liberales.

---

[12] PIZARRO, Daniel, *ob. cit.,* pág. 318.
[13] PIZARRO, Daniel, *ob. cit*., págs. 322/324.

En el ámbito de la UE comprende todas aquellas organizaciones y/o personas físicas que implementen sistemas de IA de alto riesgo, lo cual impone a estos sujetos una especial responsabilidad a la hora de garantizar y supervisar el cumplimiento del RIA, y sobre todo un deber de prevención derivado del uso de sistemas de IA.

La RIA y la propuesta de Directiva sobre responsabilidad por inteligencia artificial[14] establecen una serie de obligaciones y deberes en cabeza de los responsables de despliegue de sistemas de IA.

Sin embargo, el problema está en determinar quién responde cuando un sistema de IA causa daños. Y en particular, cómo el demandado puede eximirse de responsabilidad alegando la actividad del usuario de sistema de IA.[15]

De este modo, entendemos que cuando el usuario profesional utiliza sistemas de IA para el desarrollo de su actividad puede ser considerado responsable, y eventualmente contribuir con su conducta total o parcialmente a la producción del resultado dañoso.

Quizás el problema sea determinar si su conducta se torna en causa adecuada para el resultado dañoso. O bien, corresponde hablar de culpa, es decir de falta de diligencia debida en los cuidados concretos que le son exigibles como sujeto que implementa sistemas de IA de modo profesional (*deployer*).

La propuesta de Directiva de Responsabilidad Civil de la IA considera responsable al usuario profesional que no cumple con su obligación de utilizar y/o supervisar el sistema de inteligencia artificial conforme con las instrucciones de uso suministradas por el proveedor. Igualmente, cuando omite suspender y/o interrumpir el uso; o bien expuso al sistema datos de entrada bajo su control que no eran pertinentes si se tiene en cuenta la finalidad prevista por el proveedor (art. 26 del RIA)

La falta de actualización de los sistemas de IA impone un deber de prevención y una obligación en cabeza del responsable de despliegue dado

---

[14] Directiva del Parlamento Europeo y del Consejo por la que se adaptan las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad por inteligencia artificial. Online: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022PC0496&from=ES

[15] Que en nuestro sistema bien podría encuadrar en las eximentes de hecho de un tercero (*deployers*) y hecho del damnificado (usuario final).

que su omisión puede ocasionar eventuales daños[16]. La responsabilidad ante su omisión se impone.

Cómo se podrá advertir hay una serie de imposiciones que influyen en la potencialidad dañosa de los sistemas de IA, y que pueden derivar en un resultado dañoso.

Así, consideramos que el hecho o actividad desplegada por el usuario profesional/*deployer* se convierte en una eximente que interrumpe total o parcialmente el nexo causal entre el daño y el hecho del demandado. En su caso deberá responder total o parcialmente frente a la víctima, ya que encuadraría en un típico supuesto del hecho de un tercero. La carga de la prueba será siempre de quién la alega.

La responsabilidad bien puede caer en la órbita contractual en caso de que el damnificado sea un consumidor, o bien parte de una relación contractual.

Nada obsta, a que la actividad del usuario profesional y la conducta del demandado concurran en la causación del resultado dañoso. En algunos casos, los deberes de cuidado del sistema de IA corresponden tanto el proveedor como el usuario profesional del sistema, por lo que ambos responderían frente a la víctima de forma solidaria o concurrente según el caso.[17]

¿Qué sucede si el daño se ha producido por caso fortuito o fuerza mayor? Por ejemplo, una bajada de la latencia de la red, un mal funcionamiento de la infraestructura, problemas con la interoperabilidad, la seguridad del sistema de IA que no se deben a un cumplimiento de un deber de su parte (el sistema de IA ha tomado una decisión imprevisible funcionando correctamente, pero ha causado daños).

---

[16] En este sentido el art. 10.2 de la propuesta de Directiva de Producto Defectuoso.

[17] En una relación de consumo puede entenderse este supuesto como una unidad comercial tecnológica. Así, "*cuando dos o más personas cooperen de forma contractual o similar en el suministro de diferentes elementos de una unidad comercial y tecnológica, y cuando la víctima pueda demostrar que al menos un elemento ha causado el daño pero no qué elemento, todos los posibles autores del daño deben ser y solidariamente cometido frente a la víctima*." Art. 29 "*Liability for Artificial Intelligence and other emerging digital technologies*"- Grupo de Expertos en Responsabilidad Vivil y Nuevas Tecnologìas". Online: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2020/01-09/AI-report_EN.pdf

¿El usuario profesional podría alegar válidamente caso fortuito? Entendemos que no es posible en virtud del art. 1733 inc. e) de nuestro CCyC. Es decir, no puede alegarse el caso fortuito derivado de una contingencia propia del riesgo de la cosa o **la actividad**[18] (el resaltado nos pertenece)

Para concluir, ¿qué sucede con el usuario final cuando su actividad importe la causación de un daño?

El usuario final es aquella persona física o jurídica que utiliza las herramientas de IA para uso personal, sin incorporarlas a una actividad comercial y/o profesional.

Obviamente, no corresponder colocar en cabeza del usuario final aquellas obligaciones que se imponen al *deployer*. No obstante, consideramos que un usuario final haciendo uso de un sistema de IA puede con su conducta contribuir a su propio daño.

En ese caso, consideramos que la actividad del usuario final solo será una eximente cuando su hecho tenga una incidencia causal suficiente en el resultado dañoso producido por el sistema de IA. Es decir, cuando su conducta haya interferido sustancialmente en las condiciones de funcionamiento del sistema de IA, o bien cuando debidamente advertido (informado) no haya ejecutado una actualización crítica del sistema de IA.

En el caso de la GenAI[19], los daños ocasionados por alucinaciones del sistema encuentran en un supuesto de actividad desplegada por el usuario final como eximente de responsabilidad.

En cualquier caso, la eximente deberá ser probada por quién la alega.

4. PONENCIA

La integración de sistemas de inteligencia artificial (IA) en diversas actividades plantea diversos desafíos en torno a la determinación de la responsabilidad civil por los daños que estos sistemas puedan causar.

La IA es potencialmente dañosa, por lo que entendemos que ante el daño causado la actividad del usuario de sistemas de IA puede gravitar como

[18] COLOMBO, María Celeste, "¿La utilización de algoritmos es una actividad riesgosa?" Publicado en: LA LEY 08/11/2019, 08/11/2019, 1, Cita Online: AR/DOC/3516/2019

[19] Inteligencia artificial generativa.

eximente de la responsabilidad civil. Así, se hace necesario introducir una diferenciación clara entre el usuario profesional/*deployers*, y los usuarios finales.

Asimismo, se hace imperioso asignarles a los primeros el cumplimiento de deberes y una responsabilidad más estricta debido al uso profesional que hacen de los sistemas de IA, y especialmente a su capacidad de supervisión y control sobre estos sistemas.

La actividad de estos usuarios puede eximir a otros sujetos de responsabilidad ya sea parcial o totalmente si su conducta tiene incidencia causal en la producción del resultado dañoso. En el caso de los usuarios finales, cuando su conducta haya interferido sustancialmente en las condiciones de funcionamiento del sistema de IA, o bien cuando debidamente advertido (informado) no haya ejecutado una actualización crítica del sistema de IA.

¿CUÁL ES EL FACTOR DE ATRIBUCIÓN APLICABLE A LOS SISTEMAS DE IA? Y POR QUÉ SE TRATA DE UN FACTOR OBJETIVO

Por María Celeste Colombo[1]

I. CONCLUSIONES

1. La responsabilidad civil derivada de la utilización de algoritmos debe ser de carácter objetivo.

2. Proponemos de *lege ferenda* la reforma del art. 16 de la ley de fondo a los fines de encuadrar a los algoritmos en la categoría de cosas, tal y como actualmente se incluyen la energía y las fuerzas naturales susceptibles de ser puestas al servicio del hombre.

3. Sostenemos como posible un régimen de responsabilidad civil derivado de la utilización de los algoritmos de la siguiente manera: a) responsabilidad civil derivada de las actividades riesgosas; y b) obligación tácita de seguridad.

II. FUNDAMENTOS

1. INTRODUCCIÓN

La revolución 4.0 tiene un contrapunto inquietante, su innegable lado oscuro. Los sistemas de IA poco a poco se introducen en nuestra cotidianeidad, en la esfera más íntima del ser humano.

La naturaleza misma de los sistemas de IA —programados para aprender y adaptarse en función de datos cambiantes— plantea desafíos únicos para los marcos legales existentes, que tradicionalmente se han centrado en la conducta humana como fuente primaria de imputabilidad.

Esta ponencia se propone explorar las problemáticas jurídicas asociadas a la atribución de responsabilidad por daños causados por

---

[1] Abogada (UNC) Magister en Derecho Civil Patrimonial (UCA). Jefa de Trabajos Prácticos de la Cátedra de Obligaciones Civiles y Comerciales- Facultad de Derecho- UBA. Aval otorgado por Carla Kott, profesora adjunta de la Universidad Nacional de Buenos Aires.

algoritmos, analizando tanto los factores de atribución como las posibles vías de regulación.

En este punto cabe preguntarnos, ¿cómo encuadrar normativamente la responsabilidad por daños causados por la utilización de algoritmos en el derecho?

A nuestro criterio, y adelantando opinión, entendemos que el factor de atribución aplicable a la responsabilidad civil derivada de la utilización de algoritmos es objetivo en atención a la normativa vigente.

En los próximos apartados esbozaremos los argumentos que avalan nuestra postura.

2. EL DILEMA EN TORNO A LA ELECCIÓN DE UNA RESPONSABILIDAD OBJETIVA VS RESPONSABILIDAD SUBJETIVA

Las técnicas de *machine learning* y *deep learning* tienen características complejas que evidencian una potencialidad dañosa que puede repercutir de manera negativa en derechos fundamentales consagrados en nuestra Constitución.

Los algoritmos pueden ocasionar menoscabo al patrimonio e integridad física de las personas en al menos cuatro situaciones generadoras de daños, a saber: a) *bugs* o errores informáticos[2]; b) sesgos algorítmicos[3]; y c) manipulación algorítmica o efecto burbuja[4],

Ahora bien, en muchos países no hay una normativa específica en materia de responsabilidad civil, y ciertamente en muchos países hay un vacío legal. Es decir, no hay una norma específica que regule este tipo de responsabilidad.

Así, se pone el énfasis en la autonomía de los sistemas de IA ya que se entiende que solo responderá en tanto sea autónomo al desplegar su tarea.

---

[2] Un *bug* o error informático constituye un error de programación, ya sea porque el programa no se comportó conforme la intención del programador o no cumplió con las expectativas razonables de los usuarios.

[3] Los sistemas de IA al momento de la recolección de los datos necesarios para desarrollar sus funciones y/o en la etapa de entrenamiento pueden contaminarse con los sesgos propios de la sociedad de la cual se extraen.

[4] Denominamos efecto burbuja a la edición que hacen los algoritmos a través del perfilamiento digital.

En efecto, los sistemas de *machine learning* y GenAI no dependen de personas para realizar sus actividades. Asimismo, es necesario destacar una característica sumamente importante: los sistemas de IA evolucionan conforme aprenden de su entorno y de la experiencia de uso.

Por otro lado, debido a su autonomía, el comportamiento del sistema de IA se torna imprevisible para el proveedor y/o usuario.

Otros consideran que solamente es posible imputar responsabilidad a una persona que ha obrado de manera culposa, o dolosa.

Pero el actuar negligente o doloso no puede endilgarse a un sistema de inteligencia artificial, sino a personas. Los sistemas de inteligencia artificial no son personas.

En el mundo, cuando hablamos de responsabilidad civil, tenemos dos grandes sistemas, a saber: a) un sistema de responsabilidad por culpa, donde el damnificado debe demostrar que el autor causó el daño de manera culposa o intencional; y b) un sistema de responsabilidad objetiva. En muchos casos, basado en el riesgo. Es decir, que se responde por el daño causado por una cosa o una actividad. En este contexto, si una persona se beneficia por la utilización de la cosa o la ejecución de una actividad debe responder por el daño causado.

En este punto, entra en discusión la carga de la prueba del daño.

Ante el daño ocasionado por un sistema de inteligencia artificial, cuando aplicamos un sistema de responsabilidad subjetiva se torna imposible demostrar la culpa o el dolo programador, desarrollador, usuario profesional, etc. Las víctimas se encontrarían desprotegidas ya que resultaría muy complejo probar la diligencia debida del sujeto dañador.

Sin embargo, otros autores entienden que existe la posibilidad de imputar responsabilidad readecuando la noción de *responsabilidad por hecho ajeno*.

Así, encuentran un fundamento adecuado en este tipo de factor de atribución objetivo de garantía, entienden que debemos tener en cuenta la actuación del humano y el sistema de inteligencia artificial, de suerte que la actividad o conducta de cada uno de ellos sea relevante para establecer si existe responsabilidad o no, o bien si hay un incumplimiento de deberes de cuidado.

El ser humano, en este caso, responde por el sistema de inteligencia artificial ya que ha infringido una conducta de cuidado. Sin embargo,

también requiere una mala actuación por parte del sistema de IA (principio de equivalencia funcional). Como se podrá advertir es una responsabilidad del principal por el hecho de sus dependientes, en este caso la dependencia existe entre el ser humano y el sistema de inteligencia artificial. Por tanto, existe un principal, el humano; y un auxiliar, el sistema de inteligencia artificial. Se hace cargar al principal con las consecuencias dañosas el comportamiento del sistema de inteligencia artificial del que se sirve y se beneficia[5].

3. EL FACTOR OBJETIVO COMO FACTOR DE ATRIBUCIÓN APLICABLE A LOS SISTEMAS DE IA

Los algoritmos pueden erigirse en agentes dañosos.[6] A través del uso de sistemas de IA es que pueden afectarse derechos personalísimos como la dignidad, el derecho a la imagen, el derecho al honor, al trato digno y equitativo, el derecho a la privacidad, a la libertad de contratar (arts. 14, 19, 33, 42, art. 75 inc. 22 de la CN; arts. 9º, 51, 52, 53, 55, 1097,1098 y 1099 del CCyC; y arts. 4 a 10 de la Ley de Protección de Datos Personales).

Los daños pueden verificarse directamente sobre la persona humana, o bien que el repercutir en el patrimonio del sujeto. Incluso, en caso de corresponder, afectar la esfera íntima de la persona pudiendo reclamarse el daño extrapatrimonial.

¿Y en cual es al factor de atribución de responsabilidad?

He aquí el *quid* de la cuestión, la posibilidad de atribuir a los propios sistemas de IA la responsabilidad por las consecuencias dañosas. Este dilema es quizás sea uno de los problemas a resolver centrales a los fines de establecer el marco legal apropiado.

Así, consideramos que resulta apropiado decantarse por la responsabilidad del tipo objetiva. No parece acertado poner en cabeza del damnificado la tarea de probar quién omitió obrar con la diligencia debida, o quién actuó con dolo, lo que descarta de plano un factor subjetivo de atribución.

---

[5] NAVAS NAVARRO, Susana, "Daños ocasionados por sistemas de inteligencia artificial", Editorial Comares, Granada, 2022, págs. 60/61

[6] COLOMBO, María Celeste, *"¿La utilización de algoritmos es una actividad riesgosa*?", La Ley, 8/11/2019, Cita Online: AR/DOC/3516/2019.

Los sistemas de IA de *machine learning y deep learning*− y más aún los sistemas de GenAI − tienen características muy complejas como la opacidad, el comportamiento autónomo y la capacidad de generar contenido por sí mismos. Estos sistemas evidencian una potencialidad dañosa que puede repercutir de manera negativa en los derechos fundamentales consagrados en nuestra Constitución.

Por este motivo proponemos[7] que, con nuestra normativa, podemos diagramar un régimen de responsabilidad civil derivado de la utilización de algoritmos, a saber: a) responsabilidad civil derivada de actividades riesgosas, toda actividad desplegada por sistemas de IA que utilicen técnicas de *machine learning* y *deep learning* encuadran en el concepto de actividad riesgosa por los medios empleados o por las circunstancias de su realización. La responsabilidad es objetiva según lo normado por los arts. 1722, 1757 y 1758 del C.CyC[8]. ; b) obligación tácita de seguridad, en todo contrato pesa sobre las partes contratantes un deber tácito de seguridad por los daños que puedan ocasionar durante su ejecución. La responsabilidad en este caso también es de naturaleza objetiva, siendo de aplicación los arts. 1722 y 1723 del CCyC.[9]

a) La utilización de algoritmos como actividad riesgosa

Atento lo expuesto en el apartado anterior podemos concluir que estamos convencidos de que el factor de atribución objetivo que más se ajusta a este tipo de responsabilidad civil es el de riesgo creado.

Esta teoría tiene recepción en nuestra ley de fondo en el art. 1757, y comprende: a) los daños causados por las cosas riesgosas por su naturaleza; b) los daños causados por las cosas que no son riesgosas per se, pero cuya intervención activa provoca un daño (potencialidad dañosa); y c) daños ocasionados por actividades riesgosas o peligrosas por su naturaleza, por los

[7] Para mayor abundamiento, véase: COLOMBO, María Celeste, "Propuestas para encuadrar la responsabilidad civil derivada de la utilización de algoritmos. Una perspectiva argentina", en CORVALAN, Juan, ob. cit., Tomo II, pág. 401/439.

[8] COLOMBO, María Celeste, "¿La utilización de algoritmos es una actividad riesgosa?", La Ley- 8/11/2019- Cita Online: AR/DOC/3516/2019

[9] PIZARRO, Daniel, *Tratado de la Responsabilidad Objetiva*, La Ley, Buenos Aires, 2015, Tomo II, págs. 297/308.

medios empleados o por las circunstancias de su realización, intervengan o no cosas en la actividad desarrollada.[10]

Una primera lectura del art. 1757 del C.Cy C nos presenta con un primer obstáculo, la norma es aplicable al vicio o riesgo de una cosa. Un algoritmo no es jurídicamente una cosa en los términos del art. 16 de la ley de fondo.

Asimismo, es necesario destacar que tampoco puede considerarse al algoritmo como software. Un algoritmo no es un programa, aunque pueda formar parte de él. Podríamos decir que la naturaleza jurídica de un algoritmo encuadra en el concepto de bien inmaterial. Los sistemas de IA tampoco ingresan en la categoría de cosas[11]

Sin embargo, y atento la complejidad del tema que nos ocupa, proponemos de *lege ferenda* la reforma del art. 16 de la ley de fondo a los fines de encuadrar a los algoritmos en la categoría de cosas, tal y como actualmente se incluyen la energía y las fuerzas naturales susceptibles de ser puestas al servicio del hombre.

Entonces ¿por qué entendemos que a la responsabilidad derivada de la utilización de algoritmos le es aplicable el régimen del art. 1757 del CCyC?

Básicamente, consideramos que la actividad desplegada por los sistemas de IA de *machine learning y deep learning* configura una actividad riesgosa por los medios empleados y circunstancias de realización.

La responsabilidad derivada de la actividad riesgosa está receptada por el art. 1757 del CCyC que expresa: "*Toda persona responde por el daño causado por(...) las actividades que sean riesgosas o peligrosas por su naturaleza, por los medios empleados o por las circunstancias de su realización(...)"*

---

[10] WIERZBA, Sandra, *Manual de Obligaciones Civiles y Comerciales*, La Ley- Buenos Aires- 2019- pág. 586; GALDÓS, Jorge, "*El art. 1757 del Cód. Civ. y Com. (el anterior art. 1113 Código Civil*)", RCyS 2015-IV, 176; AR/DOC/778/2015.

[11] A salvo, claro está, de aquellos sistemas de IA que estén anexados a robots. Los robots con inteligencia artificial incorporada son cosas y por lo tanto le es aplicable el régimen del art. 1757 y sgtes. del CCyC. , sea estos o no sistemas de GenAI. En conclusión, en principio, no cabría aplicar la responsabilidad derivada del vicio o riesgo de la cosa (art. 1757 del CCyC) a los algoritmos y sistemas de IA.

La doctrina enseña que la actividad es comprensiva tanto de hechos como de acciones desplegadas por el hombre en combinación con elementos mecánicos o inmateriales, incluyendo los métodos para realizarla.[12]

En este orden de ideas, entendemos que los sistemas de IA que utilizan técnicas de *machine learning*, y muy especialmente de *deep learning*, despliegan una actividad tendiente al aprendizaje automático. Asimismo, al tomar decisiones automatizadas[13]

En el caso de la GenAI todo es mucho más palpable, ya que en los grandes modelos de lenguaje (LLMs) al responder al *prompt* de un usuario están realizando una tarea, una actividad ordenada.

En base a lo anteriormente mencionado, creemos firmemente que tanto los sistemas de *machine learning* como la GenAI se ajustan al concepto desarrollado por Zavala de González. Por lo tanto, consideramos que estas técnicas son actividades riesgosas que por los medios empleados y circunstancias de su realización pueden causar un daño (art. 1757 CCyC).

Pero ¿a quién atribuimos la responsabilidad por los daños causados por la actividad desplegada por los sistemas de IA?

En atención a que quien realiza la actividad es el sistema de IA, el sindicado como responsable será indefectiblemente aquel sujeto pasivo que tenga la posibilidad de dirigir, fiscalizar y/o controlar al sistema de IA. La doctrina señala que "*realizar la actividad no significa necesariamente desplegar actos materiales en que consiste, sino llevarla a cabo o dirigirla, por sí mismo o a través de otros*"[14] Nosotros agregamos, deberá imputarse

---

[12] ZAVALA DE GONZALEZ, Matilde / GONZALEZ ZAVALA, Rodolfo, *"La responsabilidad civil en el nuevo código",* Alveroni Ediciones, 2018, Tomo III, pág. 755.

[13] Se denomina toma de decisiones automatizadas al proceso mediante el cual un sistema de IA adopta una resolución por sí misma − sin intervención humana− alguna una cuestión sometida a su *expertise*. Estas decisiones generalmente pueden basarse en datos emitidos por la persona, así como en perfiles creados digitalmente o datos inferidos. Una ADM no requiere un perfilamiento previo necesariamente, aunque suele ser lo usual. como el otorgamiento de un crédito, investigar un fraude en seguros, y/o evaluar la admisión de un estudiante a una universidad, no hacen otra cosa más que desarrollar una actividad tendiente a la consecución de un objetivo.

[14] ZAVALA DE GONZALEZ, Matilde / GONZALEZ ZAVALA, Rodolfo, ob. cit., Tomo III, pág. 770**.**

la responsabilidad a todo aquel que se beneficie económicamente de ella aun cuando no desarrolle la actividad. (arts. 1758 CCyC).

No obstante, hay que recordar que la responsabilidad alcanza a quien fiscaliza, supervisa o controla la actividad, por lo que serán legitimados pasivos a quienes le quepa la genérica supervisión sobre los medios empleados o las circunstancias de realización de la actividad

Finalmente, el responsable se exime de responder probando la causa ajena, es decir el hecho del damnificado, el hecho de un tercero y/o el caso fortuito (arts.1728, 1729 y 1730 del C.C y C). Se exime también aquel que demuestra que la actividad del usuario del sistema de IA tiene incidencia causal total o parcialmente en la producción del resultado dañoso.

No constituye eximente la autorización administrativa para la realización de la actividad, ni el cumplimiento de las técnicas de prevención (art 1757, último párrafo del CCyC).

Por último, y por imperativo legal, los responsables responden concurrentemente frente al tercero damnificado (art. 1758 del CCyC).

b) La obligación tácita de seguridad y el uso de algoritmos

En todo contrato pesa sobre las partes contratantes un deber tácito de seguridad por los daños que puedan ocasionar durante su ejecución.

La obligación tacita de seguridad tiene fundamento en el principio de la buena fe (art. 9, 729 y 961 del C.CyC). Todo contratante tiene el deber tácito de preservar la integridad de los bienes y la persona de su co-cotrantante. Esta obligación es secundaria y coexiste de manera autónoma junto con la obligación principal de un contrato.

El ámbito de aplicación es en aquellos contratos que por la naturaleza de sus prestaciones imponen al deudor un deber de indemnidad con relación a la persona o bienes del acreedor. Es requisito que la actividad contractual desplegada por el deudor tenga el carácter de riesgosa en atención a su naturaleza o por el riesgo de los medios empleados en su realización.[15]

La doctrina reseña una serie de contratos que cumplen los requisitos antes mencionados, a saber: contrato de transporte, contrato de espectáculos

[15] PIZARRO, Ramón, *ob. cit*., Tomo II- págs. 302/303.

públicos, contrato de espectáculos deportivos, contrato de práctica deportiva, contrato de trabajo.

Nosotros agregamos todo contrato donde una de las partes ponga a disposición de la otra para la ejecución de una tarea a un sistema de IA de *machine learning y/o deep learning*, redes neuronales, IA de propósito general, grandes modelos de lenguaje, etc. En definitiva, de todo sistema de IA que atención de su complejidad sea intrínsecamente opaco.[16]

La obligación tácita de seguridad es una obligación de resultados en los términos de los arts. 774 inc b y c y 1723 C.CyC) por lo que la responsabilidad es objetiva. En las obligaciones de resultados el deudor garantiza la consecución de un resultado por lo que en caso de incumplimiento responde objetivamente, se exime se responder acreditando causa ajena.

En este sentido, entendemos que en contratos donde se despliegan sistemas de IA, se impone en cabeza del deudor una especial obligación −la de garantizar la seguridad−Esta obligación de seguridad se extiende sobre los bienes y la persona del usuario del sistema de IA[17].

c) ¿La norma de clausura brinda una solución?

Nuestra ley de fondo contiene una norma de clausura para cubrir la laguna normativa que podría presentarse sobre la aplicación del factor de atribución en el caso concreto.

El art. 1721 del C.CyC establece que "*en ausencia de normativa, el factor de atribución es la culpa*". En otras palabras, en atención a que no hay una norma expresa que regule el factor de atribución aplicable a la responsabilidad derivada de la utilización de algoritmos podríamos decir que la culpa emerge como regla de clausura.

[16] COLOMBO, María Celeste, *ob. ci*t. en CORVALAN, Juan (Dir.)- *ob. cit*., Tomo II- pág. 434.

[17] COLOMBO, María Celeste, ob. cit. en CORVLAN, Juan (Dir.)- ob. cit., Tomo II- pág. 434.

Sin embargo, en nuestro ordenamiento jurídico, la norma de clausura es residual ya que solo se hace operativa cuando es imposible cubrir el vacío legal mediante el uso de la analogía.[18]

Para finalizar, creemos que es imperiosa la regulación de la responsabilidad civil de los sistemas de IA.

Sin embargo, y no obstante lo expuesto en la presente ponencia, pensamos que quizás una solución intermedia sea la de establecer dos regímenes de responsabilidad: a) para sistemas de alto riesgo una responsabilidad objetiva; b) una responsabilidad subjetiva para los daños causados con sistemas de IA que no supongan un alto riesgo.

4. PONENCIA

La creciente incorporación de los sistemas de inteligencia artificial en diversos ámbitos de la vida cotidiana y profesional plantea desafíos sin precedentes en el ámbito del derecho civil. En particular, la atribución de responsabilidad por los daños causados por estos sistemas exige una revaluación de los conceptos tradicionales de culpa y negligencia, que resultan insuficientes frente a la complejidad y autonomía de los algoritmos modernos.

Luego de analizar la normativa vigente y el impacto en nuestra sociedad de los sistemas de IA es que proponemos de *lege ferenda* la reforma del art. 16 de la ley de fondo a los fines de encuadrar a los algoritmos en la categoría de cosas, tal y como actualmente se incluyen la energía y las fuerzas naturales susceptibles de ser puestas al servicio del hombre.

A lo largo de este trabajo hemos defendido nuestra tesis: la responsabilidad civil derivada de la utilización de algoritmos debe ser de carácter objetivo. Este enfoque se justifica no solo por la dificultad que enfrentan las víctimas al intentar probar la culpa, sino también por la autonomía en la toma de decisiones del sistema, la opacidad, y la potencialidad dañosa inherente a estos sistemas.

---

[18] GALDÓS, Jorge, *Comentario al art. 1721* en LORENZETTI, Ricardo (Dir)- "*Código Civil y Comercial de la Nación. Comentado"*- Tomo VIII- Rubinzal-Culzoni Editores- Santa Fe- 2015- págs. 385.

EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN LA AFECTACIÓN DE DERECHOS PERSONALÍSIMOS

Por Ricardo Sebastián Danuzzo[1] y María Josefina Álvarez[2]

I. CONCLUSIONES[3]

De lege lata

1. La utilización de inteligencia artificial puede erigirse en la actualidad como una vía de violación al derecho a la privacidad y a la identidad personal, que requiere, por sus particularidades, de vías preventivas, resarcitorias y sancionatorios eficaces.

2. La utilización de la inteligencia artificial puede, en muchas ocasiones, constituirse en una vía que vulnera el principio de la buena fe entre los contratantes e inducir a las personas a contratar de determinada manera por manipulación de información.

3. El marco normativo vigente en la Argentina, constituido por reglas y principios, los operadores jurídicos deben buscar las soluciones jurídicas recurriendo a un adecuado uso de las herramientas legales existentes, especialmente al dialogo de fuentes conforme lo establecen los artículos 1 y 2 del Código Civil y comercial de la Nación.

---

[1] Doctor en Derecho - UNNE 2013 - Magister en Derecho Empresario - UNNE 2021 - Profesor Titular por Concurso de la materia Derecho de Daños - Catedra B de la Facultad de Derecho y Ciencias Sociales y Políticas de la UNNE.

[2] Profesora Libre de la Cátedra B Derecho de Daños. Magister en Derecho Penal UNNE, Especialista en Daños y Perjuicios UBA, Doctorado UNNE en etapa presentación de tesis, Asesora Letrada Comisario de la Policía de Corrientes. Aval del Titular de Cátedra Dr. Ricardo Sebastián Danuzzo.

[3] **Resumen:** Este trabajo parte de la exposición sintética del análisis de la nueva revolución digital y tecnológica y el impacto de la inteligencia artificial, dando lugar a nuevas situaciones dañosas, como los vehículos autónomos y los robots, direccionándose, en último término, hacia los posibles modos de abordajes legislativos de la realidad actual del derecho de daños con la aparición de novedades. Son muchos los casos de uso de Inteligencia Artificial, que pueden generar situaciones dañosas para las personas, con independencia del grupo al que pertenecen que de algún modo están expuestos a la influencia de la misma. En el mismo tomaremos posición respecto de algunos temas controvertidos.

4. No deben quedar daños sin resarcir derivados de la IA. Las personas humanas y jurídicas que la utilizan deben ser garantes de los riesgos que introducen en la sociedad, o de los riesgos de las cosas y/o actividades de las cuales se sirven. Corresponde, por ende, aplicar los estándares previstos en los arts. 1710 y concordantes para la prevención del daño y 1757, 1758 y concordantes para su reparación, siendo el factor de atribución indudablemente objetivo.

5. Si el vínculo jurídico fuera calificado como relación o contrato de consumo, la responsabilidad que resulta del vicio o defecto de la cosa o de la prestación del servicio además será solidaria de todos los integrantes de la cadena de producción de conformidad con lo que dispone el Art. 40 de la Ley Nº 24.240.

II. FUNDAMENTOS

Este trabajo parte de la exposición sintética del análisis de la nueva revolución digital y tecnológica y el impacto de la inteligencia artificial, dando lugar a nuevas situaciones dañosas, como los vehículos autónomos y los robots, direccionándose, en último término, hacia los posibles modos de abordajes legislativos de la realidad actual del derecho de daños con la aparición de novedades. Son muchos los casos de uso de Inteligencia Artificial, que pueden generar situaciones dañosas, tanto a usuarios, como a terceros que de algún modo están expuestos a la influencia de la misma. Basta con enumerar alguno de los usos más comunes, a los que estamos expuestos la detección facial de los teléfonos móviles y las redes sociales, los vehículos autónomos, los chatbots -que suelen atendernos y evacuar nuestras consultas vía web o telefónicamente en forma automática- también nos sugieren, hoteles, restoranes, lugares para visitar etc., de acuerdo con nuestro historial de búsqueda. Youtube, Spotify o Netflix, cuando arman nuestro perfil, se utiliza IA; como así también Google. Las plataformas virtuales o digitales de economía colaborativa, como Rappi, glovo y Uber, entre otra utilizan inteligencia artificial para todas sus actividades. También en el ámbito de las finanzas, aconsejando hacer inversiones. En el transporte y circulación (Waze, Google Maps, tráfico, estado de rutas. Uso en el sistema de salud, existen robots que operan y detectan enfermedades mejor que los humanos Destaco también el uso Legal, bots que realizan operaciones jurídicas, el uso en Smart Contracts, inteligencia artificial

aplicada a sentencias, demandas, dictámenes fiscales (sistema prometea en Argentina), contratos y solución de controversias.

Asimismo del problema de cómo nuevas situaciones dañosas surgen a raíz de la tecnología, en donde ya casi es imposible encontrar al responsable, por la forma en las que se dan los hechos.

Se debería encontrar un nuevo régimen normativo, que propenda, en primer lugar a regular nuevas situaciones dentro del derecho de daños, que hoy en día podrían quedar al margen de una regulación específica y que sea al mismo tiempo compatible, con los lineamientos de la Constitución Nacional.

Es necesario dedicarle un tratamiento especial al desarrollo tecnológico y su vinculación con la responsabilidad. Ello en el convencimiento de que la importancia irá aumentando hacia el futuro porque los daños estarán cada vez más asociados al uso de tecnologías que apenas son conocidas.

El mundo del Derecho se encuentra actualmente afectado por los cambios tecnológicos y por los cambios que se producen en las relaciones interpersonales, su modo y su forma de comunicación. , pensemos en los daños que producen los buscadores de internet, en las ondas de radio emitidas por un equipo de telefonía celular que son absorbidas por el cerebro humano, en el Phishing, en la publicidad engañosa, en la invasión de la privacidad y del espacio aéreo producidas por cámaras, satélites y drones que captan absolutamente todo lo que acontece, el notable impacto de la inteligencia artificial, los vehículos autónomos, los robots y todo el daño que afecta a la sociedad toda que produce la contaminación ambiental. Los daños potenciales y actuales están ahí, a la vista de todos, y ante esto no podemos ignorar tal situación, si podemos detectarlos, reconocerlos, prevenirlos como así también, resarcirlos en forma justa.

La inteligencia artificial es una combinación de algoritmos planteados con el propósito de crear máquinas que presenten las mismas capacidades que el ser humano.

En nuestro marco de la responsabilidad civil, todas estas innovaciones generan una crisis de la legislación que queda evidentemente desactualizada, toda vez que fue dictada sin tener en cuenta estas novedades, con lo cual habrá que ver de lege lata como afrontarlas con el derecho positivo actual y lege ferenda que cambios se deberán proponer.

Frente a ausencia de normativas específicas, hay quienes proponen otorgarle personería jurídica electrónica a los robots totalmente autónomos, igualando los mismos al régimen de las sociedades y/o persona jurídicas. En el informe de la Unión Europea dispone que en el marco actual, los robots no pueden ser jurídicamente los responsables de los daños que causen; que las leyes actuales de responsabilidad civil solo prevén casos en los que es posible atribuir la conducta activa u omisiva del sistema robótico a una persona humana o jurídica determinada, como puede ser el fabricante, el garante, el vendedor, el operador, el guardián, el propietario y/o el usuario—, y en los que dicho agente podía haber previsto y evitado el comportamiento del robot que ocasionó los daños; que, además, los fabricantes, los operadores, los propietarios o los usuarios podrían ser considerados objetivamente responsables de los actos u omisiones de un robot. En el caso de nuestro sistema, fundamentando la responsabilidad en los artículos 1757 y 1758 del código civil y comercial.

Ante todo lo expuesto se advierte un nuevo horizonte de la responsabilidad civil, derivado de los daños que surgen a raíz de la inteligencia artificial.

En Argentina se registraron numerosos casos en diversas ciudades, de daños sufridos por estafa por WhatsApp, utilizando IA. Una nueva modalidad de estafa a través de WhatsApp, está siendo aplicada en todo el mundo y Argentina no es la excepción. Esta estafa, conocida como “vishing” utiliza la inteligencia artificial (IA) para engañar a las víctimas y obtener dinero o realizar otras maniobras fraudulentas. Así se registraron numerosos casos de vishing en diversas ciudades argentinas, como Buenos Aires y Mar del Plata. Los estafadores utilizan números de teléfono desconocidos, a menudo provenientes del exterior, para realizar llamadas por WhatsApp, y clonan voces para hacerse pasar por familiares o amigos de las víctimas.

El abogado Rodrigo Bionda, especialista en prevención de ciberdelitos y residente de Mar del Plata, hizo varias recomendaciones para protegerse de estas estafas.

"Debemos empezar a descreer de todo lo que vemos y escuchamos", advirtió Bionda, subrayando la dificultad de distinguir una voz clonada de una real cuando la grabación supera el medio minuto.

Bionda, destacó la creciente sofisticación de estas tecnologías. “Hice una prueba de video llamada con una versión paga de inteligencia

artificial y es imposible darse cuenta si estamos frente a la persona original", explicó el abogado.

Ante esta situación, se recomienda no atender llamadas de números desconocidos, especialmente aquellos provenientes de la India y otros países donde se han detectado numerosos casos de vishing.

Además, es fundamental verificar cualquier solicitud de dinero o información personal mediante un canal de comunicación alternativo antes de realizar cualquier acción.

Una encuesta reciente realizada por McAfee reveló que el 77% de las víctimas de este tipo de fraude enviaron dinero a los estafadores. Esta estadística subraya la efectividad de las técnicas de vishing y la necesidad urgente de aumentar la concienciación y las medidas preventivas para proteger a la población.

Los expertos recomiendan estar siempre alerta y sospechar de cualquier solicitud de dinero o información personal, incluso si parece provenir de un conocido. Es crucial utilizar métodos seguros de verificación antes de realizar cualquier transferencia o compartir datos sensibles.

El estado de derecho debe tomar por las riendas muchos cambios sociales que se están produciendo como consecuencias de avances tecnológicos vertiginosos. Se debe promover la creatividad emprendedora y minimizar los riesgos de la utilización irresponsable de nuevos desarrollos. Si bien Argentina no cuenta con una legislación que regule la responsabilidad algorítmica, podemos encontrar leyes relacionadas como la Ley de Protección de Datos Personales Nº 25.326, la Ley de Propiedad Intelectual Nº 11.723, la Ley de Defensa del Consumidor Nº 24.240 y la Ley de Telecomunicaciones Nº 19.798. A nivel internacional encontramos que el derecho ha ido adaptándose a los desafíos que del avance tecnológico, por ejemplo: en el caso de accidentes causados por coches autónomos los seguros seguirán siendo el primer destinatario de las reclamaciones; en cuanto a las compañías que utilicen sistemas de inteligencia artificial para sus procesos de selección laboral podrán ser demandadas en caso de incurrir en prácticas discriminatorias, y también las aseguradoras que incurran en prácticas contra el consumidor derivadas de los análisis generados por sus modelos de inteligencia artificial para fijar precios y decidir a quién aseguran seguirán teniendo que responder como empresas.

La regulación es disímil en cada país: en Estados Unidos, por ejemplo, se está apostando por estándares que controlen el riesgo de los sistemas de inteligencia artificial.

Actualmente encontramos normativa internacional a la que Argentina adhirió como los principios generales para el abordaje ético de la inteligencia artificial, de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) la cual emitió la Recomendación sobre la Ética de la Inteligencia Artificial dictada. Asimismo, podemos mencionar la Declaración de Qingdao, aprobada en 2015, sobre el aprovechamiento de las tecnologías de la información y la comunicación (TIC) para lograr el ODS 4. También podemos destacar la normativa dictada por el Poder Ejecutivo a través de decretos, por ejemplo, podemos mencionar el decreto 50/2019 o el decreto 2/2023 el cual establece recomendaciones para una inteligencia artificial fiable. Asimismo, si bien el artículo 3° de la Ley 25.467 establece principios de carácter irrenunciable y aplicación universal, que regirán en cualquier actividad de investigación en ciencia, tecnología e innovación, nos parece importante ampliar dicha consideraciones en una normativa que profundice el tema. Más allá de lo valioso de normas dictadas por el Poder Ejecutivo, es un tema que debe ser debatido y trabajado en el Poder Legislativo, ámbito más plural y representativo de las diferentes miradas para obtener una legislación estable y amplia.

III. BIBLIOGRAFÍA:

- **Danesi, Cecilia C.** Inteligencia artificial y responsabilidad civil: un enfoque en materia DE VEHÍCULOS AUTÓNOMOS SUP. ESP. LEGALTECH 2018 (NOVIEMBRE), 05/11/2018.

- **Pizarro**, Ramón Daniel / Vallespinos, Carlos Gustavo "TRATADO DE RESPONSABILIDAD CIVIL" Tomo I 2017.

- https://www.cronista.com/ INFO.

- **Sup. Esp. LegalTech** 2018 (noviembre), 05/11/2018, 39 de vehículos autónomos . Prometea es un sistema de IA creada en el ámbito del Ministerio Público Fiscal de CABA. Con SKILLS QUE VAN DESDE AUTOMATIZACIÓN HASTA PREDICCIÓN EN LA GENERACIÓN DE DICTÁMENES FISCALES, FUENTE HTTPS://IALAB.COM.AR/PROMETEA/

- Informe del 27/01/2017 de la Comisión de Asuntos Jurídicos con recomendaciones a la Comisión Europea para creación de una directiva relativa a las normas de legislación civil en materia de robótica.

- PROYECTO DE LEY RESPONSABILIDAD ALGORÍTMICA Y PROMOCIÓN DE LA ROBÓTICA, ALGORITMOS VERDES E INTELIGENCIA ARTIFICIAL EN LA REPÚBLICA ARGENTINA. ttps://leyesabiertas.hcdn.gob.ar/).

EL IMPACTO DE LA DISRUPCIÓN DE LA IA EN EL DERECHO. HACIA UNA REGULACIÓN ADAPTATIVA EN ARGENTINA

Por Ricardo Sebastián Danuzzo[1]

I. CONCLUSIONES[2]

De lege lata

1. Nuestro régimen legal tiene el potencial para dar respuestas a estos desafíos partiendo de los principios de la responsabilidad objetiva (artículos 1757 y 1758 del CCC).

2. Una adecuada calificación del vínculo jurídico, como de consumo o de adhesión permitiría aplicar el régimen de especial naturaleza tuitiva del protección de los consumidores vigente, siendo mayores las ventajas con las que cuente el operador jurídico, abriendo el espectro de los legitimados activos y pasivos, generando la aplicación régimen de responsabilidad solidaria por vicio o defecto de la cosa o la prestación del servicio y otorgando facilidades procesales y probatorias entre otras.

3. De propenderse a una protección integral de la persona a través la plena vigencia de la acción preventiva del daño y propiciando además una reparación plena de la misma.

De lege ferenda

4. Es necesario complementar la legislación vigente con una norma específica, que permita optimizar el régimen de responsabilidad civil inspirada en la reciente Ley de la Unión Europea, que clasifíquelos sistemas inteligentes según su riesgo y grado de autonomía, y prevea la

---

[1] Profesor Titular de Derecho de Daños. Profesor Titular de Derecho de los Contratos. Facultad de Facultad de Derecho y Ciencias Sociales y Políticas de la UNNE.

[2] **Resumen:** La disrupción tecnológica y el avance acelerado de la inteligencia artificial (IA) presentan en la actualidad un escenario distópico en el que las máquinas inteligentes, con autonomía y capacidad de autoaprendizaje, imitan características humanas. Este nuevo panorama plantea retos significativos para el derecho civil, especialmente en la regulación de daños causados por sistemas inteligentes autónomos y la atribución de responsabilidad.

responsabilidad en cada caso, contemplando aquellos que derivan de los sesgos algorítmicos.

Todas estas cuestiones serán desarrolladas en el presente trabajo en que, ha sido de esencial valía el aporte de la Profesora Eugenia Asc[3], integrante de la catedra, a quien agradezco especialmente su contribución.

II. FUNDAMENTOS

1. INTRODUCCIÓN

En el contexto actual caracterizado por el avance exponencial en tecnologías disruptivas como la inteligencia artificial (IA), enfrentamos nuevos paradigmas que desafían, entre otras cuestiones, nuestro sistema jurídico.

La inteligencia artificial, al integrar algoritmos sofisticados para desarrollar sistemas con capacidades semejantes a las humanas, nos introduce en una era en la que las máquinas no solo realizan tareas específicas, sino que operan con un grado de autonomía significativo.

Así, esta IA avanzada, denominada "autoconsciente", tiene la capacidad de tomar decisiones en situaciones imprevistas por sus creadores. La capacidad de autoaprendizaje y decisión autónoma de los sistemas inteligentes no solo amplía sus aplicaciones, sino que también incrementa el riesgo de eventos dañosos, exacerbados por posibles sesgos en los algoritmos que pueden llevar a errores de identificación y discriminación.

Frente a estas nuevas hipótesis de daños, surgen los principales interrogantes en materia de responsabilidad: ¿Quién será civilmente responsable por los daños causados por las acciones de estas máquinas autónomas?¿Cuál es el factor de atribución aplicable? ¿Qué eximentes podrán alegarse en cada caso?

Dado que el marco normativo argentino actual, no abarca adecuadamente las complejidades de la IA, se vuelve crucial una revisión y adaptación legislativa. En consecuencia, se buscará precisar el régimen legal vigente considerando la necesidad de una normativa específica y adecuada

[3] Profesora Adscripta de Derecho de Daños. Facultad de Facultad de Derecho y Ciencias Sociales y Políticas de la UNNE

a cada contexto, asegurando protección y seguridad jurídica frente a los daños derivados del uso de la inteligencia artificial.

2. DESARROLLO

La capacidad de autoaprendizaje y autonomía de la inteligencia artificial y la consecuente imprevisibilidad en la toma de sus decisiones, ponen en crisis a los institutos tradicionales de la responsabilidad civil. El documento anexo a la comunicación de la Comisión Europea titulada "Inteligencia Artificial paraEuropa", destaca que lacombinaciónentre el autoaprendizajey la autonomía conlleva a que el comportamiento de las nuevas tecnologías sea difícil de predecir[4].

En los posibles escenarios distópicos que la inteligencia artificial (IA) podría generar, surge la necesidad de examinar la responsabilidad civil por los daños que la robótica puede ocasionar a personas o bienes. Estos daños podrían derivarse de desperfectos en la programación, de ataques de seguridad, o simplemente de los riesgos inherentes a su operación.

En este contexto, es crucial investigar no solo quiénes deben asumir la responsabilidad de indemnizar, sino también cuál es el factor de atribución aplicable y las posibles eximentes que podrían alegarse en cada caso.

3. MARCO NORMATIVO ACTUAL Y LIMITACIONES

a) Responsabilidad derivada de la intervención de cosas y de ciertas actividades

Frente a este escenario, podemos decir prima facie que resultan aplicables los principios de responsabilidad objetiva de la normativa argentina, representada por los artículos 1757 y 1758 del CCC.

Siendo el robot una cosa, el supuesto de responsabilidad no podría ser otro que el de la “responsabilidad por el riesgo o vicio de las cosas”, previsto en el art. 1757, CCCN. Así, a tenor del primer párrafo del art. 1758 CCCN, lucen como responsables primarios y concurrentes su “dueño” o “guardián”.

---

[4] European Commission. *Staff Working Document: Liability for Emerging Digital Technologies*. SWD (2018) 137. Bruselas, 25 de abril de 2018.

Sin perjuicio de ello, no cabe duda que las actividades realizadas mediante la utilización del robot califican como "actividades riesgosas". Las actividades pueden resultar riesgosas tanto por su naturaleza, por los medios empleados o por las circunstancias de su realización (art. 1757 CCCN). En cuanto a la legitimación pasiva, en este caso, sería más amplia en cuanto art. 1758, 2do, párr., CCCN indica como responsables a: "quien la realiza, se sirve u obtiene provecho de ella". No obstante, podríamos decir que no quedaría comprendido quien simplemente obtiene un provecho, por estar disociado con la creación del riesgo. Excepto que tenga cierta facultad de control o dirección en la organización de las tareas del robot.

Finalmente, el artículo 1757 en su última parte prescribe que la responsabilidad es objetiva y no son eximentes la autorización administrativa para el uso de la cosa o la realización de la actividad, ni el cumplimiento de las técnicas de prevención. Es decir, en ningún caso, la adopción de técnicas de prevención disminuye o aniquila la responsabilidad.

b) Ley de Defensa del Consumidor

Por otra parte, respecto de la aplicación de la legislación aplicable, cuando un consumidor se ve afectado, la responsabilidad por problemas con un sistema de IA se extiende a todos los actores involucrados en su cadena de comercialización. Esto incluye al fabricante, diseñador, programador, desarrollador, proveedor e incluso a quienes distribuyen o modifican el sistema.

Según el artículo 40 de la Ley de Defensa del Consumidor, todos estos actores son responsables solidariamente por los daños causados por el vicio o riesgo del producto o servicio. Solo pueden liberarse de responsabilidad si demuestran que el daño no fue causado por su acción.

4. PROBLEMAS ESPECÍFICOS ASOCIADOS CON LA IA

Si bien las normativas citadas ofrecen un marco general para la responsabilidad civil, no abarcan completamente las complejidades inherentes a la IA. La legislación vigente necesita ser complementada con reformas específicas que aborden las particularidades de la IA, que prevea la responsabilidad por daños derivados de los sesgos algorítmicos, que determine la legitimación pasiva y, en definitiva, qué patrimonio garantizará la reparación del daño causado.

Hasta aquí podemos decir que nuestro régimen actual permite determinar el factor de atribución aplicable y la legitimación pasiva en estos casos, pero ¿qué pasará si los sujetos que *prima facie* aparecen responsables intentan liberarse de responsabilidad alegando el hecho de un tercero o caso fortuito?

5. PERSONALIDAD JURÍDICA ROBÓTICA

Como lo hemos referido, en la actualidad emergen dispositivos equipados con algoritmos que mejoran continuamente su capacidad para procesar datos almacenados en su memoria, lo que les permite tomar decisiones con una notable autonomía. En particular, estos algoritmos se basan en redes neuronales que utilizan el llamado "aprendizaje por refuerzo".

Así, las nuevas hipótesis dañosas pueden ser resultado de defectos en el diseño general de los sistemas de IA o del uso de datos que puedan ser sesgados sin una corrección previa o, peor aún, de la autodeterminación de los sistemas inteligentes que funcionan de forma autónoma y toman decisiones que no pueden ser previstas por sus desarrolladores y mucho menos evitables.

Los sesgos inherentes en los algoritmos pueden llevar a errores de identificación y decisiones discriminatorias, impactando la equidad y la justicia en la aplicación de la tecnología.

Esta pérdida de dirección que afecta al creador, propietario o programador del sistema inteligente, plantea otro problema jurídico relevante: el de dilucidar a quién debe imputársele la responsabilidad por el daño causado por el robot dentro de este margen de autonomía[5].

La Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica, establece que «*...ahora la humanidad se encuentra a las puertas de una era en la que los robots, bots, androides y otras formas de inteligencia artificial cada vez más sofisticadas parecen dispuestas a desencadenar una nueva revolución industrial*».

---

[5]NUÑEZ ZORRILLA, M. *Inteligencia Artificial y Responsabilidad Civil. Régimen Jurídico de los daños causados por robot autónomos con inteligencia artificial*, Editorial Reus, Madrid 2019, p. 13.

Dicha Resolución incluye entre sus propuestas la de «... *crear a largo plazo una personalidad jurídica específica para los robots, de forma que como mínimo los robots autónomos más complejos puedan ser considerados personas electrónicas responsables de reparar los daños que puedan causar, y posiblemente aplicar la personalidad electrónica a aquellos supuestos en los que los robots tomen decisiones autónomas inteligentes o interactúen con terceros de forma independiente*»[6].

En este contexto, surge la controvertida propuesta de otorgar una personalidad jurídica a los robots. Idea probablemente errónea dado que, aunque la ley concede personalidad jurídica a las personas jurídicas, estas entidades están constituidas por personas humanas que actúan de manera libre y consciente. Es decir que, de atribuir responsabilidad a un ser inanimado o a un software, siempre existirá detrás una persona susceptible de ser declarada responsable.

Se ha sostenido que los robots podrían responder con su propio valor económico, embargándose su software o su estructura física[7]. Sin embargo, descartamos la posibilidad y conveniencia de atribuirles personalidad jurídica, y nos inclinamos por considerarlo una "cosa": bien material con valor económico (art. 16 CCCN).

Así, sería más coherente, atribuirles la categoría de «*cosas*», pues encuadra perfectamente con su propia definición: "Los bienes materiales se llaman cosas" (Artículo 16 CCCN). Frente a ello, y ante la ausencia de una regulación específica, la responsabilidad por la actividad de ciertas actividades y cosas riesgos parece más adecuada.

En suma, un robot no puede ser responsable directo por los daños que cause (art. 1749 CCCN responsabilidad por el hecho propio). El titular registral (dueño) y el sujeto que tenga a su cargo el mantenimiento del *soft-ware* (guardián), responderán en forma concurrente.

6. NECESIDAD Y PROPUESTA DE UNA REGULACIÓN ESPECÍFICA

[6] https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_ES.html

[7] CORVALÁN, J.; DANESI, C.: *Responsabilidad civil de la Inteligencia Artificial.Tratado de Inteligencia Artificial y Derecho.* T. III, Thomson Reuters La Ley, Buenos Aires, p.303, (2021).

El principio rector de la constitucionalizacion del derecho de daños es que "todo daño a la persona, cualquiera sea su origen o naturaleza, debe ser reparado". La persona es el centro del derecho y éste ha sido creado para su protección preventiva, unitaria e integral. Por lo tanto, si nos encontramos ante un daño a la persona, sus consecuencias deben ser reparadas[8].

El objetivo principal es que no queden daños sin resarcir y que quien introduce un riesgo a la sociedad sea garante del mismo.

La implementación de una normativa adaptada para la IA halla asidero en los principios constitucionales. El artículo 16 garantiza la igualdad, el artículo 17 protege la propiedad en todas sus formas, y el artículo 19 consagra el principio de *neminem laedere*. Resulta imperiosa una regulación que tutele de forma equitativa y confiera seguridad jurídica a las víctimas de daños causados por las nuevas tecnologías.

La Unión Europea aprobó este 1 de agosto la primera ley en el mundo que regula la Inteligencia Artificial[9] cuya aplicación obligatoria comenzará en dos años. La misma aborda temas como la transparencia, la rendición de cuentas, la protección de los derechos fundamentales y la seguridad; buscando un equilibrio entre la innovación con la protección de los ciudadanos.

Establece un marco para la regulación enfocado en el nivel de riesgo de la inteligencia artificial, reconociendo tres categorías: los sistemas que suponen un riesgo inaceptable, los sistemas de alto riesgo y los sistemas de riesgo limitado. Quedando prohibidos los que "suponen un riesgo inaceptable".

Los sistemas de reconocimiento facial para vigilancia masiva en espacios públicos sin consentimiento y justificación legal son considerados de riesgo inaceptable y están prohibidos con el fin de proteger los derechos y libertades individuales. La identificación biométrica ha mostrado sesgos que afectan la objetividad y pueden llevar a errores de identificación y discriminación. Sin embargo, su uso puede ser autorizado en excepciones estrictas mediante permisos judiciales.

---

[8] FERNÁNDEZ SESSAREGO, Carlos. "El Daño Moral" LA LEY 21/07/2014, 21/07/2014, 1 – LA LEY 2014-D, 902.

[9] https://artificialintelligenceact.eu/es/chapter/1/

La ley se enfoca en los sistemas de IA de alto riesgo, que afectan significativamente la salud, seguridad y derechos fundamentales. Establece responsabilidades para los proveedores y exige evaluaciones de riesgo y medidas de mitigación antes y después de la comercialización. Además, regula el uso de la IA para prevenir aplicaciones como la automatización de ciberataques.

En cuanto a la legitimación pasiva, la ley europea establece diferentes niveles de responsabilidad según el riesgo del sistema de IA disponiendo que cualquier distribuidor, importador, implantador u otro tercero será considerado proveedor de un sistema de IA de alto riesgo y tendrá las mismas obligaciones. Esto incluye poner su nombre en un sistema existente de alto riesgo, o si se altera la finalidad de un sistema para hacerlo de alto riesgo. El proveedor original del sistema debe cooperar con el nuevo proveedor y facilitarle la información y el acceso técnico necesarios.

Siguiendo este enfoque de la Comisión Europea, se propone una clasificación de la IA según el nivel de riesgo. Esta clasificación permitiría una regulación más precisa, adaptada a los riesgos específicos de cada tipo de tecnología.

En consonancia con ello, todos los proveedores deben cumplir con regulaciones pertinentes a mantener la privacidad y la protección de datos y garantizar la supervisión humana del sistema de IA. Resultando objetivamente responsables por los daños que la IA pueda causar, independientemente de la causa.

Resulta necesaria la creación de un registro a fin de asociar fácilmente al robot con los proveedores y otros datos pertinentes.

Asimismo, la normativa debería regular expresamente la responsabilidad del mantenimiento y actualización del software de los sistemas inteligentes. Siendo esencial para prevenir daños derivados de malfuncionamientos.

Los programadores deben tener una responsabilidad particular, ya que son responsables de los datos y su manejo en sistemas de IA.

En consonancia con ello, la ley debe prevenir el uso malintencionado de la IA, como en la automatización de ciberataques.

Recordemos que el art. 1710, inc. “b” del CCC precisa que el deber de no dañar también puede ser vulnerado si una persona no adopta las

medidas de prevención que razonablemente, de acuerdo con la buena fe y según las circunstancias del caso, se hallaban a su cargo[10].

Finalmente, resulta indispensable que la normativa prevea la creación de un régimen de seguro obligatorio de responsabilidad civil para las nuevas tecnologías que utilizan los sistemas de IA y establezca un fondo de compensación que garantice la reparación de los daños causados por IA ante la ausencia de un seguro.

7. REFLEXIONES FINALES

Ante el rápido desarrollo de tecnologías disruptivas, resulta imperioso que el sistema jurídico evolucione y regule la inteligencia artificial a fin de tutelar los derechos fundamentales delas personas asegurando la justicia y la seguridad jurídica.

El futuro es hoy y la necesidad de una reparación integral de daños derivados del uso de la IA es inminente. El desarrollo de una normativa específica que se base en la clasificación de riesgos, permitirá abordar de manera efectiva los daños causados por la IA.

De *lege lata*, nuestro régimen legal vigente tiene el potencial para dar respuestas a estos desafíos partiendo de los principios de la responsabilidad objetiva y otros mecanismos vigentes de protección de la persona.

De *lege ferenda*, en consonancia con los principios de la responsabilidad objetiva, resulta imperiosa la sanción de una norma específica, inspirada en la reciente Ley de la Unión Europea, que clasifique los sistemas inteligentes según su riesgo y grado de autonomía, y prevea la responsabilidad en cada caso, contemplando aquellos que derivan de los sesgos algorítmicos. En particular, a fin de conferir seguridad jurídica y protección de los derechos fundamentales de las personas, será esencial: la creación de un registro a fin de asociar la IA con los proveedores; la implementación de seguros y un fondo de compensación que garantice la reparación de los daños.

---

[10] PICASSO, S. – SÁENZ, L., *Tratado de Derecho de Daños*, La Ley, 2019, t. I, p. 108.

LA ASUNCIÓN DE RIESGOS EN LOS DAÑOS DERIVADOS DE INTELIGENCIA ARTIFICIAL CON CARACTERÍSTICAS DE AUTOAPRENDIZAJE Y AUTONOMÍA

Por Rosario Echevesti[1] y Casiano Highton[2]

I. CONCLUSIONES

1. La eximente de asunción de riesgos no puede operar en los daños causados por sistemas de IA con características de autoaprendizaje y toma de decisiones autónomas. Por sus características de autonomía en las decisiones, no es posible considerar que estos sistemas exhiban un riesgo notorio, específico ni previsible que la víctima pueda voluntariamente asumir al punto de interrumpir el nexo causal (art. 1719 CCCN).

2. Cuando estos sistemas actúan conforme a lo programado, no hay un riesgo específico y evidente cuya asunción por parte de la víctima pueda romper el nexo causal (los riesgos genéricos de la vida en sociedad como el de subir a un auto, cruzar la calle, o caminar por la vereda, no implican asunciones de riesgo).

3. Por su parte, cuando las decisiones aparezcan como no esperadas, no puede hablarse de un riesgo asumido, en tanto no puede haber sido conocido, ni por ende previsible, ni por ende voluntariamente asumido por la víctima.

II. FUNDAMENTOS

1. ASUNCIÓN DE RIESGOS. GENERALIDADES. CARACTERÍSTICAS DEL RIESGO ASUMIDO

Hay asunción de riesgos cuando alguien decide participar de una actividad determinada a sabiendas de que ello implica un peligro y que, de su intervención, podría derivar un daño. La asunción de riesgos "suscita una

---

[1] Profesora Adjunta Derecho Privado II (UNLP).

[2] Profesor Adjunto Obligaciones Civiles y Comerciales y Derecho de Daños (UBA).

serie de supuestos en los cuales la víctima se expone de manera consciente y voluntaria a un peligro específico creado por otro"[3].

Sin perjuicio de la amplitud lingüística de la expresión, para que la asunción de riesgos adquiera alguna relevancia en el ámbito de la responsabilidad civil, es necesario indagar la repercusión que pueda tener en la procedencia de la obligación de reparar el daño que acontece cuando ese riesgo -potencia- se efectiviza en el perjuicio.

Para arribar a una respuesta plausible, cabe realizar una serie de precisiones.

En primer lugar,entendemos por riesgo la contingencia o proximidad de un daño y/o la posibilidad de que un daño se produzca.

Ahora bien, dentro de esta noción, y a efectos de analizar la figura que nos ocupa, cabe realizar una distinción. Y es aquella que se suscita entre riesgos genéricos y riesgos específicos. Sólo en el marco de estos últimos la asunción de riesgos puede adquirir cierta significación.

Es que los riesgos genéricos de la vida en sociedad no tienen ninguna incidencia en la responsabilidad civil; mientras que sí tiene relevancia la conducta de la víctima del daño cuando ésta asumió un riesgo específico, que además debe exceder los riesgos normales, ordinarios o genéricos. La más autorizada doctrina así lo ha entendido[4].

Cierto es que la clasificación entre riesgos normales o anormales, genéricos o específicos, típicos o atípicos, puede presentarse confusa en determinadas ocasiones. El encuadre "dependerá en definitiva de las expectativas que se asume deberían estar presentes en quienes participan de determinada actividad. Dichas expectativas dependerán de lo que resulte

---

[3] PREVOT, Manuel y MAYO, Jorge, "La idea de aceptación de riesgos en materia de responsabilidad civil", LA LEY 31/08/2009, 1, LL 2009-E, 992.

[4] Entre otros, ZAVALA DE GONZÁLEZ, Matilde, Resarcimiento de Daños, Tomo 4, Hammurabi, 1999, p. 287, CALVO COSTA, Carlos, "Asunción de riesgos y consentimiento del damnificado. Parecidos, pero diferentes", LA LEY 03/09/2014, 03/09/2014, 1, LA LEY 2014-E, 749. Cita Online: AR/DOC/2913/2014; PICASSO, Sebastián, "La antijuridicidad en el Proyecto de Código", LL 30/08/2013, 30/08/2013, 1; LL 30/08/2013, 1; LL 2013-E, 666. Cita Online: AR/DOC/3184/2013; SILVESTRE, Norma O., "Asunción de riesgos y consentimiento del damnificado en el Proyecto de Código. A propósito del `turismo aventura´", LL 22/11/2013, 22/11/2013, 1; LL 2013-F, 854; Cita Online: AR/DOC/3328/2013).

previsible, de acuerdo a la experiencia, a la información que las partes posean y a lo que regularmente suele suceder"[5].

La falta de tratamiento legislativo que respecto de la figura exhibía el Código derogado, provocó que existiera discrepancia doctrinaria en torno a su validez como eximente.

La figura se encuentra receptada hoy en el texto del art 1719 del CCCN que, en su parte pertinente dispone:

"*Asunción de riesgos. La exposición voluntaria por parte de la víctima a una situación de peligro no justifica el hecho dañoso ni exime de responsabilidad a menos que, por las circunstancias del caso, ella pueda calificarse como un hecho del damnificado que interrumpe total o parcialmente el nexo causal.*"

Claro que "asumir un riesgo no debe ser sinónimo de consentir el daño que pueda derivarse de dicho evento; la vida en sociedad nos enfrenta a numerosas situaciones cotidianas plagadas de riesgos que afrontamos a diario (desde cruzar una calle hasta viajar en un ferrocarril), pero no por ello debemos concluir que de resultar dañados en alguna de esas actividades hemos consentido los perjuicios y no podamos reclamar su reparación[6]".

De este modo, la asunción de riesgos, como regla no es un eximente de la responsabilidad, y lo será únicamente cuando el hecho de haber asumido ese riesgo, interrumpa el nexo causal (1719 CCCN).

La figura, entonces, requiere que la víctima tenga conocimiento del riesgo, y se exponga voluntariamente[7].

De este modo, el resultado dañoso derivado de una situación en la que exista asunción consciente de un riesgo por parte de quien lo sufre debe

---

[5] TOLOSA, Pamela - GONZÁLEZ RODRÍGUEZ, Lorena, "Asunción de riesgos y consentimiento del damnificado en el nuevo Código Civil y Comercial", Publicado en: RCyS2015-IV, 46 Cita: TR LALEY AR/DOC/902/2015).

[6] CALVO COSTA, Carlos, "Asunción de riesgos y consentimiento del damnificado. Parecidos, pero diferentes", Publicado en: LA LEY 03/09/2014, 1 - LA LEY2014-E, 749 Cita: TR LALEY AR/DOC/2913/2014).

[7] CALVO COSTA, Carlos, *Derecho de las Obligaciones*, ed Hammurabi, 2023, pág 679).

ser, en definitiva, imputable la propia víctima en términos causales para poder operar como eximente.

Dicho esto, es importante recabar sobre las características que debe poseer un riesgo para que pueda ser susceptible de asunción voluntaria, en fin, para que pueda ser tenido en consideración a la hora de computarlo como eximente cuando el daño se concreta.

Si bien las imprecisiones del lenguaje y la versatilidad de las clasificaciones han hecho que la doctrina haya echado mano a diversos calificativos, en esencia el riesgo, para poder ser asumido, deber ser, en primer lugar, conocido.

Existe consenso en sostener que el riesgo ha de ser patente y de la suficiente entidad como para exigir del dañado un acto de asunción o rechazo. Es que la asunción es el contenido de un acto voluntario, con discernimiento, intención y libertad. En esos términos comienza el texto del actual art. 1719 "la exposición voluntaria por parte de la víctima…"

Además, aquella potencialidad riesgosa que se decide afrontar, debe tener un alcance concreto y específico (no genérico). Se ha propuesto la locución de "riesgo específico consentido", lo que implica admitir que sólo en relación con los riesgos específicos —y no a los genéricos— la asunción del riesgo por parte de la víctima puede tener alguna trascendencia eximitoria o excluyente de la responsabilidad[8].

Es que en realidad lo que aquí sucede, es que la víctima debe encontrarse en condición de poder representarse la posibilidad de ocurrencia del daño que, en potencia, representa el riesgo concreto que asume. De allí que ese riesgo debe resultar obvio, evidente, manifiesto, fácilmente asequible, en fin, ser la revelación de la potencia de un daño, cuya ocurrencia y vinculación con ese riesgo, es razonablemente previsible.

Lo expuesto, advertimos, nos ubica nuevamente en un terreno donde los discursos de culpa y causa se superponen.

La atribución de responsabilidad por aquellas conductas que, incrementando el riesgo permitido o tolerable como parte de la vida cotidiana, producen resultados inaceptables para el sistema normativo,

[8] MARCHAND, Silvina - PARELLADA, Carlos A. - BURGOS, Débora, "La asunción del riesgo ¿Causa eximente o de justificación?", Publicado en: LA LEY 08/09/2009, 1 - LA LEY 2009-E, 1065).

genera indudablemente una indefinición en sus límites axiológicos de tanto o mayor problema que los propios de la causalidad adecuada y que se pretende evitar.[9]

Se ha dicho que esa exposición por parte de la víctima a un riesgo que podría haber evitado, es lo que la coloca en una situación de culpabilidad idónea para fracturar el nexo causal[10].

Podríamos decir entonces que la víctima, a través de su conducta de exponerse a un riesgo palmario, del que puede sin esfuerzo preverse la ocurrencia de un perjuicio, fue quien "causó" su propio daño.

Más allá de la superposición denunciada, lo cierto es que, como consecuencia lógica de lo expuesto, deben quedar excluidos de toda posibilidad de aceptación aquellos riesgos que queden por fuera de toda posibilidad de representación. Riesgos que alguna doctrina ha denominado impropios o anormales de la actividad, por su condición de inasequibles en términos de previsibilidad.

Se ha sostenido que la distinción tiene su relevancia por cuanto en general se ha entendido que el damnificado ha aceptado los riesgos que son propios de la actividad que decidió compartir, pero no si se trata de riesgos que no se producían normalmente[11].

2. LA ASUNCIÓN DE RIESGOS EN EL MARCO DE DAÑOS GENERADOS POR IA CON CARACTERÍSTICAS DE AUTOAPRENDIZAJE Y TOMA DE DECISIONES AUTÓNOMAS

El derecho de Daños tal como lo hemos estudiado y tratado hasta ahora ha quedado evidentemente desactualizado, se ha ido alejando la realidad jurídica, de la realidad fáctica, nos encontramos ante los nuevos paradigmas de la revolución digital y tecnológica, con un evidente y claro

---

[9] RAMOS MARTINEZ, María Florencia, "La relación de causalidad en el derecho de daños"Ed. Rubinzal - Culzoni pág. 1, 2024).

[10] CALVO COSTA, Carlos, *Derecho de las Obligaciones*, ed Hammurabi, 2023).

[11] TRIGO REPRESAS, Félix A., La noción de las "eximentes" y su vigencia en el Derecho argentino. Eximentes y causas de justificación. Los presupuestos y las eximentes, en Revista de Derecho de Daños, 2006-1, Edit. Rubinzal-Culzoni, Santa Fe, 2006, pág. 107.

distanciamiento de las teorías clásicas de la responsabilidad civil, contexto que requiere un abordaje del tema específico y actualizado.

Es necesario dedicarle un tratamiento especial al desarrollo tecnológico, a la inteligencia artificial y a su vinculación con la responsabilidad. Ello en el convencimiento de que la importancia irá aumentando hacia el futuro porque los daños estarán cada vez más asociados al uso de las nuevas tecnologías -que usan inteligencia artificial- y que se encuentran en un constante desarrollo exponencial.

La inteligencia artificial (IA) funciona mediante una combinación de algoritmos, modelos matemáticos y grandes volúmenes de datos para simular ciertos aspectos de la inteligencia humana.

La IA es un campo en constante evolución, y nuevas técnicas y mejoras se desarrollan continuamente para hacer que los sistemas sean más precisos y eficientes.

Una de las características más importantes, es que la IA va autoaprendiendo y toma sus propias decisiones, con lo cual toma distancia respecto de la "voluntad" de su creador o programador.

Tal como sabemos, los sistemas de IA aprenden en base a datos recolectados, lo cual les permite tomar por sí mismos decisiones, según hayan sido programados. Esto es lo que se denomina toma de decisiones automatizadas.

El algoritmo, de manera autosuficiente, gestiona problemas que se le plantean y los resuelve sin necesidad de que se lo haya programado para la resolución de estos específicos planteos. Dicho de otro modo, la IA es capaz de solucionar problemáticas para las que no se encontraba originalmente programada. Los algoritmos que se usan en las técnicas de aprendizaje automático -machine learning-, y más especialmente los utilizados en el aprendizaje profundo -deep learning-, están programados para aprender y adquirir cada vez mayor autosuficiencia en la resolución de problemas.

Nos preguntamos si es posible, en ese escenario, invocar la asunción de riesgos como eximente, en el caso de que una persona que utilice un sistema de IA con esas características, resulte a la postre dañada como consecuencia de una decisión tomada -y/o ejecutada- por ese sistema.

Apenas volvamos a indagar en el análisis de las características que un riesgo debe tener para poder ser asumido, que reseñamos anteriormente, encontraremos que la eximente no puede operar en este ámbito.

En primer lugar, para que la asunción pueda tener lugar, debe ser el fruto de un acto voluntario. La acción voluntaria de asumir el riesgo se sustenta en el discernimiento, la intención y la libertad. El quid, creemos, se encuentra en la intención, en tanto la asunción no puede considerarse intencionada si no se conoce adecuadamente el riesgo.

El riesgo, para ser asumido voluntariamente, primero debe ser conocido. Hablamos anteriormente de un riesgo notorio, palmario, evidente. Ahora bien, no son pocas las evidencias científicas que indican que las personas típicamente no son conscientes de los riesgos a los que están sometidas[12].

Además tanto los humanos como los algoritmos que utiliza la IA están abiertos a contener sesgos de diversa especie, La diferencia radica en que los humanos podemos reflexionar sobre esos sesgos, y los algoritmos en definitiva, no son más que entidades inconscientes que manipulan mecánicamente símbolos a los que no son capaces de asignar significado.

A partir de lo expuesto podemos decir que los seres humanos somos propensos a caer en las heurísticas y sesgos porque nuestra manera de razonar es en general intuitiva y rápida, y en ese contexto tomamos decisiones, a veces con poca información o con información errónea.

Si pensamos en una situación en la que se esté haciendo uso de un sistema de IA, el vertiginoso ritmo y la inmediatez que el modo de funcionar propio del sistema nos suele imponer, seguramente sea un ámbito más que propicio para caer en el artificio de los actos sesgados.

A ello debemos agregar que, a efectos de analizar el efectivo conocimiento o siquiera la cognoscibilidad del riesgo, se nos impone una mirada mucho más estricta ante casos de personas vulnerables (edad, educación, condición social, consumidores, etc).

En este sentido, entendemos que la mera utilización de un sistema con las características reseñadas, difícilmente pueda encuadrarse en una asunción voluntaria de un riesgo por parte del usuario común, ante quien raramente esos riesgos se presentarán de forma evidente.

---

[12] Maximiliano Ferrer y José María Lezcano "Anotaciones sobre cuestiones de la responsabilidad civil y la inteligencia artificial. Actores, seguros y la aceptabilidad del riesgo", Memorias de las 51 JAIIO - SID - ISSN: 2451-7496 - Página 85).

Ahora bien, dijimos antes también que, de acuerdo a lo que ha entendido la doctrina, el riesgo que intencionadamente se asume, debe, además, ser un riesgo concreto.

La voluntad de asunción por parte de la víctima debe estar circunscripta, dirigida a someterse voluntariamente a un riesgo determinado, circunstanciado. Para eso, el daño que puede surgir si ese riesgo se concreta, le debe resultar previsible. A tal punto que, reiteramos, el reproche a la víctima pareciera referirse a su hecho culposo cuando "por las circunstancias del caso" pueda calificarse como interruptivo del nexo causal (art. 1719).

De allí que, aun cuando un usuario se encuentre en conocimiento de un riesgo, eso por sí solo no implica consentir el daño si ese riesgo se concreta.

Como dijimos: la víctima debe haber asumido un riesgo que se presentó ante sí de un modo palmario, evidente, poniéndola en condiciones de representarse la ocurrencia de un daño. La pregunta es qué riesgos podrían considerarse "patentes" y por ende, vinculados con un daño razonablemente previsible, en lo relativo al uso de un sistema que opera con IA, con funciones de autoaprendizaje y de autonomía en la toma de decisiones.

En nuestro sistema, lo causal finca en lo previsible (aquello que sucede según el curso normal y ordinario de las cosas, 1726, 1727 CCCN). Lo normal, lo evidente y lo anticipable es lo que acontece regularmente, de ordinario, según la experiencia de la vida. Lo otro sería, entonces, aquello que escapa a cualquier posibilidad de anticipación o previsibilidad.

De allí que los daños derivados de las "decisiones" que un sistema de IA ejecute de acuerdo con los parámetros que razonablemente se esperan, con su modo de operar regular y habitual, según el modo en que ha sido programada y los datos de los que se la ha alimentado, derivan de un riesgo genérico, igual que el que puede representar cualquier otra actividad -aun riesgosa-, y cuya asunción no resulta susceptible de ser encuadrada en un hecho de la víctima que fracture el nexo causal.

Pero en los sistemas de IA con un rango de actuación que implica la toma y ejecución de decisiones autónomas, las decisiones, llegado cierto punto se vuelven imprevisibles hasta para su propio creador. En ocasiones, ante la toma de una decisión autónoma, es imposible anticipar el recorrido para explicar el modo en que el sistema de IA resolverá, o siquiera

posteriormente poder explicar por qué el sistema de IA resolvió de una determinada manera y no de otra.

Los algoritmos en numerosas oportunidades suelen tomar atajos impensados por el programador -o por nadie-, o bien obtienen un resultado inesperado y/o no deseado al momento de su creación.[13]

Ante este tipo de situaciones, aun estando en conocimiento, comprensión y control del código fuente original, quizás no sea posible anticipar el resultado, ni determinar por qué el algoritmo se comportó de determinada forma, cuando se habría esperado que actúe de otra.

En fin, la IA suele presentar cierta opacidad en la toma de decisiones, lo cual descarta la posibilidad de asunción un riesgo concreto, cuando el daño deriva de un comportamiento imprevisto del sistema[14]. Mucho menos podría entenderse que el riesgo era de una evidencia tal, que la conducta (culposa?) de la víctima al asumirlo pueda ser interruptiva del nexo causal, en los términos en que opera la norma del art. 1719.

Así planteado, el eximente de asunción de riesgos parece quedar circunscripto a un escasísimo ámbito de aplicación en el ámbito de los daños derivados del uso de IA, es decir, a situaciones puntuales en las que pueda afirmarse que una víctima haya causado su propio daño, al asumir de manera voluntaria un riesgo evidente, conocido y concreto, del que deriva un perjuicio previsible. No pudiendo jamás operar ante riesgos genéricos, ni ante decisiones autónomas de la IA, que resulten imposibles de anticipar en parámetros de una razonable previsibilidad.

---

[13] COLOMBO, María Celeste, "La responsabilidad civil derivada de la utilización de algoritmos en el derecho de consumo", 1a ed. - Ciudad Autónoma de Buenos Aires : La Ley, 2023. Libro digital, PDF Archivo Digital: descarga y online ISBN 978-987-03-4546-6, pág. 28).

[14] COLOMBO, Maria Celeste, ob. cit.

LA IA COMO RIESGO DEL DESARROLLO. LOS PRINCIPIOS PREVENTIVO Y PRECAUTORIO

Por Esther H. Silvia Ferrer[1], Leonardo F. Fernández[2], Lucía Martínez Lima[3] y Paula Noelia Bermejo[4*]

I. CONCLUSIONES

1. Las aplicaciones de IA resultan posibles de encuadrar como riesgos del desarrollo.

2. La función preventiva resulta una herramienta útil en los casos de riesgos del desarrollo por IA ya que permite evitar el agravamiento del daño cuando el mismo haya comenzado a producirse.

---

[1] Profesora Adjunta de Contratos Civiles y Comerciales. Profesora Adjunta de Derecho de Familia y Sucesiones de la Facultad de Derecho de la Universidad de Buenos Aires, donde también es. Profesora de grado, posgrado y doctorado. Investigadora con dedicación exclusiva en la misma casa de estudios. Miembro del Instituto de Investigaciones Jurídicas y Sociales "A. L. Gioja". Directora de Proyectos de investigación UBACyT "Vulnerabilidad, inteligencia artificial, transhumanismo y riesgo del desarrollo. La sociedad de la incertidumbre y el mercado. Los posibles daños: ética y/o eficiencia", Programación Científica 2023, Código: 20020220300170BA. E-mail: esthersilviaferrer@gmail.com

[2] Profesor Adjunto Regular de Contratos Civiles y Comerciales, de la Facultad de Derecho, Universidad de Buenos Aires. Integrante formado de proyectos UBACYT. Especialista Universidad de Oxford Euromoney Training, Summer School for International Financial Law. Actual integrante de proyecto UBACyT "Vulnerabilidad, inteligencia artificial, transhumanismo y riesgo del desarrollo. La sociedad de la incertidumbre y el mercado. Los posibles daños: ética y/o eficiencia." Autor de diversas publicaciones.

[3] Becaria UBACyT de Maestría en Derecho Comercial y de los Negocios en el proyecto UBACyT "Vulnerabilidad, inteligencia artificial, transhumanismo y riesgo del desarrollo. La sociedad de la incertidumbre y el mercado. Los posibles daños: ética y/o eficiencia", Programación Científica 2023, Código: 20020220300170BA. Auxiliar de segunda en la materia Contratos Civiles y Comerciales, de la Facultad de Derecho, UBA.

[4] Profesora Adjunta Interina de Contratos Contratos Civiles y Comerciales y Auxiliar de Segunda de Derecho de Familia y Sucesiones de la Universidad de Buenos Aires. Magíster en Derecho Comercial y de los Negocios de la misma casa de estudios . Integrante del Proyecto UBACyT "Derecho y sociedad: teoría y prácticas para el abordaje de los conflictos transversales a la niñez y la adolescencia." Coordinadora del Seminario "Vulnerabilidad y Derecho" del Instituto de Investigaciones Gioja (Facultad de Derecho UBA). E-mail: paulaberrmejo@derecho.uba.ar.

* La presente ponencia integra los desarrollos del proyecto de investigación UBACYT "Vulnerabilidad, inteligencia artificial, transhumanismo y riesgo del desarrollo. La sociedad de la incertidumbre y el mercado. Los posibles daños: ética y/o eficiencia", Programación Científica 2023, Código: 20020220300170BA y colaboraron en la misma **Lidia Garrido Cordobera, Alejandra Noemí Tevez, Salvador Francisco Etchevers, Roque Piccinino Centeno Garrido, Silvana Cristina Vivó, Agustina Belén Levinsonas, María de la Cruz Ceballos Arenas y Constanza Sofía Fernández.**

3. Asimismo y fundamentalmente, resulta aplicable a la IA como riesgo del desarrollo el principio precautorio cuando no haya certeza científica de la producción del daño.

4. Son legitimados activos para solicitar tales medidas, además de las autoridades de contralor, los damnificados mediante acciones individuales o colectivas, las asociaciones de consumidores, los fabricantes, el Defensor del Pueblo y cualquier tercero con interés legítimo, tales como aseguradoras o fondos de garantía.

I. FUNDAMENTOS

1. INTRODUCCIÓN A LA PROBLEMÁTICA

La Inteligencia artificial (IA) es un término acuñado por primera vez por McCarthy[5], para referirse a distintos desarrollos sobre redes neuronales, que actúan en base a algoritmos programados por humanos para el desarrollo de tareas, se trata de fórmulas que identifican patrones y aplican soluciones. Así esta herramienta resulta valiosa para todo tipo de actividades, especialmente en la identificación de patrones que permiten hacer previsiones, lo que es particularmente útil para el análisis y proyección de modelos de negocio.

Advertimos que si bien es una disciplina con un avance exponencial, ha generado como otros avances lanzados al mercado, en algunos casos, después de la interacción masiva con usuarios fallas, errores, bugs y defectos o factores del uso que afectan la programación original, generando daños traducibles en afectación de derechos. Cierto es que hasta el momento se han retirado del mercado algunos programas dañosos, otros, fueron corregidos, pero esto ha sido con posterioridad a la generación de daños, dado que en muchos casos, la falta de técnicas adecuadas para detectar fallas en las etapas previas al lanzamiento ha derivado en que pudiesen identificarse estos errores en base a la experiencia de usuarios.

Puede decirse entonces, que si bien la implementación de la IA supone la asunción de riesgos que surgen de sus etapas de creación, que

[5] El informático lo utilizó por primera vez durante la conferencia "Dartmouth Summer Research Project on Artificial Intelligence" en Dartmouth College durante el verano de 1956.

generan daños y para los cuales aún no hay técnicas adecuadas para su detección temprana; los beneficios que la misma puede suponer hacer inevitable su implementación.

En Argentina no se ha sancionado ninguna normativa específica. En este sentido, debe mencionarse que el derecho es dinámico, y debe adecuarse a la sociedad; por lo que siempre debe acompañar el avance científico, y no frenarlo.

En nuestro derecho la propia Carta Magna prevé en el artículo 75 inciso 18, el derecho al progreso que tiene su correspondencia en las normas de derechos humanos. En concordancia, el art. 75 inc. 22 en cuanto incorpora al bloque de constitucionalidad y convencionalidad, entre otros instrumentos internacionales, el Pacto Internacional de Derechos Económicos Sociales y Culturales -específicamente, los arts. 15 y 42- y la Declaración Universal de Derechos Humanos -art. 27- donde se establece el derecho de acceso a la ciencia y el progreso.

Propender al progreso supone en este caso, no prohibir completamente la IA por los riesgos que puede suponer, dado que sería una regulación irrazonable. En cambio, se debe encuadrar la misma en el sistema de derecho las pautas para el uso de la misma, y en especial, las medidas de precaución que pueden tomarse para evitar daños.

En la presente ponencia planteamos soluciones a la problemática que presenta ante el desarrollo de IA generador de daños detectables con posterioridad a su lanzamiento al mercado y en función a la aparición de nuevas técnicas, supuesto de riesgo del desarrollo.

2. EL DERECHO DE DAÑOS Y LA IA

La masificación de la oferta de productos y servicios elaborados con IA, y sus consecuencias jurídicas en la sociedad actual plantean nuevos desafíos para la responsabilidad civil por los daños causados por estos, su prevención y su precaución.

Los desarrollos de IA, son programados por personas que proveen las instrucciones (algoritmos) para resolver problemas, pero también pueden aprender por sí mismas cómo resolver problemas (es decir, reprogramarse), a través del llamado “machine learning”. Esta última modalidad es hasta cierto punto, impredecible.

Frecuentemente, estos desarrollos se ofrecen al mercado en versiones gratuitas para ser probadas, y dado lo incompleto de los sistemas de testeo de calidad: fallan. Todas estas situaciones, hacen que el consumidor se encuentre ante un daño sufrido injustamente, al cual el derecho debe asignar un responsable. Pero por sobre todo debe propender a la evitación o agravamiento del daño.

3. EL RIESGO DEL DESARROLLO

La noción de "riesgo del desarrollo" hace referencia a los daños causados por un producto, que al momento de su lanzamiento al mercado por un productor o fabricante, era considerado inocuo en base a los métodos de verificación de calidad existentes a esa fecha, pero que como consecuencia del avance tecnológico, se descubre su potencialidad dañosa.

En otros términos, "se trata de productos que al momento de su distribución entre los consumidores, son *subjetivamente inocuos*, considerando los conocimientos y procedimientos técnicos existentes al momento de dicha distribución, pero *objetiva y potencialmente nocivos*, aunque dicha nocividad no resulta detectable sino en un momento futuro y a merced de la aparición de nuevas técnicas."[6] Por ende, el concepto de riesgo del desarrollo, excluye a los daños causados por un producto cuya nocividad era objetivamente detectable a partir de los conocimientos y técnicas existentes al momento de su lanzamiento al mercado y que, sin embargo no fueron detectados.

Asimismo, este concepto en virtud de su marco normativo, puede ser aplicado a los servicios ofrecidos en el mercado cuya calidad y técnicas aplicadas eran consideradas inocuas en base a los métodos de control existentes al momento de ser ofertados, pero que luego se descubre su potencialidad dañosa.

El ofrecimiento masivo de productos y servicios desarrollados con IA, exponen al usuario o consumidor en algunos casos, a riesgos que no

[6]FERRER DE FERNÁNDEZ, Esther; "La responsabilidad por productos elaborados y el riesgo del desarrollo en el contexto del derecho del consumidor"; La Ley. 2016. Cita Online: AP/DOC/38/2016, artículo basado en la tesis doctoral de FERRER DE FERNÁNDEZ, Esther, "La responsabilidad civil por productos elaborados y riesgo del desarrollo en el contexto del derecho del consumidor desde la perspectiva del Análisis Económico del Derecho", Facultad de Derecho UBA, defendida el 29/04/2009, dirigida por la Prof. Dra. Lidia Garrido Cordobera.

pueden ser comprobados por una falta de pruebas de calidad adecuadas, al momento de lanzarse al mercado, pero que sin embargo pueden ser dañosos. Esta situación configura a la IA como un potencial riesgo del desarrollo.

4. EL PRINCIPIO PREVENTIVO Y PRECAUTORIO

Comprendemos en esta problemática del riesgo del desarrollo en general y en especial, producida por utilización de IA que, corresponde la aplicación de los principios preventivos y precautorios. Por estos temas, venimos bregando desde hace años y en las últimas Jornadas Nacionales de Derecho Civil, a instancia de una ponencia de nuestro equipo de investigación, se incluyó en el punto 14 de las Conclusiones de la Comisión de Daños por unanimidad se expresó "la función preventiva de la RC constituye una herramienta útil en casos de riesgos del desarrollo a los fines de evitar el agravamiento o continuación del daño"[7].

Esto resulta así pues, el deber de prevención que encuentra basamento legal en el art. 1710 del CCCN establece que "toda persona tiene el deber, en cuanto de ella dependa, de: a) evitar causar un daño no justificado; b) adoptar, de buena fe y conforme a las circunstancias, las medidas razonables para evitar que se produzca un daño, o disminuir su magnitud; si tales medidas evitan o disminuyen la magnitud de un daño del cual un tercero sería responsable, tiene derecho a que éste le reembolse el valor de los gastos en que incurrió, conforme a las reglas del enriquecimiento sin causa; c) no agravar el daño, si ya se produjo".

La función preventiva del derecho de daños tiene un cariz netamente humanista primordialmente pero ello resulta así, no sin destacar también el aspecto económicamente eficiente que se rescata de la misma.

En tal sentido confiere importancia tener en cuenta los estudios enjundiosos formulados por la "Teoría del Análisis Económico del Derecho", pergeñada por Ronald Couse[8] y Guido Calabresi[9] y continuada

---

[7] Punto 14 de las Conclusiones de la Comisión 3 de Derecho de Daños de las Jornadas Nacionales de Derecho Civil, desarrolladas en 2022 en la Ciudad de Mendoza.

[8] COUSE R., "The problem of social cost" Journal of law and economics, 1960.

[9] CALABRESI,G "El coste de los accidentes. Análisis económico y jurídico de la responsabilidad civil" trad. BISBAL, Ed. Ariel S.A.,Barcelona, 1984.

por Cooter-Ulen[10] Schaefer & Ott[11] y Torres López[12], entre muchos otros, que valorizaron la prevención desde el ámbito de la eficiencia, para lo cual se requiere considerar que el costo de la prevención ha de resultar menor al del daño y que asimismo, debe hallarse en manos de quien ha de reparar en su caso, como aspectos centrales a evaluarse al momento de imputarse el deber de prevenir[13].

En esta cuestión requiere resaltarse que las reparaciones deben ser fácilmente determinables ex ante, a fin de que al potencial dañador o responsable le resulte posible realizar el cálculo de maximización y evite la producción invirtiendo en prevención concreta.

Por otra parte, podemos encontrarnos frente a casos de posible encuadre del principio preventivo, en el inciso b) del art. 1710, es decir, acciones tendientes a evitar el agravamiento del daño cuando éste ya se haya producido.

Frente a los usos de la IA que configuren riesgo del desarrollo y en el supuesto de agravamiento del daño, se podrá solicitar el retiro del mercado de estos productos y servicios; lo que implica, en este caso, la "desconexión" y/o borrado del programa o desarrollo de IA.

En cuanto al principio precautorio parte de la existencia de una incertidumbre sobre la dañosidad del producto. Habiendo sido detectado un riesgo potencial, este principio obliga a las autoridades a evaluar si dicho riesgo es admisible o no, y en base a esa evaluación determinar las medidas a tomar [14].

---

[10] COOTER-ULEN "Derecho y economía", Fondo de cultura económica, México, 1998.

[11] SCHAEFER & OTT, "Manual de análisis economico del derecho civil" Ed. Tecnos, Madrid, 1991.

[12] TORRES LOPEZ "Análisis económico del derecho. Panorama doctrinal", Ed. Tecnos, Madrid 1987.

[13] Ver al respecto FERRER DE FERNANDEZ Tesis de doctorado "La responsabilidad civil por productos elaborados y el riesgo del desarrollo en el contexto del derecho del consumidor desde la perspectiva del análisis económico del derecho", inédita, 2009

[14] CORTE CONSTITUCIONAL, 12/10/2004, Sentencia C- 988 de 2004, Voto del Magistrado Ponente: Dr. HUMBERTO SIERRA PORTO. Expediente D-4884.

Así el principio precautorio importa una perspectiva de "control anticipado del riesgo potencial" a fin de evitar e impedir daños irreparables, siempre teniendo en cuenta la razonabilidad como criterio para su aplicación.

Por otra parte, encontramos sustento para aplicar el principio precautorio, en materia de riesgo del desarrollo en general y en especial de la utilización de IA, cuando no haya certeza científica de la producción del daño; en lo dispuesto en el art. 42 de la Constitución Nacional, el art. 1710 del CCCN, la Ley General del Ambiente N° 25.675 y en la Ley del Consumidor N° 24.240.

Son legitimados activos para solicitar tales medidas, además de las autoridades de contralor, los damnificados mediante acciones individuales o colectivas, las asociaciones de consumidores, el Defensor del Pueblo, los fabricantes y cualquier tercero con interés legítimo, tales como aseguradoras o fondos de garantía.

Las funciones preventivas y precautorias resultan una herramienta útil para prevenir daños a los consumidores y usuarios con especial referencia en los desarrollos que recurren a la utilización de IA.

PRUEBAS Y CONSECUENCIAS. CLAVES DE LA RESPONSABILIDAD PATRIMONIAL POR DAÑOS CAUSADOS POR LA INTELIGENCIA ARTIFICIAL[1]

Por Martín A. Frúgoli[2]

I. CONCLUSIONES

1. Quienes omitan mostrar y abrir el funcionamiento y utilización de su inteligencia artificial (*disclosure*), cargan con una presunción de responsabilidad civil en su contra que sólo podrá desvirtuarse mediante la demostración de la causa ajena.

2. Quienes muestren y abran el funcionamiento y utilización de su inteligencia artificial, pueden demostrar su no culpa.

3. Ante situaciones actuales impredecibles e inverificables por desconocimiento, aun luego de la apertura (*disclosure*), tales como las redes neuronales profundas y las máquinas de vectores de soporte, deberán contar con seguros razonables de responsabilidad civil.

II. FUNDAMENTOS

1. EL COSTO DE DETECTAR EL USO ANTIJURÍDICO DE LA INTELIGENCIA ARTIFICIAL Y EL COSTO DE LAS SANCIONES

Un análisis extremadamente básico desde el Derecho y la Economía, podría sostener que se deben orientar los incentivos de manera correcta para los fines (loables) que se buscan. Para ello, cualquier agente racional puede analizar el costo de ser detectado o descubierto en su conducta antijurídica, y la sanción efectiva que podría recibir por ello (probabilidad), luego de lo cual decidirá su curso de acción, como ser, utilizar o no utilizar a la

---

[1] Sin perjuicio de los avances tendientes a mejorar estos sesgos en el ámbito de la inteligencia artificial (p.v. v.gr.: BREM, Alexander - RIVIECCIO, Giorgia, "Artificial Intelligence and Cognitive Biases: A Viewpoint", n° 44 – Journal of Innovation Economics & Management 2024/2 DOI: 10.3917/jie.044.0223, disponible en https://www.researchgate.net/).

[2] Profesor Adjunto de Daños y Obligaciones en U.N.R

inteligencia artificial para incrementar beneficios particulares sin importar los daños actuales o potenciales de otros.

A su vez, se evalúan (consciente o inconscientemente) las facilidades o fricciones[3] existentes para determinadas acciones u omisiones (relacionado esto a las ciencias del comportamiento y al uso, abuso, o indiferencia, en torno a los sesgos cognitivos que, por supuesto, no resultan ajenos a la inteligencia artificial[4]).

Ahora bien, un primer problema crucial que se presenta al momento de detectar o descubrir aquel uso antijurídico de la inteligencia artificial es ¿cómo se probará este uso antijurídico? Pues, el primer reparo que existe, y existirá al respecto será que, ante cualquier intento de apertura del software de la particular inteligencia artificial de que se trate, la negativa a su pretendida apertura florecerá para todo aquel que realice un uso antijurídico de la misma (pues se suele decir que; "el ladrón no va a tocar el timbre antes de robar" o, con alguna precisión más técnica que pretende aplicar un principio penal al civil; "nadie está obligado a declarar contra sí mismo"). Incluso, dicha negativa podría presentarse por otras razones que no tengan que ver, necesariamente, con usos antijurídicos de la inteligencia artificial, como ser, datos sensibles, datos privados, datos comerciales, obligaciones conexas, etc.

Así, entre dos empresas y ante el pedido de una para abrir la otra, se podría argumentar que son datos comerciales privados y no pueden abrirse o mostrarse a requirentes. Por su parte, entre empresas y consumidores, se podría argumentar que la apertura de cualquier software de inteligencia

---

[3] P.v. al respecto una propuesta muy interesante en: ACCIARRI, Hugo and AZAR-BAUD, María José and MARZETTI, Maximiliano, "Inteligencia Artificial, Compliance y Derecho del Consumo Estructuras de gobernanza empresarial y estatal frente al empleo de algoritmos durante la pandemia y más allá." (Artificial Intelligence, Compliance and Consumer Law. Corporate and State Governance Structures Facing the Use of Algorithms during the Pandemic and Beyond) (July 5, 2021). Disponible en SSRN: https://ssrn.com/abstract=3898876 or http://dx.doi.org/10.2139/ssrn.3898876 .

[4] Como el caso de los patrones oscuros, v.: MILLS, Stuart and WHITTLE, Richard, "Detecting Dark Patterns Using Generative AI: Some Preliminary Results" (October 27, 2023). Disponible en SSRN: https://ssrn.com/abstract=4614907 o http://dx.doi.org/10.2139/ssrn.4614907 ; en Argentina p.v. WAJNTRAUB, Walter, "Patrones comerciales oscuros y cumplimiento contractual en el derecho del consumidor", TR LALEY AR/DOC/1491/2024.

artificial excede el ámbito individual o colectivo del conflicto, o que se presentan datos privados, confidenciales, o sensibles.

Entonces, sin perjuicio de las aspiraciones de los/as operadores/as jurídicos (algunas de las cuales quedan en la mera expresión de deseos que, en el mejor de los casos, se plasma en una norma) el primer punto para intentar una orientación de incentivos loables no resulta sencillo en la realidad práctica y requiere asumir la complejidad y acercarse a esta para soluciones concretas.

Pero un acercamiento a estos controles podría ofrecerse mediante la demostración de la existencia de auditorías y monitoreos técnicos que transparenten el uso no antijurídico de la inteligencia artificial. También podrían presentarse programas de *compliance*[5], y muchas otras demostraciones más que cabe imaginar (por ejemplo: incorporar políticas internas que garanticen el derecho de los afectados o potenciales afectados a obtener una explicación comprensible de las decisiones automatizadas que les afectan y a revisarlas técnicamente –con trazabilidad suficiente-; realizar auditorías periódicas de algoritmos; garantizar que los sistemas de inteligencia artificial sean evaluados regularmente para detectar posibles fallos o sesgos; ajustarse a permanentes estándares globales de máxima seguridad y transparencia que cumplan los desarrolladores y operadores de inteligencia artificial; creación de comités de ética que revisen el impacto social y ético de la inteligencia artificial antes de su implementación; revisión regular de logs y registros para detectar cualquier acceso no autorizado, modificaciones sospechosas o patrones de uso inusuales; desarrollar o utilizar herramientas diseñadas específicamente para detectar deepfakes, manipulación algorítmica en redes sociales y otras plataformas, etc. etc.).

Sin embargo, estas aproximaciones podrían ser insuficientes para lograr una profunda, verificable y objetiva investigación tendiente a detectar en forma verosímil el uso –palpable u oculto[6] - de la inteligencia artificial.

---

[5] VIGO, Rodolfo L., "Del Estado de Derecho Legal al Estado de Derecho Constitucional", Sup. Const. 2010 (febrero), 1-LL 2010-A, 1165).

[6] V.gr.: Cám. Ap. Civ. y Com. (Sala IV), Rosario, "FELICI, LEONOR SUSANA C/ BANCO SUPERVIELLE SA S/ MEDIDA ASEGURAMIENTO DE PRUEBAS 21-02905241-4 Nro. Expediente: 108/2020". En este caso se solicitó (y se rechazó) la siguiente información: "2º) Informe los usuarios y clientes de ese Banco que se encuentren incluidos en el Sistema Previsional Argentino (ANSES), indicando nombre y DNI de cada uno de

No obstante, tampoco será suficiente, y más allá del control interno o externo contratado que tenga quien utilice inteligencia artificial, lo cierto es que, todo aquél que decida no aportar sus softwares de inteligencia artificial que demostrarían –al menos parcialmente- cómo es el uso presente y pasado de esa inteligencia artificial, debiera cargar con las consecuencias de tal actuar (como veremos seguidamente partiendo de conflictos particulares).

2. UN CONFLICTO SIMILAR EN SITUACIONES PARTICULARES

Seguidamente pasaré revista de algunas particularidades –ad similique se presentan entre consumidores de servicios bancarios y entidades financieras. Veamos:

Un consumidor o varios consumidores sospechan verosímilmente de una serie de conductas antijurídicas que se presentan mediante el uso de herramientas de inteligencia artificial por parte de una entidad financiera. Por tal razón, solicitan una serie de informes y acceso al conocimiento del uso de la inteligencia artificial que lleva a cabo esta entidad financiera, por sí o por relaciones contractuales conexas desconocidas con certeza por aquellos consumidores.

Sin embargo, ante este pedido, sigue una férrea oposición por parte de esta entidad financiera. Los argumentos de uno y otro lado suelen ser los siguientes:

Por parte de la entidad financiera se sostiene que los datos solicitados son confidenciales, tienen secreto bancario, son sensibles, no se los puede obligar a presentarlos porque se obligaría a declarar contra sí mismos y, además, exceden los límites del conflicto –individual o colectivo-.

---

ellos y que cobran sus haberes por caja de ahorro de la seguridad social abierta a tal fin. 3º) Informe los débitos, seguros y coseguros que se les debitan automáticamente o manualmente en sus cuentas de seguridad social a los usuarios beneficiarios del Sistema Previsional Argentino (ANSES). 8º) Informe los préstamos otorgados en los últimos 5 años contados desde la fecha del respectivo oficio hacia atrás, a beneficiarios del Sistema Previsional Argentino (ANSES).". El argumento de la Sala para rechazar el pedido de esta información a la entidad financiera, pese al rechazo del recurso interpuesto por esta última, fue: "Más allá de lo resuelto precedentemente, debe aclararse que no integrará el informe requerido al banco demandado lo solicitado en los puntos 2, 3 y 8 (fs. 9 y vta.), en tanto se trata de información que alude a la relación del banco con terceros, cuya confidencialidad se halla constitucionalmente protegida (arg. art. 43, CN)."

Frente a ello, los consumidores manifiestan que, en rigor, los arts. 6 y 7 de la ley de habeas data N° 25.326, de ninguna manera impiden el suministro de los datos que se solicitan para una causa judicial no penal en que son parte estos consumidores, y que los datos y accesos que se solicitan no son informes "confidenciales" o "sensibles" de terceros, sino datos autorizados por el art. 5 inc. 2 de la mencionada ley. Datos que también se encuentran autorizados por la ley 21.526 mediante el art. 39 inc. a. Sostienen, asimismo, estos consumidores, que si eventualmente se considerase "privada" o "sensible" la información solicitada que, por otro lado, se utiliza casi sin reparos por los proveedores al contratar con consumidores con la diferencia que estos no conocen con precisión cómo se utilizan estos datos y dónde terminan (que, insisten, no lo es por disposición expresa de los arts. 2 y 5 inc. 2 b y c de la ley 25326), podrá el tribunal previamente realizar el relevo expreso del secreto o confidencialidad, a fin de ser aportados a la causa abriendo aquella información y brindando los datos que de allí se extraigan.

En definitiva, argumentan estos consumidores, que la información que solicitan la requieren para acreditar (o desacreditar) su demostración del uso de la inteligencia artificial actual o potencialmente dañadora. Y que, en todo caso, se podrán reservar las actuaciones para los fines de la particular causa judicial, ya que ostenta razones de interés público y requiere de un contralor difuso de constitucionalidad, pues hace al cumplimiento de las normas –v.gr. ley 24240-, desde el Estado Constitucional de Derecho por el cual todos/as deben velar (incluyendo los poderes del Estado ante los compromisos internacionales asumidos conf. art. 75 inc. 22 CN)[7].

[7] V.gr.: Juzgado 1ra. Inst. Civil y Comercial 1ra. Nom., Rosario, "IEZZI GUTIERREZ MARÍA FABIANA C/ BETA S.A Y OTROS S/ DEMANDA DE DERECHO DE CONSUMO 21-23547542-9", Auto de proveído de pruebas de fecha 28.02.2024, Tomo: 2024 Folio: Resolución: 41, el argumento aquí fue que no se podía analizar la pertinencia de la prueba en esa etapa procesal, sino en la sentencia (por razones de la norma ritual santafesina que así lo indica). Algo similar pero en otro ámbito: El 5 de noviembre de 2021 la Procuración General de la Nación emitió dictamen en «Asociación Civil por la Igualdad y la Justicia (ACIJ) c/ EN – AFIP s/ amparo Ley 16.986» (Expte. CAF40994/2019/CS1-CA1), aconsejando rechazar el recurso extraordinario federal interpuesto por la Administración Federal de Ingresos Públicos contra la sentencia dictada el 18 de febrero de 2020 por la Sala III de la CNCAFed, mediante la cual se condenó a dicha entidad estatal a entregar la información solicitada por la organización actora (vinculada con empresas que recibieron beneficios fiscales).

El conflicto anterior tiene algunas resoluciones judiciales que inclinan su balanza hacia la negativa de acceso a la información solicitada[8], y otras hacia el otro extremo[9].

Ahora bien, en estos casos no es posible omitir la escasa fuente de control que existe en materia consumeril, más allá de los hermosos deseos del legislador, pues, la autoridad de contralor de la ley consumeril no parece tener demasiados recursos para lograr un efectivo y óptimo control del uso interno de la inteligencia artificial por parte de responsables potenciales ante daños eventuales y masivos (menos aun cuando se trata de microdaños porque pasan generalmente desapercibidos). Tampoco pareciera un incentivo suficiente intentar años de litigio mediante acciones colectivas que van en contra del sesgo cognitivo del presente[10] y que están –en general- repleta de fricciones y costos -fundamentalmente de tiempo y dinero-.

---

[8] ZAMIR, Eyal - TEICHMAN, Doron, "Behavioral Law and Economics", Oxford University Press, New York, 2018, p. 89.

[9] ZAVALA DE GONZÁLEZ, Matilde y GONZÁLEZ DE ZAVALA, Rodolfo, Las cargas dinámicas en el Código Civil y Comercial, en obra colectiva "Responsabilidad Civil en el Código Civil y Comercial", Director Fernando MARQUEZ, Ed. Zavalía, Buenos Aires, 2015, T. 1, p. 341 y ss.

[10] Redes neuronales profundas: Una red neuronal profunda se basa en la capacidad de una red de neuronas artificiales para aprender gradualmente sobre la base de su programación y los resultados del procesamiento de datos. Al igual que en las neuronas humanas, los enlaces útiles se fortalecen y los superfluos se descartan. En esta metodología se utilizan varias capas de neuronas interconectadas para encontrar patrones en los datos de forma progresiva, o para hacer conexiones lógicas o relacionales entre puntos de datos (Negnevitsky, 2011). Dado que no hay una "neurona" que codifique una parte específica del proceso de toma de decisiones y se llega a la decisión sobre la base de la red de "neuronas", en este punto del desarrollo tecnológico no es posible reducir la decisión a pasos lógicos específicos (Bathaee, 2018). Por consiguiente, las redes neuronales profundas implican una toma de decisiones que es compleja de descifrar.

Máquinas de vectores de soporte: Los humanos tienen la capacidad de imaginar espacios tridimensionales, es decir, crear una imagen mental de un plano usando tres variables; cualquier cosa más allá de las tres dimensiones no es de fácil acceso para nuestro cerebro (Carroll, 2009). Las máquinas de vectores de soporte resultan bastante misteriosas para los humanos porque llegan a una decisión encontrando patrones geométricos entre muchas variables que los humanos no pueden visualizar fácilmente. Por lo tanto, las curvas no lineales generadas por las máquinas de vectores de soporte son cajas negras para la mente humana por su gran dimensión.

(Fuente de esta nota: "El aporte de la inteligencia artificial y las TIC avanzadas a las sociedades del conocimiento. Una perspectiva de Derechos, Apertura, Acceso y

Como observamos, este primer conflicto no es ficción.

3. CONSECUENCIAS. RESPONSABILIDAD CIVIL

De lo anterior, parece consistente pensar en una regla que tenga en cuenta los costos de las condiciones en que se encuentran las partes en un conflicto y, con base a eso, proyectar las consecuencias posibles.

Es decir, aquel usuario que no quiera presentar su *disclosure*, o apertura de sus sistemas que utilice de inteligencia artificial, que verifiquen y detecten los usos que se hicieron de la inteligencia artificial, podrá cargar con tales consecuencias y generar una presunción de responsabilidad civil en su contra, sea por presunción de relación de causalidad o por aplicación de responsabilidad objetiva ante actividades riesgosas o peligrosas.

Por el contrario, aquellos que decidan abrir sus cajas, softwares de inteligencia artificial y sistemas, podrán invertir con sus aportes los reclamos de los que son blancos y, de esta manera, mostrarán sus diligencias y previsibilidades con usos loables de la inteligencia artificial.

Lo anterior resulta consistente con la regla del *cheapest cost avoider*, y las cargas probatorias dinámicas, explicada esta última y propuesta en forma amplia por un sector de la doctrina nacional, vía interpretación del art. 1735 del CCyC.

Lo anterior, también podría resolverse de manera similar aplicando un factor de atribución subjetivo en caso de apertura del software y sistemas de inteligencia artificial (algo similar al anterior "daño con la cosa"). Y, en caso de negativa, aplicando un factor de atribución objetivo por el riesgo de la cosa ("daño por la cosa") o actividad riesgosa.

Sin embargo, existe un segundo problema quizás más complejo, y es que aun cuando se permita o decida abrir el sistema de inteligencia artificial (*disclosure*), el mismo podría no ser descifrado o entendido. Tal lo que ocurre con las llamadas "cajas negras", como las redes neuronales profundas y las máquinas de vectores de productos. En tal caso, al momento de escribir estas líneas pareciera tener como posible solución la cobertura asegurativa de la responsabilidad civil que se genere por tales actividades riesgosas no del todo conocidas hasta hoy.

Múltiples actores", Ediciones UNESCO, disponible en http://creativecommons.org/licenses/by-sa/3.0/igo).

LA IA Y LA AUTONOMÍA PRIVADA

Por Mario César Gianfelici[1] y Florencia Romina Gianfelici[2]

I. CONCLUSIONES

1. Cláusulas de *disclaimer*. Las cláusulas de *disclaimer* incluidas entre los Términos y Condiciones que rigen el funcionamiento de los distintos modelos de lenguaje de la IA, son inválidas cuando afecten derechos indisponibles de los usuarios del sistema.

2. Utilización de los datos personales. La recopilación, procesamiento y utilización de los datos personales por parte de la IA exige, necesariamente, requerir el consentimiento previo y expreso de sus titulares. Para satisfacer dicha exigencia no es suficiente recurrir al silencio del interesado como medio de manifestación de su voluntad.

II. FUNDAMENTOS

1. CLÁUSULAS DE *DISCLAIMER*

Es común que entre los Términos y Condiciones de los modelos de lenguaje de la Inteligencia Artificial que utilizamos en la actualidad, como Meta AI, Chat GPT, Copilot, Gemini, se incluyan cláusulas de dispensa de responsabilidad, conocidas en el derecho angloamericano como *Disclaimer*.

En tal orden, se introducen disposiciones de "No garantía" por la cual se informa al usuario que el contenido es proporcionado "tal cual" está, sin garantizar la exactitud, actualidad o idoneidad de éste. Más aún, se agrega que quienes lo desarrollan no se responsabilizan por "los daños o pérdidas derivadas del uso de aquel contenido".

---

[1] Doctor en Ciencias Jurídicas y Sociales (FCJS-UNL). Profesor titular ordinario por concurso en Derecho de las Obligaciones y Profesor titular ordinario por concurso en Derecho de los Contratos. Facultad de Ciencias Jurídicas y Sociales, Universidad Nacional del Litoral.

[2] Abogada. Especialista en Derecho de Daños (FCJS-UNL). Especialista en Derecho Informático (UBA). Especialista en Derecho de la Empresa (FCJS-UNL). Profesora ayudante de cátedra. Facultad de Ciencias Jurídicas y Sociales, Universidad Nacional del Litoral.

Justifican tal normativa invocando limitaciones en los datos de entrenamiento de tales modelos de lenguaje, entendiendo que aquellos pueden estar desactualizados o incompletos, en tanto que su base de conocimiento parte de datos históricos, que incluso es posible que reflejen errores o sesgos humanos.

Asimismo se ha invocado que tales modelos de lenguaje pueden interpretar mal el contexto o la intención detrás de una pregunta, lo que lleva a respuestas inexactas. Sumado a que algunos temas son ambiguos o complejos.

Además, el hecho de que la información disponible en Internet es susceptible de cambiar rápidamente y su conocimiento pueda no estar actualizado en tiempo real, exigiría que el usuario verifique la información que el sistema de IA le proporciona, especialmente si se trata de decisiones importantes o situaciones críticas.

Entendemos que todos esos justificativos son insuficientes para admitir la validez de las cláusulas de referencia, cuando están de por medio los derechos indisponibles de las personas, como la vida y la salud, a tenor de lo que dispone expresamente el art. 1743, CCCN. Tal cuando la consulta verse sobre diagnóstico médico, tratamiento de enfermedades, contraindicaciones de medicamentos, etc. Es que la IA, a diferencia de otras fuentes de información, despierta una confianza especial en el usuario fundada en la creencia normal de que aquella es certera por conjugar, supuestamente, la totalidad de los conocimientos existentes sobre el tema.

Es verdad que siempre existe el riesgo de que pese a todo la información suministrada sea defectuosa, pero no es menos cierto que la IA debe responder por ello. En cuanto ha creado, para el público, la posibilidad de acceder de manera sencilla y automática a una bastedad de información, que muchas veces podría derivar en un cóctel de datos inadecuados a la situación planteada por el usuario, impactando perjudicialmente en su persona.

Por tal razón, cuando estén de por medio derechos indisponibles, no será suficiente para excluir la responsabilidad de la IA con consignar una cláusula de dispensa de responsabilidad. Sino que, al efecto, deberá adoptarse los siguientes recaudos: a) los resultados que suministre deberán ir acompañados de información clara y transparente sobre las limitaciones del modelo de lenguaje; b) deberá abstenerse de proporcionar información que pueda ser interpretada como consejo médico o profesional; y c) remitir

a los usuarios a fuentes confiables y actualizadas para obtener información precisa.

Si pese a ello, el usuario experimentara un daño derivado de la desatención de tales advertencias, cabría invocar la incidencia del hecho de la víctima para excluir total o parcialmente su responsabilidad (conf. doc. art. 1729, CCCN).

2. UTILIZACIÓN DE LOS DATOS PERSONALES

Si bien los datos personales constituyen un bien que su titular puede disponer (conf. doc. art. 1720, CCCN), la Ley 25.326 de Protección de Datos Personales, exige que aquel, al efecto, preste su consentimiento de manera libre, expresa e informada, debiendo constar por escrito o por otro medio que se le equipare (art. 5, Ley 25.326).

La IA se escuda para cumplir con tal exigencia legal en que la reticencia del titular para autorizar el uso de sus datos personales va en desmedro, entre otros, de su capacidad para aprender y mejorar, su velocidad y eficiencia, su diseño y funcionamiento o bien restringir su capacidad para tomar decisiones autónomas.

Sin embargo, consideramos que ello no es argumento suficiente para que la IA quede exceptuada de respetar dicha norma. Por ello los desarrolladores, como cualquier integrante de la comunidad, deben diseñarla de modo tal que tales modelos de lenguaje requieran el consentimiento de referencia a los titulares respectivos, de modo expreso y escrito como lo exige la ley.

A tal fin no es suficiente implementar la inveterada práctica de recurrir al silencio del titular como manifestación positiva de su voluntad (conf. doc. art. 263, CCCN).

En consecuencia, la utilización de datos personales sin que su titular haya prestado el consentimiento del modo indicado precedentemente, puede generar la responsabilidad del desarrollador del modelo del lenguaje del que se trate.

RESPONSABILIDAD CIVIL POR LOS DAÑOS DERIVADOS DE LA ROBÓTICA

Por Mario César Gianfelici[1] y Florencia Romina Gianfelici[2]

I. CONCLUSIONES

1. Regulación legal. Si bien no contamos con normas que regulen específicamente la responsabilidad civil derivada de la robótica, resulta necesario precisar cuáles son los supuestos de responsabilidad que serían aplicables de conformidad al régimen jurídico vigente, no resultando admisible la autoregulación del sector.

2. Categoría jurídica. No resulta conveniente atribuir personalidad jurídica electrónica a los robots y otros dispositivos, actividades o procesos gobernados por IA. Corresponde que se los considere objetos de derecho.

3. Responsabilidad directa e indirecta. Siendo el robot una "cosa" (art. 16 CCCN) no resulta aplicable la responsabilidad por el hecho propio ni la del principal por el hecho del dependiente o la de los padres por los hechos de los hijos.

4. Responsabilidad por el riesgo o vicio de las cosas. La responsabilidad civil por los daños causados por robots es un supuesto de responsabilidad por el riesgo o vicio de las cosas. Por lo que resultan responsables su dueño y el guardián (art. 1757 y sgte. CCCN).

5. Responsabilidad por actividades riesgosas. El empleo de la robótica debe ser considerado una actividad riesgosa por su naturaleza y por los medios empleados. Por lo que resultan responsable quien la realiza, se sirve u obtiene un provecho de ella por sí o por terceros (art. 1757 y sgte. CCCN). No califica como sujeto pasivo quien simplemente

---

1 Doctor en Ciencias Jurídicas y Sociales (FCJS-UNL). Profesor titular ordinario por concurso en Derecho de las Obligaciones y Profesor titular ordinario por concurso en Derecho de los Contratos. Facultad de Ciencias Jurídicas y Sociales, Universidad Nacional del Litoral.

2 Abogada. Especialista en Derecho de Daños (FCJS-UNL). Especialista en Derecho Informático (UBA). Especialista en Derecho de la Empresa (FCJS-UNL). Profesora ayudante de cátedra. Facultad de Ciencias Jurídicas y Sociales, Universidad Nacional del Litoral.

obtiene un provecho como el consumidor, por estar disociado a la creación del riesgo.

6. Responsabilidad civil en materia de consumo. Siendo el damnificado un consumidor son responsables todos los integrantes de la cadena de comercialización (art. 40 Ley 24.240 de Defensa del Consumidor).

7. Responsabilidad civil de los profesionales de la robótica. Están sujetos al régimen de responsabilidad subjetiva en los términos del art. 1768 CCCN salvo que "se haya comprometido un resultado concreto o que el daño derive del vicio de la cosa empleada", en cuyo caso la responsabilidad es objetiva.

8. Eximentes. Varían según el supuesto general especial de responsabilidad de que se trate. Siendo objetiva sólo es invocable la causa ajena (arts. 1722 y 1729/31 CCCN) tales la incidencia causal del hecho de la víctima, el caso de fuerza mayor y el hecho de un tercero que lo configure. Igualmente constituye eximente la utilización del robot en contra de la voluntad expresa o presunta de su dueño o guardián (art. 1758 1er. parr. ult. pte. CCCN). El riesgo del desarrollo es invocable en cuanto el daño configure un caso de fuerza mayor. Siendo subjetiva bastará con demostrar la diligencia normal o el simple caso fortuito.

II. FUNDAMENTOS

1. REGULACIÓN LEGAL

No podemos hablar de robótica sin hacer alusión a la Inteligencia Artificial (IA). No obstante, no todos la tienen. Así pueden existir robots con IA y sin ella destinados a realizar tareas mecánicas y repetitivas en base a los comandos externos que reciben[3].

Recientemente el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, publicado el 12/07/24, en su art. 3, inc.1, define a los sistemas de IA como “un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos

[3] CORVALÁN, Juan G.; DANESI, Cecilia C., Responsabilidad civil de la Inteligencia Artificial en “Tratado de Inteligencia Artificial y Derecho”, 1era. Edición Thomson Reuters La Ley, Buenos Aires, 2021, tomo III, p.279

explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales"[4].

En nuestro derecho positivo no contamos con normas que regulen especialmente la responsabilidad civil derivada de la robótica.[5] Por lo que son aplicables las normas generales sobre responsabilidad civil previstas en el Libro III, Título 5, Cap. 1 del Código Civil y Comercial de la Nación.

La autoregulación del sector empresarial (Google, Facebook, Microsoft) esconde una estrategia de no rendir cuentas a nadie[6]. Es por ello, que la comunidad internacional, a través de comités, consejos y grupo de expertos, en general se ha movilizado para discutir un régimen jurídico público en torno a la IA[7].

2. RESPONSABILIDAD CIVIL DEL ROBOT

En este orden, cabe observar que atribuir responsabilidad al robot, traería aparejado excluir la concerniente a la de quien se enmascara a través de su actuación. Así, como es fácilmente imaginable, se podría recurrir al

---

[4] PARLAMENTO Y EL CONSEJO DE LA UNIÓN EUROPEA, "Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial", 12/07/24, p.46. Disponible en https://eur-lex.europa.eu/legalcontent/ES/TXT/PDF/?uri=OJ:L_202401689. Repárese que en esta oportunidad se hace referencia a la idea "máquina" no contemplado la Ley de Inteligencia Artificial (2021). COMISIÓN EUROPEA. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión, 21/04/21, p.20. Disponible en https://eurlex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF

[5] GIANFELICI, Florencia Romina, "Personalidad jurídica del Robot y la responsabilidad civil por sus hechos", en Tratado de Inteligencia Artificial y Derecho, 2da. Edición, Thomson Reuters La Ley, Buenos Aires, 2023,tomo II, p. 454.

[6] En tal sentido no compartimos el criterio seguido por las XXVIII Jornadas Nacionales de Derecho Civil (Mendoza, 2022), cuya Comisión Nº10, Transdisciplina, que abordó el tema "Inteligencia Artificial, Mercado y ética", sostuvo "la necesidad de incluir la posibilidad de la autorregulación". Disponible en https://mendozalegal.com/omeka/files/original/6def87998fdb30f4ced16899f5a94952.pdf

[7] MARTINO, Antonio A., "Ética y sistemas inteligentes" en Corvalán Juan C., Tratado de Inteligencia Artificial y Derecho, 1era edición, Thomson Reuters, La Ley, Buenos Aires, 2021, tomo I, p. 431.

robot para violar impunemente el deber general de no dañar a los demás, que se encuentra previsto expresamente por el art. 1716, Cód. Civ. y Com.

En tal sentido, la Propuesta de reglamento relativo a la responsabilidad civil en materia de inteligencia artificial (20/10/20), superando la postura del Proyecto de Informe del 2017, enuncia que "cualquier cambio necesario del marco jurídico vigente debe comenzar con la aclaración de que los sistemas de IA no tienen personalidad jurídica ni conciencia humana, y que su única función es servir a la humanidad" (inc. 6) (el destacado es propio). A partir de esto, aclara que no es necesario atribuir personalidad jurídica a los sistemas de IA.

Se deja en claro que "la persona que cree el sistema de IA, lo mantenga, lo controle o interfiera en él debe ser responsable del daño o perjuicio que cause la actividad, el dispositivo o el proceso (el destacado es propio). Ello en tanto que la persona que crea o mantiene un riesgo para el público es responsable si dicho riesgo causa un daño o un perjuicio y, por lo tanto, debe minimizar ex ante o indemnizar ex post dicho riesgo. Por consiguiente, el auge de los sistemas de IA no implica la necesidad de revisar completamente las normas en materia de responsabilidad civil en toda la Unión" (inc. 8). A mayor abundamiento, no se explica qué patrimonio garantizaría la reparación del daño causado. Sobre la base de que los robots carecen de derechos patrimoniales, se ha sostenido que podrían responder con su propio valor económico, embargándose su software o su estructura física. Mas esta idea luce desacertada, pues con la misma tónica de la personalidad robótica se le podría oponer la idea de su inviolabilidad, tal lo previsto por el art. 51 Cód. Civ. y Com. respecto de la persona humana.

3. DISTINTOS SUPUESTOS DE RESPONSABILIDAD.

Descartada la posibilidad y conveniencia de atribuir personalidad jurídica al robot, no queda otra alternativa que considerarlo una "cosa". Es que como bien se ha dicho, desde una perspectiva filosófica, "objeto" en general, es lo que "está opuesto" a la persona como sujeto cognoscente[8]. Conforme al art. 16 del Cód. Civ. y Com., "cosa" son los "bienes materiales susceptibles de valor económico". Siendo así, no cabe considerar al robot

[8] LARENZ, Karl, Derecho Civil. Parte general, trad. Miguel Izquierdo y Macías Picavea, 1a ed., Editorial Revista de Derecho Privado. Editoriales de Derecho Reunidas, Madrid, 1978, p. 51.

sujeto pasivo de responsabilidad por los daños que ocasione (responsabilidad por el hecho propio, art. 1749 Cód. Civ. y Com.)[9].

Contrariamente a lo que se ha sostenido en la doctrina[10], no cabría subsumirlo en el supuesto de responsabilidad del principal por los hechos del dependiente (art. 1753, Cód. Civ. y Com.), desde que éste debe tratarse de una persona humana. Incluso se ha llegado al extremo de sostener[11] que cabría aplicar al robot autónomo o entidad con inteligencia de aprendizaje profundo la idea de la responsabilidad de los padres por los hechos de los hijos (art. 1754 CCCN) y la de capacidad progresiva. Consideramos que tal conclusión pese a lo ingeniosa no condice con la real naturaleza jurídica que asignamos al robot, a saber, la de ser cosa y no persona.

Siendo el robot una cosa, el supuesto de responsabilidad no puede ser otro que el de la "responsabilidad por el riesgo o vicio de las cosas", previsto en el art. 1757, Cód. Civ. y Com. A tenor del art. 1758 Cód. Civ. y Com., lucen como responsables primarios y concurrentes su dueño o guardián. Se trata de un supuesto de responsabilidad objetiva[12].

Debe entenderse por dueño quién resulte ser su propietario al momento de la causación del daño, es decir quién sea titular de un derecho real de dominio sobre la cosa (art. 1941 Cód. Civ. y Com.). Y por guardián "quien ejerce por sí o por terceros, el uso, la dirección y el control de la cosa o a quien obtiene un provecho de ella" (art. 1758 Cód. Civ. y Com.). Se adopta así la tesis ecléctica de considerar guardián tanto al que tiene la guarda intelectual como la guarda provecho. Tal sería el supuesto de quien recibe en locación un robot o quien tiene a cargo su mantenimiento.

---

[9] En consecuencia no compartimos lo sostenido por el conferencista Dr. Armando Andruet, en el seno de las XXVIII Jornadas Nacionales de Derecho Civil (Mendoza, 2022), Comisión Nº10 precitada, como igualmente lo consignado en la conclusión nro. 5, en cuanto considera la necesidad de crear una nueva categoría de seres distinta a los hombres y a las cosas, a fin de poder incluir en ellas la robótica, la domática y la evolución progresía de la IA.

[10] COSOLA, Sebastián J.; SCHMIDT, Walter César, El derecho y la Tecnología, 1a ed., Thomson Reuters, La Ley, Buenos Aires, 2021, t. II, ps. 380 y ss.

[11] Ídem.

[12] PIZZARRO, Ramón D.; VALLESPINOS, Carlos G., Tratado de Responsabilidad Civil, 1a ed., Rubinzal-Culzoni Editores, Santa Fe, 2018, tomo I, ps. 255 y ss.

Sin perjuicio de lo expuesto, no cabe duda que las actividades realizadas mediante la utilización del robot califican como actividades riesgosas tanto por su naturaleza, como por los medios empleados en su realización (art. 1757 CCCN)[13].

En cuanto a la legitimación pasiva, la previsión legal del art. 1758, 2do, párr., CCCN luce amplia, en cuanto indica como responsables a: I) quien realiza la actividad, II) quien se sirve de ella, III) quien obtiene un provecho. No obstante, se ha considerado que no quedaría comprendido quien simplemente obtiene un provecho, como el consumidor (por ejemplo, quien recibe en su domicilio una pizza que le fue remitida a través de un robot delivery) por estar disociado con la creación del riesgo. Por ello, se sostuvo que para ser legitimado pasivo no será suficiente con la realización de la actividad, el servirse o tener un provecho de ella, sino que además deberá tenerse cierta facultad de control o dirección en la organización de las tareas del robot[14].

Además de los legitimados pasivos enunciados precedentemente, siendo el damnificado un consumidor, la responsabilidad se extendería, concurrentemente, al fabricante, y a todos los integrantes de la cadena de comercialización del robot quienes deben responder solidariamente respecto de los vicios causados por su intervención. Lo cual está expresamente previsto, por el art. 40 de la ley 24.240 de Defensa del Consumidor.

Independientemente de las normas internacionales que imponen reglas éticas de conducta a los profesionales de la robótica[15], estos estarían sujetos dentro de nuestro ordenamiento jurídico, a un régimen de

---

[13] GIANFELICI, Florencia Romina, "Robótica y Responsabilidad civil", SADIO, Electronic Journal of Informatic and Operation Research, 2022, Vol. 21, nº1, p.52. Disponible en https://publicaciones.sadio.org.ar/index.php/EJS/article/view/212/184 p.53 y ss. Tal es así que el reciente Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo precitado dedica el Capítulo III a los Sistemas de IA de Alto Riesgo. Igualmente en la Comisión N° 3 de las "XXVII Jornadas Nacionales de Derecho Civil" (Santa Fe, 2019), se admitió por unanimidad el carácter riesgoso de los "sistemas operados por inteligencia artificial".

[14] GIANFELICI, Mario César y GIANFELICI, Florencia Romina, "Legitimación pasiva del consumidor frente a la responsabilidad civil por actividades riesgosas o peligrosas", Revista de la Facultad de Ciencias Jurídicas y Sociales. Nueva Época, Ediciones UNL, 2020, N° 11, p. 183 y ss.

[15] GIANFELICI, Florencia, "Personalidad jurídica del robot y la responsabilidad civil …", Ob. Cit., p. 466 y ss.

responsabilidad subjetiva en los términos del art. 1768 CCCN. Salvo que "se haya comprometido un resultado concreto o que el daño derive del vicio de la cosa empleada", en cuyo caso la responsabilidad es objetiva.

4. EXIMENTES DE RESPONSABILIDAD

En los casos en que la responsabilidad es objetiva, como los analizados, sólo se admite como eximente la causa ajena (art. 1722, CCCN), entre las que cabría incluir la actividad de los hackers en cuando pudiesen interferir de manera imprevisible e inevitable en la conducta dañosa del robot (doc.art. 1730 y 1731 CCCN). Sin perjuicio de ello, no cabe soslayar que la Propuesta del Parlamento Europeo sobre Régimen de responsabilidad civil en materia de inteligencia artificial, excluye expresamente, como eximente, el supuesto en que el daño haya sido causado por un tercero ilocalizable o insolvente, que haya interferido en el sistema de IA por medio de una modificación de su funcionamiento o sus efectos[16].

Por lo contrario, cabe excluir el simple caso fortuito propio del riesgo del robot o de la actividad que éste desempeñe al causar el daño (art. 1733, inc. e., CCCN). En este sentido el Proyecto de Informe del 2016, admite que podrían producirse eventuales daños derivados de que "la programación de un robot falle, así como la de las posibles consecuencias de un fallo del sistema o de ataques informáticos contra robots interconectados".

En cuanto a los llamados riesgos del desarrollo, consideramos que sólo darían lugar a un caso de fuerza mayor eximente de la responsabilidad objetiva, en la medida que el daño generado constituya una consecuencia objetivamente imprevisible e inevitable, lo cual debe valorarse al momento de su producción. En tal sentido, el reciente Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo mencionado con anterioridad, impone una serie de requisitos para los Sistemas de IA de Alto Riesgo y un cúmulo de obligaciones a los proveedores y responsables del despliegue de sistemas de IA de alto riesgo (Sección II, Cap. III) entre las que se menciona

[16] PARLAMENTO EUROPEO, "Propuesta de Reglamento relativo a la responsabilidad civil en materia de Inteligencia Artificial, Resolución del Parlamento europeo con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de Inteligencia Artificial" (2020/2014(INL), 20/10/2020, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_ES.html.

el deber de llevar a cabo una evaluación del impacto que la utilización de dichos sistemas puede tener en los derechos fundamentales (art. 27).

Entre los supuestos de causa ajena no puede descartarse la posible incidencia del hecho del damnificado en la producción del daño (art. 1729 CCCN). En igual sentido el Reglamento europeo sobre Régimen de responsabilidad civil en materia de inteligencia artificial (2020) establece en su art. 10 que "el operador no será responsable si la persona afectada o la persona de la que esta es responsable es la única a la que se le puede achacar el daño o perjuicio causado", facultando al operador a utilizar los datos generados por el sistema de IA para demostrar la negligencia concurrente de la persona afectada. Lo que coincide con lo previsto en el Reglamento (UE) 2016/679 y otras leyes en materia de protección de datos relevantes. La persona afectada también podrá usar esos datos con fines probatorios o aclaratorios en la demanda por responsabilidad civil.

En este punto cabe hacer una referencia a las actualizaciones que exigen estos productos digitales, que constituyen una parte necesaria de ellos sin las cuales puede convertirse en obsoletos o peligrosos. Como una aplicación del deber de información, el proveedor debe comunicar al consumidor y poner a su disposición las actualizaciones que fuesen necesarias para velar por la continuidad de la vida útil del producto. Existiendo responsabilidad del consumidor si no las instalase dentro de un plazo debido o lo hiciese incorrectamente pese a las instrucciones del proveedor.

A las eximentes reseñadas, cabe agregar el posible uso del robot en contra la voluntad expresa o presunta de los legitimados pasivos (art. 1758, 1º parr. últ. pte. CCCN), lo que podría acontecer por ejemplo, en caso de robo del robot o su uso indebido por parte de quien lo tenga en su poder con fines de mantenimiento.

PROBLEMAS DOGMÁTICOS EN LOS DAÑOS CAUSADOS POR LA INTELIGENCIA ARTIFICIAL

Por Martín Juárez Ferrer[1] y José Fernando Márquez[2]

I. CONCLUSIONES

Proponemos que las Jornadas Nacionales de Derecho Civil resuelvan:

De lege lata:

1. A los fines del análisis de la responsabilidad civil, no es necesario crear nuevas categorías, tales como las "no cosas", ni tampoco otorgar personalidad jurídica a las cosas que operan bajo AI La responsabilidad civil por daños causados por máquinas que operan bajo AI (en adelante MAI), se rige por el régimen general del Código Civil y Comercial y, en su caso, de la Ley de Defensa de consumidores y usuarios.

2. No todo daño causado mediando intervención de la AI es un daño causado por la AI. El concepto tradicional de causalidad adecuada se basa en la previsibilidad, y cuando el daño no resulta previsible entonces mal puede haber tal causalidad adecuada. Puede ser necesaria una reforma o reconstrucción dogmática de las ideas de causa a partir de los problemas que genere la AI, ya que puede ponerse en crisis el concepto de causa jurídica, y eventualmente hacer necesario un nuevo criterio de imputación y atribución de conductas y daños.

3. La causación de daños con AI presenta desafíos en la identificación de los autores que causan esos daños, ya que la autoría se despega de lo material, haciéndose más estructural o funcional, y también se despega del ámbito contractual, puesto que tiende a identificarse al autor del daño con el programador o fabricante o desarrollador del sistema de AI, a la manera del sistema de la LDC o de las reglas de Product Liability en el ámbito anglosajón.

---

[1] Profesor Titular Derecho Privado VIII (UCC) y Profesor Adjunto por Concurso Derecho Privado III (Contratos) (UNC).

[2] Prof. Titular de Derecho Privado VII, Universidad Nacional de Córdoba.

4. Debe distinguirse entre la responsabilidad derivada de la utilización de MAI en relaciones de consumo de las relaciones no incluidas en la LDC.

5. El régimen legal aplicable a daños sufridos por consumidores y usuarios por MAI es el prescripto por el art. 40 de la LDC (daños causados por cosas y actividades riesgosas), en correlación con los artículos 1757 y 1758 Código Civil y Comercial. En consecuencia, serán responsables ante el consumidor y usuario todas las personas que hayan intervenido en su proceso de creación y puesta en circulación en el mercado, en forma solidaria.

6. La cuestión de la causa en los daños causados con AI también ofrece problemas en relación a la extensión del daño, derivados de eventual pérdida del lugar central que hoy ocupa la previsibilidad en la construcción de la idea de causa

De lege ferenda:

7. Es necesaria la reglamentación legal de la creación y utilización de AI, a través de un estatuto especial. A tal fin es imprescindible un amplio debate, con la participación de todos los intereses involucrados, tanto de los usuarios, potenciales damnificados, como de los operadores y productores de la inteligencia artificial.

8. Es atendible el criterio de que las reclamaciones por responsabilidad civil deben centrarse contra el operador de un sistema de AI, toda vez que es quien controla un riesgo asociado al sistema de AI, independientemente de dónde se lleve a cabo la operación y de que esta sea física o virtual.

9. Se deberá diferenciar entre actividades especialmente riesgosas, con un régimen de responsabilidad objetiva, de aquellas que no lo son, en el que se debe instaurar un régimen menos riguroso (sea a través de atribución subjetiva, o mediante una mejor posición probatoria).

II. FUNDAMENTOS: ALGUNOS PROBLEMAS DE LA CAUSA EN LA RESPONSABILIDAD POR DAÑOS CAUSADOS CON LA INTELIGENCIA ARTIFICIAL

1. NUEVAS CATEGORÍAS Y TAXONOMÍAS

Se ha propuesto la creación de nuevas categorías dogmáticas, tales como la de no-cosa, y también la ampliación del concepto de personalidad

jurídica de las cosas que funcionan u operan con AI. Por nuestra parte, creemos que ello no resulta necesario en el marco del derecho argentino vigente.

a) Cosa y no cosa.

Una primera pregunta que debe encararse es si la Inteligencia Artificial (AI) es una cosa o bien estamos ante una serie de procesos no materiales.

El desarrollo de la física moderna indica que incluso los rayos de luz son materia que viaja, y por ende, en el fondo del fondo del uso de la AI hay materia, partículas subatómicas en movimiento, y que por ende, si hay materia hay cosas.

Si la AI es una cosa entonces podría aplicarse a los daños que se causen con su uso el régimen del art. 1757 CCC, si es que la consideramos una cosa riesgosa o viciosa.

También puede considerarse que la AI no es otra cosa que una serie de procesos, es decir, no una cosa sino un conjunto de decisiones secuenciadas y al menos en parte automatizadas pero que no son cosas. Si la AI no es un bien o no es una cosa, entonces la aplicación del art. 1757 CCC resulta sólo posible si la consideramos una actividad, o mejor dicho, si consideramos que su utilización implica desarrollar una actividad riesgosa.

Esta cuestión, entonces, resulta de especial interés en orden a determinar si es aplicable o no el régimen de responsabilidad objetiva de los arts. 1757 y ss. CCC.

Por cierto que su clasificación taxonómica como cosa, bien o actividad no zanja la cuestión, puesto que todavía queda determinar si, con este encuadramiento, además es riesgosa o viciosa.

No es necesaria, por ende, la creación de nuevas categorías tales como las de no-cosa[3].

---

[3] ANDRUET, Armando S. *Escenarios utópicos o distópicos en perspectiva digital - La dialéctica del 'ser humano mejorado' y del 'artefacto humanizado'.* Exposición en la Academia Nacional de Derecho y Ciencias Sociales de Córdoba, 2.7.24.

Creemos que, en todos los casos, estamos ante cuestiones interpretativas, que no requieren legislación sobre el particular, sino la clásica labor de la dogmática jurídica de interpretación e integración, o al decir de Riccardo Guastini[4], de construcción de la norma.

b) Personalidad jurídica de la IA

1.1.1. En el ámbito europeo se ha propuesto como marco para la responsabilidad civil por daños causados con la AI acudir a la responsabilidad del principal por el hecho del dependiente o responsabilidad vicaria[5].

Por ello es útil la pregunta de si es posible identificar o trabajar la responsabilidad de la AI como una responsabilidad vicaria. Por nuestra parte creemos que en la responsabilidad vicaria ya hay un criterio de imputación causal cuya relación con la previsibilidad es más débil.

Un elemento favorable para encuadrar a los casos de daños causados por AI en la responsabilidad vicaria es que en Argentina estas reglas no exigen voluntariedad el acto, sino que simplemente se responde por el daño con independencia de la imputación subjetiva de la acción.

Sin embargo, en nuestro país la AI no es una persona, y los criterios para el otorgamiento de personalidad jurídica no parecen estar alineados para su otorgamiento. Además de ello debe notarse que el legislador argentino ha sido muy reticente a la utilización de la técnica de la personalidad jurídica en tiempos recientes, en los que el fideicomiso no es una persona jurídica.

Adicionalmente, creemos que esto no es necesario para nuestro derecho, en donde las reglas del CCC y de la LDC ofrecen soluciones razonablemente completas desde la perspectiva del derecho a la reparación integral de los daños, y por ello no resulta necesario acudir a estas figuras,

---

[4] GUASTINI, Riccardo. *Rule-scepticism restated.* En GREEN, Leslie y LEITER, Brian (eds.). *Oxford Studies in Philosophy of Law.* New York, Oxford University Press, 2011.

[5] MORGAN, Phillip. *Tort Law and AI. Vicarious Liability*, incluido en LIM, Ernest y MORGAN, Philip (eds.). *The Cambridge Handbook of Private Law and Artificial Intelligence.* Cambridge, 2024, p. 135 y ss.

sin perjuicio de que una regulación de la AI en general, como proponemos de lege ferenda, pueda contener alguna solución en este sentido.

2. EL VÍNCULO CAUSAL

En segundo lugar, surgen una serie de interrogantes relativos al vínculo causal entre AI y daño.

a) Causalidad adecuada e IA

Nos preguntamos si el estándar de causalidad adecuada, con su clásica formulación en el sentido de lo que era previsible que ocurriera de acuerdo al curso normal y ordinario de las cosas. Creemos que esta es una pregunta seria, que debe ser abordada cuidadosamente.

Es necesario evitar la tentación de simplemente afirmar de modo dogmático que la AI es riesgosa y de que cualquier cosa que ocurra es lo que suela ocurrir, ya que ello transformaría al Derecho de Daños en una disciplina de Derecho Público, basada eminentemente en consideraciones de justicia distributiva, en donde la responsabilidad sería absoluta, ya que no habría interrupción posible del nexo causal. Advertimos con preocupación una tendencia a suponer que cualquier daño en el que ha intervenido la AI es un daño causado por la AI lo que eventualmente puede servir para reparar daños al costo de atribuirlos sin fundamento causal (por ende, a quien no pudo evitarlos, entre otros problemas), tendencia vinculada con el ataque a litigantes con deep pocket[6] y otras formas de pauperización de la dogmática del derecho de daños.

Ciertamente, la causalidad adecuada no es un criterio científico sino un criterio jurídico de imputación objetiva, basada en la previsibilidad. Es decir, la causalidad adecuada es una de las especies de posibles criterios de imputación objetiva, que se basa en la previsibilidad.

Dado que pueden presentarse casos en que el criterio de imputación bajo causalidad adecuada pueda resultar subinclusivo[7] de casos en que podría pensarse como justo puede ser conveniente revisar la construcción dogmática del concepto de *causalidad adecuada* y eventualmente su

---

[6] CALABRESI, Guido, *Una vista desde la Catedral.* Completar referencia-

[7] SCHAUER, Frederick. *Las reglas en juego.* Madrid, Marcial Pons, 2004, p. 89 y ss.

reemplazo por otro (lo que, creemos, implicaría de modo necesario una reforma legislativa en el CCC o una norma específica al efecto).

b) La idea de causa en daños con intervención de la AI.

Da la impresión de que la atribución de responsabilidad en daños causados por la AI puede poner en crisis el criterio de previsibilidad para la determinación de causa.

Dado que en ARG el criterio de atribución casual se vincula a la previsibilidad, no parece sencillo la ampliación a otros criterios de imputación objetiva sin una intervención legislativa.

Por cierto el legislador puede decidir atribuir causa, en forma de imputación objetiva de consecuencias, pero es algo tan distinto a la causalidad adecuada, es decir, a la atribución por curso de acción ordinario evitable y previsible, que es difícil reconocer el concepto de causa jurídica allí. Estaríamos ante un nuevo criterio de imputación causal, una nueva forma de causa.

3. AUTORÍA.

Un desafío es la identificación del autor en los daños causados por AI.

a) La autoría se despega de lo material:

No necesariamente hay una acción imputable que conecte autor con damnificado, sino una larga serie de acciones conectadas, atribuibles a diversas personas físicas o jurídicas, entre las que existen una serie de ellas que son seleccionadas como causa.

La materialidad de la acción se difumina y se hace tenue y por ende, la acción se hace más estructural o funcional.

b) La autoría se despega de lo contractual.

Una responsabilidad por daños causados con la AI refuerza el achicamiento de la responsabilidad contractual, ya que en muchos casos vinculará a fabricante / programador con damnificado.

Esto será un desafío para jurisdicciones en donde no existe una norma que habilite demandar a fabricantes de modo claro. En USA existe esta posibilidad de la mano de la Product Liability Law.

En ARG también existe está posibilidad en el ámbito de la LDC (art. 40 LDC). Sin embargo, en ARG esto es algo excepcional, y será de difícil funcionamiento fuera de la LDC. Una puerta de entrada podrá estar dada por la responsabilidad por actividades riesgosas (art. 1757 CCC).

4. EXTENSIÓN DEL DAÑO

Dado las dificultades de la previsibilidad en el ámbito de la AI, cabe preguntarse por la extensión del daño vinculada a la AI. En particular si es posible perfilar la extensión del daño a partir de la idea de previsibilidad.

Dada la posibilidad de reducción del rol de la previsibilidad en la imputación causal entonces la extensión del daño ya no sería modulada por la previsibilidad sino que, por el contrario, no tendría otra modulación que la inmediatez del daño producido, y una extensión más tenue hacia lo mediato. No es claro el corte causal entre lo inmediato y lo mediato

En este contexto, el riesgo del desarrollo como eximente vinculada a la falta de previsibilidad también pierde fuerza, y parece más difícil de admitir en un contexto de causa no vinculada exclusivamente a la previsibilidad.

DAÑOS OCASIONADOS POR EL MAL USO DE LA INTELIGENCIA ARTIFICIAL EN EL SISTEMA EDUCATIVO ESCOLAR

Por Carla María Kott [1] y Clidia Rodríguez Marchese[2]

I. CONCLUSIONES

A modo de preguntas e interrogatorios suficientemente válidos para el buen desempeño escolar del niño y adolescente, consideramos que la Inteligencia Artificial en el uso cotidiano y como instrumento de enseñanza en el proceso educativo, deja de lado el pensamiento crítico del propio ser humano en desarrollo.

¿Es la inteligencia artificial una conducta reprochable al pensamiento humanitario, debido a que insta a reemplazarlo y/o sustituirlo sin las experiencias previas y propias del ser humano?

¿Podemos pensar en la responsabilidad de la Inteligencia Artificial desde un factor de atribución subjetivo, en la culpa, cuando el ser humano debe confiar en la información proporcionada?

Las IA suelen tener serias dificultades para comprender los matices del lenguaje y contexto sociocultural humano, algo que los niños / adolescentes comprenden con mucha facilidad, por ejemplo, el uso del lenguaje figurativo en un texto o mismo las analogías, metáforas creativas que se suelen estimular en las aulas**. Las IA tiene serios conflictos para**

---

[1] Carla María Kott, es Abogada. Doctoranda en Derecho Civil (UBA) Magister en Derecho Civil Patrimonial. (UCA) Especialista en Derecho de Daños (UBA) Docente (UBA) Profesora Adjunta Interina en Derecho de Consumo. Profesora Adjunta Interina en Obligaciones Civiles y Comerciales. Docente (UCES) Universidad de Ciencias Empresariales y Sociales Adjunta Interina Materias Obligaciones y Contratos, Derecho Laboral, Contratos Civiles y Comerciales. Integrante del Proyecto de Investigación UBACYT 2019-2022. Docente (UBA) del Ciclo Profesional Orientado Discapacidad y Derechos. Miembro Organizativo y Asistente de varias Actividades Académicas relacionadas con el desarrollo de las materias afines. Autora y Coautora de varios artículos, revistas y libros relacionados con sus materias.

[2] Clidia Rodríguez Marchesse, es Abogada egresada de UBA, Magister en Derecho Internacional Privado. Actualmente colabora como docente en la materia Obligaciones Civiles y Comerciales de la catedra del Dr. Leandro Vergara, UBA Ejerce como abogada independiente, en redes sociales es divulgadora del derecho por medio de su cuenta @clidiamarchese.

poder desarrollarlas o contextualizarlas al momento de ser utilizadas como herramienta estudiantil.

II. FUNDAMENTOS

1. INTRODUCCIÓN:

No podemos dejar de mirar hacia los ojos de las nuevas tecnologías que fueron creciendo poco a poco y en los últimos tiempos a pasos agigantados.

La inteligencia artificial ha traspasado y hasta si se quiere decir, ha comenzado a reemplazar varios aspectos de la vida de la persona, y en especial el que hoy nos toca abordar es el del ámbito educativo.

Si bien los estudiantes pueden tomarlo y/o acondicionarlo como una materia trasformadora del sistema didáctico, a la hora de abordar un tema, lo cierto es que puede generar daños colaterales, en la formación intelectual de los niños y/o adolescentes.

Esto como generador de daño y/o perjuicio se ve empeorado por el motivo de que la Inteligencia Artificial si bien es instaurada por seres humanos, está inevitablemente marcada por defectos en el diseño de un estudio de investigación científica o bien el método que se utilice para poder interpretar la información deseada.

Hoy en día la funcionalidad con que los buscadores de internet facilitan la tarea humana, no puede echarse a un costado, el ser humano ha sido adiestrado inconscientemente a ello, a fin de buscar y difundir información a la hora de tener que emitir y adentrarse sobre un argumento.

Lo han hecho a través de los buscadores de internet, es decir de aquellos que nos proveen los servicios que se van entrecruzando con otros buscadores, siempre, por supuesto, respetando los motores de búsqueda.

Esta búsqueda puede o no generar un daño, en el sentido de nuestro ordenamiento jurídico, pero desde el punto de vista educacional ocasiona dependencia tecnológica y pasividad en el proceso de enseñanza / aprendizaje.

2. ¿CUÁL ES LA VERDADERA FUNCIÓN DE LA INTELIGENCIA ARTIFICIAL? ¿CUÁL SERÍA SU FACTOR DE ATRIBUCIÓN ACORDE A LA RESPONSABILIDAD GENERADORA DEL DAÑO?

Cuando hablamos de la función de la Inteligencia Artificial, podemos pensar en el reemplazo del ser humano como pensamiento crítico, ella es la combinación de algoritmos planteados cuyo propósito es la creación de máquinas que presenten las mismas capacidades del ser humano.

¿Podemos pensar que una simple máquina?, o quizá no tan simple…. ¡¡Pero maquina al fin!! puede reemplazar al ser humano, y desde este planteo, el pensamiento, la creatividad, las vivencias de un niño y/o adolescente en pleno desarrollo escolar, en opinión personal no seria de agrado, pensar en ello.

Ahora bien, conforme a la Real Academia Española, ***nos dice que la definición de algoritmo es: "Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema".***

En el ámbito jurídico, no existe una normativa específica que regule de manera explícita o clasifique los algoritmos o la inteligencia artificial.

Una definición más técnica señala que se trata de un "conjunto de reglas que, aplicada sistemáticamente a unos datos de entrada apropiados, resuelven un problema en un número finito de pasos elementales.[i3]

Los algoritmos no se consideran bienes materiales en los términos del art. 16 Código Civil y Comercial de la Nación, ….***los bienes materiales se llaman cosas. Las disposiciones referentes a las cosas son aplicables a la energía y a las fuerzas naturales susceptibles de ser puestas al servicio del hombre***. Este articulado refiere a la titularidad de los derechos individuales de las personas sobre los bienes que conforman su patrimonio, es decir comprende al derecho subjetivo sobre un bien individualmente disponible por su titular, es decir que estamos en el patrimonio de la persona.

Pues bien, entonces, serian bienes intangibles, es decir que no tienen un cuerpo propio, no pueden palparse.

---

[3] PENA MARI, Ricardo, "De Euclides a Java, la historia de los algoritmos y de los lenguajes de programación", Ed. Nivola Colombo María Celeste La Responsabilidad Civil derivada de la utilización de algoritmos en el derecho de consumo

Al referirnos a este punto, ¿podemos preguntarnos si el algoritmo es una cosa riesgosa en sí misma?, y también podemos agregar, ¿depende cómo y para que sea utilizada?

Y acá sería el juicio de ponernos a pensar si los daños derivados de la Inteligencia Artificial corresponden a un factor de atribución objetivo o subjetivo.

Tenemos ante estas preguntas las respuesta correctas…,? en lo personal estimamos que no hay una sola respuesta dado que la Inteligencia Artificial puede funcionar como cosa riesgosa en si misma, pero ahora bien, de donde surge la información plasmada en ella?

Claro esta que es el ser humano quien vuelca dicha información para luego ser utilizada, *en reemplazo del ser humano*, por otro sujeto, y que tal vez….dicha información, puede o no ser certera.

De donde surge el deber de controlar este tipo de utilización en el sistema educativo, si nos remitimos exclusivamente a ellos, tendremos el factor de atribución objetivo del 1767 Código Civil y Comercial de la Nación, al igual que si el niño / adolescente está bajo la responsabilidad de los padres, conforme al art 1754 y 1755 CCyCN seguimos, pues con el factor de atribución objetivo.

No nos olvidemos que anteriormente la responsabilidad que se endilgaba a los padres era bajo un factor de atribución subjetivo, este cambio surgió con la modificación de la ley 17711, en torno a múltiples situaciones que generan el deber de reparar la conducta dañosa, no solo era necesaria para la justicia sino para aquellas situaciones que así lo ameritaban.

Endilgarles responsabilidad a los padres y/o docente achacando la misma en un factor subjetivo simplemente por la culpa *in vigilando* e *in eligendo* necesitaba un cambio y, por cierto, un deber de garantía que cautivó de a poco el derecho de daños.[4]

La culpa ***in eligendo*** sostiene que el fundamento de la responsabilidad por el hecho del dependiente radica en la omisión de adoptar la diligencia del caso al seleccionarlo y designarlo, de ahí, va de suyo, el reproche de su conducta.

[4] Carla María Kott Revista Temas de Derecho Civil Persona y Patrimonio. Editorial Erreius

La culpa ***in vigilando*** radica en la vigilancia debida de aquella persona que está a cargo de otra, por ejemplo, en el caso de los niños / adolescentes que deben buscar información y utilizan para ellos la Inteligencia Artificial, hay un buen uso de la misma?, como podemos controlar esa búsqueda de datos, o mejor dicho, saber si los mismos son certeros a la hora de plasmar la información deseada**, *es por eso que nos atrevemos a llamar <u>el daño por el mal uso de la inteligencia artificial en esta etapa de educación.</u>***

Habíamos expresado, que los datos y/o información frente a los cuales se enfrentan los niños y/o adolescentes en el momento de utilizar la inteligencia artificial, están brindados por seres humanos, ¿podríamos decir que cambiamos el factor de atribución objetivo por el factor de atribución subjetivo?

Tarea difícil que nos proponemos en este trabajo.

Entonces, donde y desde que ámbito enfocamos el factor de atribución, cuando hablamos de **<u>daños producidos dentro del sistema educativo provocados por el uso o mal uso de la inteligencia artificial</u>**, si son los niños / adolescentes quienes se nutren de la información que provee el ser humano a través de sus propias experiencias.

Si nos adentramos desde la perspectiva de la responsabilidad civil en el marco de la educación debemos entender si la definición de Inteligencia Artificial se adecua a lo que en nuestro Código Civil y Comercial tenemos como factor de atribución objetivo, el 1767 CCyCN, que establece que: ***Responsabilidad de los establecimientos educativos. El titular de un establecimiento educativo responde por el daño causado o sufrido por sus alumnos menores de edad cuando se hallen o deban hallarse bajo el control de la autoridad escolar. La responsabilidad es objetiva y se exime sólo con la prueba del caso fortuito.*** el cual sostiene que son responsables por el daño ocasionado a los alumnos en el tiempo que se encuentren bajo su autoridad, es decir que si este sistema de búsqueda / educativa es utilizado por los establecimientos educativos resulta evidente que son, no solo quienes deben proporcionar las herramientas necesarias para el correcto uso de dicho sistema, sino que también son los responsables por el daño que esto ocasione a los estudiantes.

A renglón seguido dicho articulado nos habla del seguro obligatorio……. ***El establecimiento educativo debe contratar un seguro de responsabilidad civil, ¿de acuerdo a los requisitos que fije la autoridad en***

materia aseguradora…por lo tanto es dable pensar que en un futuro próximo, los establecimientos educativos busquen seguros de responsabilidad civil que contemplen la utilización de la Inteligencia Artificial?,

Culmina dicho artículo mencionando y excluyendo a los establecimientos universitarios y de educación superior: ***Esta norma no se aplica a los establecimientos de educación superior o universitaria.***

Por ser los niños / adolescentes uno de los grupos vulnerables incorporados en nuestra Constitución Nacional debemos protegerlos y no es absurdo pensar en un seguro que se adecue a este tipo de daños, es decir aquellos, derivados de la Inteligencia Artificial.

El uso de la Inteligencia Artificial en las aulas y/o en los hogares como herramienta educativa, debe ser supervisada por el adulto responsable, toda vez que dicha información puede no ser veraz, de ahí la postura de un factor de atribución subjetivo, ahora bien si le sumamos a ello, la obligatoriedad del seguro del 1767 Código Civil y Comercial de la Nación, conforme a cláusulas específicas, podríamos decir que, seria esto una forma de prevenir futuros daños…?

No nos cabe duda de la responsabilidad objetiva que juega dentro del sistema la Inteligencia Artificial, pero sosteniendo que la información y/o datos que recabamos a través de ella ***nos es proporcionada desde su origen por una máquina***, ni tampoco así una cosa riesgosa, la que da comienzo a los datos que estamos solicitando, sino que viene del propio ser humano, pensamos en un factor de atribución subjetivo desde la culpa, que comprende la negligencia, la imprudencia, la impericia. ¡¡¡No desde el dolo!!!

3. EL FALLO A COLACIÓN

Si bien no hemos encontrado un fallo referente al sistema educativo, si hemos decidido abordar un fallo de EEUU, de febrero de 2024, Indexed as; // Moffatt v. Air Canadá, 2024 DCCRT 149, del Tribunal de Columbia Miembro del Tribunal Christopher C. Rivers en el cual define claramente el daño ocasionado a un sujeto y de ahí la responsabilidad civil que se le ha endilgado a la aerolínea Air Canadá, quien ha permitido brindar dicha información, a través de un CHATBOT

Hechos: El 11 de noviembre de 2022 la abuela del señor Moffat falleció en Ontario. Ese mismo día, Moffat ingresó al sitio web de Air Canadá para buscar y reservar un vuelo desde Vancouver a Ontario, utilizando las tarifas de duelo de Air Canadá.

Es cierto e indiscutible que Air Canadá proporciona ciertas plazas o lugares tales como aquellos que tienen tarifa reducida, para pasajeros que viajan debido al fallecimiento inmediato se un miembro de su familia

Moffat manifiesta que al utilizar el sitio web de Air Canadá, interactuó con un CHATBOT de soporte. A pesar de que la empresa no proporcionó ningún tipo de información sobre la naturaleza de este CHATBOT, este asistente es un sistema automático que le proporciona información a una persona utilizando un sitio web, en respuesta a los prompts que ingresó esa persona, es decir Moffat.

Se desprende del fallo en cuestión que Moffat no estaba chateando, es decir, conversando con un empleado de Air Canadá, sino con un CHATBOT, seleccionado por la empresa y allí se puede constatar el ofrecimiento de la tarifa de duelo.

Se advierte a toda luz, las inconsistencias entre lo que dice la página web de la empresa y la respuesta del CHATBOT.

En la página se deja explícito que el descuento se realiza una vez finalizado el viaje, mientras que el asistente refería una situación opuesta.

Así las cosas, Moffat no tuvo más opción que buscar tener una conversación telefónica con un representante de Air Canadá, dicho representante le ofreció una tarifa determinada pero no queda evidencia de que si la tarifa de duelo se aplicaría o no.

El señor Moffat presentó su primera solicitud de tarifa de duelo el 11 de noviembre de 2022, dentro de los 90 días que establecía el asistente proporcionado por la empresa. En la demanda se presentaron correos electrónicos posteriores al intercambio que demuestran su intento por recibir un reembolso parcial de su tarifa.

En febrero de 2023 Moffat envió un correo a Air Canadá, en el cual incluyó una captura de pantalla de la conversación con el CHATBOT, en la cual se establecía un periodo de tiempo de 90 días para solicitar la tarifa reducida y confirmaba que había llenado el formulario y proporcionado el certificado de defunción.

Luego de todo este reclamo la empresa decide poner en contacto a un representante de la empresa el cual admitió que el asistente había proporcionado **"palabras erróneas /confusas"**

El representante de la empresa señaló el link del CHATBOT hacia la página web de viajes por duelo y manifestó que Air Canadá tenía conocimiento previo que existía un problema, por lo cual a la brevedad solucionarían el mismo debido a que era solo un inconveniente de "actualización del BOT". Moffat, quien es un mero cliente y no maneja, como así tampoco tiene el deber de poder hacerlo y saber lo que estaba ocurriendo, al decir que confiaron en el CHATBOT de Air Canadá, **advirtió que están alegando una evasiva negligente.**

La misma se desprende del descuido del vendedor a los efectos de asegurar una representación precisa y no engañosa.

Podemos pensar en un factor de atribución subjetivo, la culpa, negligencia imprudencia impericia, *el subrayado me pertenece.*

A su turno al cliente, se le informo que la empresa había confiado en un CHATBOT que por lo menos se encuentra desactualizado y que no estaban tomando las medidas necesarias, ni urgentes, para poder solucionarlo, como así tampoco tenia una respuesta por parte de uno de los representantes de la empresa. ¿Será una conducta negligente……?

El tribunal entendió a pesar de los argumentos de la demanda la cual sostenía que dicho CHAT era una herramienta tecnológica la cual habían contratado y que por lo tanto no les resultaba oponible la responsabilidad de su mal funcionamiento, o desactualización en vista de que ellos no habían sido tampoco los desarrolladores del CHATBOT.

Así las cosas, el tribunal sostuvo que la responsabilidad recaía en la demandada ya que fueron ellos quienes decidieron utilizar este "asistente virtual" y por lo tanto forma parte de la empresa. Y es responsabilidad de Air Canadá el funcionamiento del CHATBOT. Finalmente, se ordena que Air Canadá deberá indemnizar a Moffat una suma de dinero por los daños ocasionados.

Reflexión: No dejemos que una maquina reemplace al ser humano, no dejemos que el pensamiento humano, critico, desde el proceso de enseñanza & aprendizaje, limite la creación del niño y/o adolescente, sobre todo a partir de los seis o siete años, momento en el cual comienza la etapa

educativa, comienza el limite…, en la enseñanza, dejemos que se pueda pensar, criticar, debatir y por sobre todo aprender.

REFLEXIONES EN TORNO A LOS DAÑOS OCASIONADOS POR LA INTELIGENCIA ARTIFICIAL

Por Emiliano Carlos Lamanna Guiñazu[1], Carlos Alberto Fossaceca[2] y Pilar Moreyra[3]

I. CONCLUSIONES

1. La novedad que trae la Inteligencia Artificial en la plasmación del daño produce un escenario de incertidumbre que debe relativizarse al analizar las normas y principios que nutren el sistema del Código Civil y Comercial de la Nación;

2. El ecosistema normativo del responder civil se nutre de dos funciones o directrices: la preventiva y la resarcitoria;

3. Los llamados microsistemas (Ley de Defensa del Consumidor) agregan valor y respuesta a estos nuevos modelos de nocimientos;

4. Determinación de los legitimados pasivos o actores jurídicos que intervienen en el proceso de plasmación de la Inteligencia Artificial: empresarios, proveedores, desarrollistas y programadores.

5. Pregonar la aplicación de un seguro, al estilo de los siniestros viales, para toda la actividad que trabaje con sistema de Inteligencia Artificial;

---

[1] Doctor en Ciencias Jurídicas (UCA), Especialista en Derecho de la Alta Tecnología (UCA) y Profesor Titular de la Pontificia Universidad Católica Argentina (UCA), en "Derecho de las Obligaciones", y "Derecho de Daños". Por las mismas asignaturas es Profesor Titular en la Universidad del Museo Social Argentino (UMSA), y Webmaster en la Facultad de Derecho de la Universidad de Buenos Aires (UBA). Profesor Titular en la Universidad Argentina de la Empresa (UADE) asignaturas "Introducción al Derecho" y "Obligaciones y Contratos"; autor del libro "Daño Agravado por el Acreedor – Formas del debido comportamiento de la víctima" por editorial ASTREA (2020), y autor de diversos trabajos de doctrina;

[2] Doctor en Ciencias Jurídicas (UCA), también Especialista en Derecho de Daños (UCA) y Profesor adjunto de la Pontificia Universidad Católica Argentina (UCA) en las asignaturas "Derecho de las Obligaciones" y "Derecho de Daños". Email: fossaceca@uca.edu.ar

[3] Abogada (UCA). Jefa de Trabajos Prácticos por la Universidad Argentina de la Empresa (UADE) en las asignaturas: "Obligaciones y Contratos" e "Introducción al Derecho". Autora de diversos trabajos de doctrina y miembro de equipos de investigación jurídica aplicada. Email: moreyrap.cs@gmail.com.

6. Necesidad de un Estatuto Propio donde se informe a la autoridad administrativa las características del sistema, finalidad y diseño; fuente, recopilación de datos, y modelo de gobernanza que se adopte;

7. Distribución de cargas probatorias dinámicas (Art. 1735 CCyCN) en atención a verificar un proceso sinérgico y virtuoso del producto o servicio dotado de IA;

8. Determinación en la aplicación de estándares del derecho consumeril a la industria tecnológica aplicable a la IA;

9. Aplicación del daño punitivo (Art. 52 bis Ley 24.240) cuando el principio de confianza haya sido vulnerado;

10. Fomentar las relaciones de interactuación de la Comunidad Internacional en vistas de controlar y mitigar atento al fenómeno transnacional de los sistemas de la IA;

II. FUNDAMENTOS

1. INTRODUCCIÓN

La inteligencia artificial (de acá en adelante, IA) se ha transformado en una de las caras visibles de este SXXI donde despunta la expansión digital. Sin temor a equivocarnos, su carácter exponencial la ha convertido en una herramienta de indispensable uso, tanto es así que la humanidad no puede prescindir de su uso.

Se trata de una realidad que debe ser estudiada y analizada. No puede ser dejada de lado. En nuestro caso, desde el ángulo jurídico, la encontramos desafiante.

Su presencia genera incertidumbre, y hasta podríamos decir temor. Cabe traer a colación escenarios distópicos, en donde la idea era presentada –allá por la década de los 80tas- en películas tales como "Blade Runner" (1982) y "Terminator" (1984). Mientras en la primera se mostraba a los replicantes ciborgs temerosos de la muerte, se alzaban en contra de los humanos buscando alargar su "vida" sintética; en la segunda la presencia de Skynet, una computadora con fines bélicos, desataba el día del Juicio Final donde las máquinas masacraban gran parte de la Humanidad, siendo esta, luego, parte de un plan metódico de exterminio masivo.

Sin embargo, el operador jurídico no puede adoptar una actitud omisiva, despreocupada. Debe dedicar con los mayores de los ahíncos a

ponderarla desde su campo especial: el Derecho. Pues el derecho existe porque existe la Persona Humana. El derecho, humaniza.

Naturalmente, una de los aspectos más destacados para analizar a la IA reside en el moderno Derecho de Daños. No sólo en su perspectiva resarcitoria, sino, también, en su faz preventiva. Esta es la cualidad que ofrece, en todos los órdenes del quehacer humano el derecho de la responsabilidad civil: el de configurar un termómetro social de lo que la realidad circundante, ofrece.

Las respuestas a las que cabe arribar podrán resultar, en todo caso, provisorias. Pero nunca innecesarias. La IA es un fenómeno que crece a pasos agigantados. Sus algoritmos corren a gran velocidad. Debemos correr, entonces, tan fuerte como podamos para poder alcanzarla.

2. REGLA PRIMERA: RESPETO POR EL SER HUMANO

Un buen ordenamiento jurídico que aspire a ser considerado como justo debe emplazar su centro de gravitación en torno al ser humano. Ello conlleva a que debe tutelarse, de manera insoslayable, la dignidad de la persona humana y sus derechos humanos fundamentales o que no menoscabe el medio ambiente[4]. Debiéndose repudiarse todo resultado discriminatorio de la IA.

Lo señalado, implica, por lo tanto, rechazar en los términos más enérgicos la postura del llamado *dataismo*, donde el flujo de información se transformaría en un Baal de adoración moderno.

Especial mención merece la protección de los datos personales *sensibles*. No debe permitir el uso de ellos por la IA sin el consentimiento de su titular que debe estar debidamente informado del resultado que se pretende obtener y que puede revocar en cualquier momento.

3. ¿CUÁL RÉGIMEN DEBE APLICARSE?

[4] Como reza el artículo 1, inciso 1 de la resolución europea sobre i.a. aprobada por el Parlamento Europeo: "*promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales, en particular la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de inteligencia artificial* («sistemas de IA»)".

Indudablemente, son aplicables los principios generales del Derecho de Daños. Al carecer de un plexo específico, los preceptos que gobiernan la responsabilidad civil en nuestro Código Civil y Comercial (Arts. 1708 a 1780) constituyen la base normativa.

Se transforman los artículos 1708 a 1780, que integran el capítulo I del título V del Libro Tercero del Código Civil y Comercial, entonces, en el norte a seguir.

a) ¿Ley del consumidor?

Los productos donde en su elaboración interviene la IA pueden ser considerados defectuosos si ocasionan un nocimiento al usuario. En consecuencia, es dable recurrir a los preceptos que gobiernan la ley 24.240 – De Defensa del Consumidor (también por aplicación Art. 1709 del CCyCN).

Los *empresarios* y *proveedores*, en consecuencia, se tornarían responsables por los defectos que exhibiesen los productos en su faz de *diseño, operación* o *información*. No hay que olvidar que rige la llamada *obligación de seguridad* que fuera indicado expresamente en el Artículo 5 del derecho consumeril[5].

4. FUNCIÓN PREVENTIVA

Indudablemente es más sabio anticiparse al daño que actuar una vez que el nocimiento haya ocurrido. Tal orden de ideas explica que la doctrina haya prestado su beneplácito a la redacción del artículo 1710 del Código Civil y Comercial. Una norma señera, ordenadora y compiladora no sólo de funciones, también de principios generales que gobiernan el derecho y dominan la disciplina (Buena Fe y Neminem Laedere).

La rapidez con la que actúa la IA provoca que cuando haya cierta *certidumbre* de peligro de daño, el juez deba adoptar medidas para evitarlos (Art. 1711 – CCyCN).

Tampoco, cabe descartar la posibilidad de que el accionar continuo de la IA agrave el perjuicio ya ocasionado (Art. 1710, inc. c - CCyCN).

---

[5] **Artículo 5º, de la ley 24.240:** *"Las cosas y servicios deben ser suministrados o prestados en forma tal que, utilizados en condiciones previsibles o normales de uso, no presenten peligro alguno para la salud o integridad física de los consumidores o usuarios".*

Es deseable, por tanto, que en los códigos procedimentales contemplaran las *vías procesales* para interponer la *acción preventiva*. La referencia a *sable de utilería*, acuñada por nuestra doctrina iusprivatista, cabe perfecto en esta cuestión.

Por su parte, se torna *recomendable* exigir a los proveedores de IA de grandes magnitudes que implementen una *evaluación de impacto* y un sistema de *gestión de riesgos*[6] antes de lanzarlas al mercado. Es decir, la prevención del daño debe anticiparse a la gestión judicial realizada por el magistrado.

Se debe fomentar que las autoridades administrativas clasifiquen los riesgos que conlleve el uso de la IA (vgcia, *inadmisibles, intolerables* o *insignificantes*) a fin de prohibir el sistema, en el caso que así sea necesario, estableciendo *medidas de mitigación* o declarar -en *forma expresa*- que no se configura ningún perjuicio por su utilización. Una garantía de indemnidad, propia del rol que configura su daño, esto es, responsabilidad objetiva (Art. 1757 – CCyCN).

Por último, se tornaría útil -de *lege ferenda*- recurrir al *principio precautorio* cuando entra en escena la IA que conlleva el riesgo tecnológico: la probabilidad de la afectación de los derechos humanos (DD.HH) y del orden constitucional obligan a no exigir –al menos, en demasía- el cumplimiento del requisito de la prueba de la relación de causalidad (Art. 1736 – CCyCN), el cual, de exigirse en su completitud, puede configurar un escenario de ralentización de las medidas preventivas, que, tal vez, puedan lamentarse en el futuro [7].

---

[6] *"El sistema de gestión de riesgos* ***se entenderá como*** *un proceso iterativo continuo* ***planificado y*** *ejecutado durante todo el ciclo de vida de un sistema de IA de alto riesgo, que requerirá* ***revisiones y*** *actualizaciones sistemáticas periódicas".* Así consta tal concepto en artículo 9, inciso 2 de la resolución europea sobre i.a. aprobada por el Parlamento Europeo.

[7] "En la responsabilidad con base en un factor de atribución objetivo, específicamente en la responsabilidad por el daño causado por el riesgo o vicio de la cosa, se había entendido que se imponía una presunción de adecuación causal o lisa y llanamente una presunción de causalidad. En esa línea, se señaló que, probado el riesgo o vicio de la cosa y que otro causó el daño, se presumía la responsabilidad del dueño o guardián. Debe señalarse que nunca se podrá presumir la responsabilidad civil porque la misma está integrada en su núcleo por cuatro elementos y ellos no pueden presumirse en su totalidad". CÓDIGO CIVIL Y COMERCIAL EXPLICADO. Doctrina y Jurisprudencia. Responsabilidad Civil Artículos 1708 a 1881, LORENZETTI, Ricardo Luis y SAGARNA, Fernando Alfredo, Rubinzal Culzoni editores, pp. 108, año 2020. -

5. FUNCIÓN RESARCITORIA

Es posible llevar a cabo un análisis de sus presupuestos:

a) Daño

La implementación de la IA puede ocasionar detrimentos que conculquen un interés lícito -tanto patrimonial como extrapatrimonial-, inclusive de incidencia colectiva (Art. 1737 – CCyCN). E insistimos una vez más, no cabe descartar el daño irrogado al medio ambiente mediante el uso de estas tecnologías.

b) Relación de causalidad

Este presupuesto implica establecer la relación entre un *hecho* y una *consecuencia* dañosa. La complejidad del funcionamiento de las IA, en muchas ocasiones, hace perder el seguimiento de las tomas de decisiones.

En caso de enfrentarnos frente a una IA dotada con algoritmos llamados de *caja negra* (sin manual de usuario), debería consagrarse de *lege ferenda* una presunción legislativa de causalidad que torne responsable a los *proveedores, creadores* o *programadores* de aquélla, hasta tanto, claro, la industria del sector recapacite sobre esta cuestión, gestionando y generando la salida al mercado de algoritmos de caja blanca (con manual de usuario). Donde la *previsibilidad* del uso sea la *vanguardia* de esta industria. Llegando el producto al usuario con todos los márgenes de incertidumbre *acotados* y *concentrados* a su propia actuación.

Se torna muy dificultoso que la teoría de la *causalidad adecuada* pueda abarcar todas las hipótesis posibles de producción de este tipo de daños. En tal sentido, habría que recurrir a otros criterios de imputación objetiva, tal como el *principio de confianza*. No tan exigente en la materia.

c) Factor de atribución

Debe descartarse la postura que exige un criterio de *imputación subjetivo*. Al menos, no por el momento. La culpa, prever las consecuencias, pero no quererlas, o el dolo, prever y querer las consecuencias, al decir del maestro Orgaz, no tiene cabida en el funcionamiento de la IA.

Esta alcanza sus fines en base a desarrollo y funcionamiento de algoritmos. La necesidad de un factor de atribución objetivo se torna

indiscutible. Sin embargo, no cabe descartar sin más las reglas de la autoría humana, verbigracia, cuando un profesional entrega un dictamen emitido por IA que contiene errores que obedeciendo a su saber debería haber advertido. Tal como mencionamos algunos párrafos atrás.

El *riesgo*, la posibilidad de ampliar el daño, explica la causa de atribución de responsabilidad objetiva. Pero no se trata del conocido como riesgo creado, sino el tecnológico, aquél que, a diferencia del uso de un coche, puede poner en peligro a toda una comunidad.

6. AUTORES JURÍDICOS

Deben ser sindicados como responsables los *diseñadores* y *programadores* cuando el sistema de IA ocasione un daño, especialmente cuando acaezca un error de funcionamiento con aplicación del Art. 1758 – CCyCN cuando el daño es aquiliano, y las reglas que gobiernan las obligaciones de *medios* y *resultado* (Art. 774 CCyCN), cuando hablamos de daño contractual (Lorenzetti).

No cabe descartar que los propios *usuarios* sean indicados como autores jurídicos del nocimiento. El inadecuado uso de la IA puede derivar en su responsabilidad, tal es el caso cuando la emplean para producir las llamadas *fake news* con la intención de desprestigiar a una persona, empresa u organización.

Para evitar tales contingencias, se deberá fomentar el conocimiento de los buenos usos de la IA. Lo que algunos llaman legislación de *pisos mínimos*.

Se torna recomendable exigir a nivel legislativo que por cada ejercicio de IA que se introduzca al mercado del sector el denominado *responsable de despliegue*[8] de esta. Es un actor más donde descansar parte del proceso, sobre todo por el carácter decisional que este tendría a través de su uso.

---

[8] Explica el considerando 13 de la resolución europea sobre i.a. aprobada por el Parlamento Europeo: *"El concepto de «responsable del despliegue» a que hace referencia el presente Reglamento debe interpretarse como cualquier persona física o jurídica, incluida cualquier autoridad, órgano u organismo de otra índole públicos, que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional. Dependiendo del tipo de sistema de IA, el uso del sistema puede afectar a personas distintas del responsable del despliegue".*

7. SEGUROS

Un mecanismo de socializar los perjuicios ocasionados resulta ser la figura del acápite, tal como acaece en el ámbito de los *siniestros viales*.

Se tornaría recomendable recurrir a la *contratación* de seguros a fin de que los perjudicados puedan ver resarcida sus perjuicios de manera más rápida. Tal sistema torna posible la viabilidad de un entorno tecnológico más seguro. Hace al ecosistema digital.

Es recomendable, por lo tanto, que este punto sea objeto de regulación expresa.

8. ¿NECESIDAD DE UN ESTATUTO PROPIO?

La respuesta afirmativa se impone como consecuencia que la IA se ha transformado en un fenómeno reciente con un alcance desconocido. Basta solo pensar en la irrupción del ChatGPT, que tuvo la capacidad y fuerza expansiva como para congelar por dos años la reciente *Ley Europea de Inteligencia Artificial*, originalmente disponible para mediados de 2022.

Deberá contener un *piso mínimo*, tal como consagrar el *principio de trazabilidad*; es decir, ser capaz de verificar los procedimientos que lleva a cabo la IA.

Tal legislación debe ser objeto de revisión continua pues la evolución de la IA resulta ser de *crecimiento exponencial y* la posibilidad de aprendizaje por parte de esta genera la necesidad de un escrutinio continuo del marco normativo.

En este sentido, se tornaría muy útil la creación de un registro de IA donde deba informarse a la autoridad administrativa las características del sistema, su finalidad y diseño, la fuente y recopilación de datos y el modelo de gobernanza que se adopte de conformidad a lo pregonado por la reciente Ley Europea de Inteligencia Artificial [9].

9. APLICACIÓN DE LAS CARGAS DINÁMICAS

A través de esta teoría, desarrollada en profundidad por el jurista rosarino Peyrano, se postula que debe acreditar los *presupuestos generales*

[9] Por ejemplo, el artículo 73 de la resolución europea sobre i.a. aprobada por el Parlamento Europeo ha creado una base de datos de las i.a. de alto riesgo.

de la responsabilidad civil quien se encuentre en mejores condiciones de hacerlo (Art. 1735 – CCyCN; y 53 de la LDC 24.240).

Se tornaría muy conveniente ante el avance gigantesco de la IA que se encuentre a cargo de sus *creadores* y *programadores* demostrar la *trazabilidad* de las decisiones que tomó. De lo contrario, debería considerar que la IA posee una caja negra.

10. UNA MIRADA DESDE EL DERECHO DE CONSUMO

A instancias de este microsistema, se podría exigir que la IA:

Calidad de servicio: Presente una garantía de *calidad del servicio* que despliega para generar confianza en los usuarios [10].

Alerta y Transparencia: Brinde mecanismos de alerta y transparencia para advertir la posibilidad de error;

Trazabilidad: los usuarios deben entender la manera de cómo se obtienen las soluciones adoptadas por ellas;

Seguridad de los Datos: Salvaguarde el contenido sensible y personal de los datos consignados en los prompt.

Exija el consentimiento informado previo por parte del usuario.

11. DAÑO PUNITIVO

Se torna objeto de aplicación la figura del Art. 52 bis, texto Ley 26.331 (LDC – 24.240) en los casos que el producto de la I.A. debía llegar con las seguridades necesarias y se transforme en el generador de los daños expansivos que pudiere haberse evitado. En todo caso, la necesidad de aplicación se circunscribe al mensaje que el derecho debe enviar al sector que produce este tipo de tecnología.

El auge de este microsistema consumeril se asemeja a esto que se señalaba hace tiempo con una analogía amigable: “el Código es el viejo centro de la Ciudad, a la que se han añadido nuevos suburbios, con sus propios centros y características barriales. Poco es lo que se visitan unos y otros; al centro se va de vez en cuando a contemplar las reliquias históricas”

[10]Verbigracia, se exige que la i.a goce de un certificado de calidad mínima en el artículo 44 de la resolución europea sobre i.a. aprobada por el Parlamento Europeo.

11. Puede que esto haya sido emitido en un tiempo donde la descodificación era un fenómeno en el que se creía. Hoy, la realidad es muy diferente, los *microsistemas*, son suburbios que los ciudadanos toman para llegar más rápidos y seguros a sus casas en la gran Ciudad, y también para visitar los espacios históricos.

12. COLABORACIÓN INTERNACIONAL

Se debe fomentar las relaciones de interactuación de la Comunidad Internacional en vistas de controlar y mitigar los eventuales perjuicios transnacionales que pueden acarrear los sistemas de la IA.

[11] LORENZETTI, Ricardo Luis, Las Normas Fundamentales del Derecho Privado, Santa Fe, pp. 14, año 1995, citado por ALTERINI, Atilio Aníbal, La Limitación Cuantitativa de la Responsabilidad Civil, Abeledo Perrot, pp. 33, año 1997.-

LA FUNCIÓN MITIGADORA DEL DAÑO COMO HERRAMIENTA PREVENTIVA FRENTE AL DAÑO PRODUCIDO POR INTELIGENCIA ARTIFICIAL – EL ROL DE LA VÍCTIMA EN LA GESTIÓN DEL DAÑO SUFRIDO

Por Emiliano Carlos Lamanna Guiñazu[1], Carlos Alberto Fossaceca[2]
Y Pilar Moreyra[3]

I. CONCLUSIONES

De lege lata:

1. **Noción:** Resulta trascendente individualizar correctamente el principio "duty to mitigate" consagrado por el Art. 1710, inciso c) del Código Civil y Comercial de la Nación (CCYCN) del principio de prevención con el que se titula el mismo. Pues se trata de principios distintos que juegan en *capilaridades* distinta del daño producido, y hasta con *actores* diversos;

2. **Naturaleza Jurídica** – **Autonomía Científica**: De origen romano, pero desarrollo doctrinario y jurisprudencial en el antiguo derecho francés y en el Common Law, la figura se positivó en el Derecho

---

[1] Doctor en Ciencias Jurídicas (UCA), Especialista en Derecho de la Alta Tecnología (UCA) y Profesor Titular de la Pontificia Universidad Católica Argentina (UCA), en "Derecho de las Obligaciones", y "Derecho de Daños". Por las mismas asignaturas es Profesor Titular en la Universidad del Museo Social Argentino (UMSA), y Webmaster en la Facultad de Derecho de la Universidad de Buenos Aires (UBA). Profesor Titular en la Universidad Argentina de la Empresa (UADE) asignaturas "Introducción al Derecho" y "Obligaciones y Contratos"; autor del libro "Daño Agravado por el Acreedor – Formas del debido comportamiento de la víctima" por editorial ASTREA (2020), y autor de diversos trabajos de doctrina;

[2] Doctor en Ciencias Jurídicas (UCA), también Especialista en Derecho de Daños (UCA) y Profesor adjunto de la Pontificia Universidad Católica Argentina (UCA) en las asignaturas "Derecho de las Obligaciones" y "Derecho de Daños". Email: fossaceca@uca.edu.ar

[3] Abogada (UCA). Jefa de Trabajos Prácticos por la Universidad Argentina de la Empresa (UADE) en las asignaturas: "Obligaciones y Contratos" e "Introducción al Derecho". Autora de diversos trabajos de doctrina y miembro de equipos de investigación jurídica aplicada. Email: moreyrap.cs@gmail.com.

de Compraventa Internacional de Mercaderías (de fuerte acento británico);

3. **Rol de la Víctima**: Si bien la figura plasmada en el Artículo 1710 ordena a *"Toda persona, en cuanto de ella dependa ..."* la intervención de esta en el inciso c) *"No agravar el daño si ya se produjo"* pone a la víctima del daño sufrido –de ser esta las que las adopte- en posición de reclamar daños ya estimables, y no el mero reintegro de gastos por medidas preventivas;

4. **Vigencia de los Principios que rigen la responsabilidad civil**: La mitigación del daño (duty to mitigate") forma parte del sistema preventivo/reparador argentino consagrado en el CCYCN 2015, por tanto, goza de la misma confluencia de principios que activan este sistema: la Buena Fe (Arts. 9; 729; 961, y 1710, inc. b); el Neminem Laedere (Art. 1717) y la llamada Reparación Plena (Art. 1740);

5. **Emplazamiento contractual y extracontractual:** Si bien hablamos de órbitas del resarcimiento que han visto devaluada la importancia de su disociación en los últimos tiempos, merced al Artículo 1716 del Código Civil y Comercial de la Nación, es de suma importancia que el distingo subsiste, tanto como existen etiologías diversas que hablan de un daño surgido de una obligación preexistente (contractual) como de un perjuicio emergente de un acto ilícito (aquiliano o extracontractual). La mitigación opera en ambos espacios;

6. **La relación de causalidad como el "activo" justificante en la construcción de un sistema mitigador**: Históricamente vinculado a la Culpa, en general, y a la noción de culpa de la víctima, en particular, la doctrina se inclina en ver a la mitigación del daño como un problema conectado a la relación de causalidad;

7. **La noción de Reparación Plena como principio preponderante:** Cómo se busca establecer la medida exacta a reparar (quantum respondeatur) el principio de reparar plenamente el daño (Art. 1740) adquiere preponderancia. Pues las medidas mitigadoras equilibran la balanza de los daños (jurídicos) a resarcir, llevando dicha estimación a sus justos límites;

8. **Inteligencia Artificial:** Desde el concepto a sus múltiples propósitos nada acapara tanto la atención de científicos, juristas, filósofos y escritores de las más diversas ramas que la Inteligencia Artificial. Las opiniones abarcan desde su domesticación científica hasta su regulación, atravesando senderos donde se conjugan el miedo, la incertidumbre y la aprobación entusiasta. Nada ha sido sereno en torno a esta tecnología;

9. **Gestión del Daño:** la mitigación del daño por el perjudicado aplica a la idea/noción de toda gestión razonable por parte de la víctima del perjuicio en evitar agravar los perjuicios ya sufridos. Gestión que apunta a disminuir la magnitud del nocimiento. Lo que puede conllevar gastos que deben ser debidamente probados y considerados en el débito del dañador (vgcia: empresa, producto, servicio que opere con Inteligencia Artificial);

10. **Lo estimado y lo producido como medida del resarcimiento:** El daño (jurídico) ya producido por la intervención de Inteligencia Artificial activa y articula los mecanismos –tanto reparadores como mitigadores del nocimiento- por lo que cuadra entender que frente al daño producido y lo estimado a producirse operará la actividad mitigadora del afectado como cierre y conclusión final del número de reparación

De lege ferenda:

11. **Conveniencia de una adecuada regulación en el Código Civil y Comercial de la Nación:** Más allá de su inclusión en el Artículo 1710, inciso c de nuestro CCYCN estimamos conveniente una doble arquitectura jurídica: la primera, su inserción como función autónoma en el Artículo 1708, juntamente con la función preventiva y la función resarcitoria, dada su autonomía conceptual y científica; lo segundo, en una norma distinta, insertar la función mitigadora con las medidas de ajuste, reembolso por gastos incurridos por la víctima por la gestión del daño sufrido;

12. **Aplicación práctica del Principio de Mitigación del Daño por la Víctima: El punto podría ser de aplicación en determinados** protocolos –que aún se debaten- que sea homogéneo y sinérgico con el sistema propuesto por el principio, a saber:

a. **Necesidad de incluir conductas prohibidas para los usuarios en los manuales de uso:** Si queremos intentar domesticar la incertidumbre generada por la IA esta debe proponer –en los propios manuales de uso- una gama de conductas prohibidas a los usuarios;
b. **Necesidad de un adecuado canal de comunicación:** Debemos enfatizar la necesidad de crear/asegurar un canal de comunicación eficaz donde el usuario pueda contactarse con aquellos responsables del producto o sectores afines al mismo;

c. **Ponderación del Hombre Razonable:** la gestión del daño sufrido debería ser ejercida ponderando el normotipo de conducta del Hombre Razonable (Reasonable Man) es decir, la del sujeto que luego de decodificar en su intelecto lo ocurrido actúa en consecuencia;

d. Responsabilidad por Gastos – Pautas de Mensura – Enriquecimiento Sin Causa: El *acreedor/damnificado* que adopta una conducta que impide agravar del daño, los gastos que irrogue ello debe ser soportados por el responsable del uso de la Inteligencia Artificial. La pauta de su métrica de agravamiento (quantum respondeatur) radica en el *enriquecimiento sin causa*. No debe serle exigida un grado de eficacia en el resultado de la misma, sino, ponderar su comportamiento como la de una persona razonable (Reasonable Man) de acuerdo a las circunstancias del caso;

e. La IA como actividad peligrosa – Aptitudes técnicas no trasladables al usuario: La utilización de productos o servicios que contengan Inteligencia Artificial deben ser catalogadas como las provenientes de una "Actividad Peligrosa" (Art. 1757 CCCN). Las aptitudes técnicas de productores, desarrolladores como de los responsables técnicos del producto o servicio no son trasladables al usuario/damnificado;

f. **Espacios o Períodos de Prueba - Necesidad de No Adopción por parte del Acreedor de Conductas Morigeradoras antes de su salida al mercado:** La mitigación del daño por parte del usuario/víctima nunca debe ser ejercida durante los llamados espacios de prueba o períodos de prueba del productos o servicio que se encuentran dotados de IA antes de su salida al mercado. Lo contrario sería trasladar a este último de un conocimiento que no posee.

II. FUNDAMENTOS

1. INTRODUCCIÓN

Las *funciones* de la responsabilidad civil en nuestro sistema codificado civil y comercial (Art. 1708) [4] sostienen que son dos: la *preventiva* (ex ante facto) y la *resarcitoria* (ex post facto). Pero la exégesis del propio código desmiente esto en el Art. 1710 inciso c) [5] al ordenar la

---

[4] Título V. Otras fuentes de las obligaciones

Capítulo 1. Responsabilidad civil

Sección 1ª. Disposiciones generales

(*)

ARTÍCULO 1708. Funciones de la responsabilidad. Las disposiciones de este Título son aplicables a la prevención del daño y a su reparación.

[5] Título V. Otras fuentes de las obligaciones

Capítulo 1. Responsabilidad civil

conducta de toda persona –enderezada, en este caso- a *no agravar el daño si ya se produjo.* Con lo cual, más allá del deber de prevención pregonado por la misma norma, consagra un fundamento distinto al preventivo, sobre todo, cuando el encargado de llevar a cabo dichas medidas es la víctima del daño. Esto es la consagración, lisa y llana, de un viejo principio del derecho de compraventa internacional de mercaderías: el llamado *duty to mitigate* (deber de mitigar el daño). [6]

2. NOCIÓN

Resulta trascendente individualizar correctamente el principio "duty to mitigate" consagrado por el Art. 1710, inciso c) del Código Civil y Comercial de la Nación (CCYCN) del principio de prevención con el que se titula el mismo. Pues se trata de principios distintos que juegan en capilaridades del daño distintas, y hasta con actores diversos;

Sección 1ª. Disposiciones generales

(*)

ARTÍCULO 1710. # Sección 2ª. Función preventiva y punición excesiva

ARTÍCULO 1710. Deber de prevención del daño. Toda persona tiene el deber, en cuanto de ella dependa, de: a) evitar causar un daño no justificado; b) adoptar, de buena fe y conforme a las circunstancias, las medidas razonables para evitar que se produzca un daño, o disminuir su magnitud; si tales medidas evitan o disminuyen la magnitud de un daño del cual un tercero sería responsable, tiene derecho a que éste le reembolse el valor de los gastos en que incurrió, conforme a las reglas del enriquecimiento sin causa; c) no agravar el daño, si ya se produjo

[6] La Convención de Viena sobre Compraventa Internacional de Mercaderías (Art. 7.1). También los Principios del UNIDROIT (Art. 1.7); también lo verificamos en los Principios del Derecho europeo de los Contratos (Art. 1:201 ex 1:106)

3. CONCEPTO – AUTONOMÍA CIENTÍFICA DEL PRINCIPIO

Tal como reza el título de la presente ponencia, la noción se torna trascendente. Pensamos que le herramienta preventiva es distinta a la de la mitigación. Pues, como ya hemos observado en trabajos anteriores, por un lado, en el artículo de doctrina titulado "Análisis del inciso c) del Artículo 1710 del Código Civil y Comercial de la Nación – ¿Prevención o Mitigación?" en las XXVI Jornadas Nacionales de Derecho Civil, año 2017, y en libro "Daño Agravado por el Acreedor. Formas del debido comportamiento de la víctima" de 2020, ambos, la prevención y la mitigación, merecen sus propios espacios en la doctrina y en la exégesis normativa. [7]

Lo dicho impone sostener no la evitación pura del daño; en efecto, tal vez estemos hablando de daños *ya producidos* de los que debamos evitar mayores consecuencias. Consecuencias, las cuales, quizás, sea la propia víctima del daño la encargada de evitar. Entendiendo, también de antemano, que ambas figuras fueron vistas en forma integrada. [8]

4. ROL (ACTIVO) DE LA VÍCTIMA FRENTE AL DAÑO TECNOLÓGICO

Si bien la figura plasmada en el Artículo 1710 ordena a *"Toda persona, en cuanto de ella dependa …"* la intervención de esta en el inciso c) *"No agravar el daño si ya se produjo"* pone a la víctima del daño sufrido –de ser esta las que las adopte- en posición de reclamar daños ya estimables, y no el mero reintegro de gastos por medidas preventivas.

La exigencia de un *rol activo* a la víctima pasa por comprender el alto impacto que ofrecen los medios tecnológicos, y como estos pueden

---

[7] En ambos trabajos de mi autoría se sentaron las bases de comprensión de un Instituto, en apariencia, novedoso. Pero que ya había sido cuidadosamente relevado en un artículo de doctrina por el notable Aníbal Norberto PIAGGIO titulado: "Daño Agravado por el Acreedor" en lo que se llamó "Enciclopedia de la Responsabilidad Civil" allá por el año 1998 en homenaje a Atilio Aníbal Alterini.

[8] "Al aceptar de antemano la disociación entre los vocablos "paradigma" y "función", podemos afirmar que, nacida bajo el amparo de la prevención del daño, la mitigación ha sido integrada como una especie de ese género. Dicha integración, podría verificarse, quizás, en el entendimiento de que quien mitiga previene un daño mayor, lo que podría aceptarse como fundamento, pero no como principio" Lamanna Guiñazú, Emiliano Carlos, Daño Agravado por el Acreedor. Formas del debido comportamiento de la víctima" Buenos Aires, editorial Astrea, pp. 33. -

promover los llamados algoritmos de *caja negra*, donde la opacidad típica de estos aplica a una funcionalidad sólo conocida por su desarrollador. En estos casos, las actividades del usuario de estos productos o servicios deberían ir acompañado de una guía de *buenas prácticas* o comportamiento responsable frente a su utilización.

5. VIGENCIA DE LOS PRINCIPIOS DEL RESPONDER CIVIL EN LA MITIGACIÓN DEL DAÑO

La mitigación del daño ("duty to mitigate") forma parte del sistema preventivo/reparador argentino consagrado en el CCYCN 2015, por tanto, goza de la misma confluencia de principios que activan este sistema: la Buena Fe (Arts. 9; 728; 961, y 1710, inc. b); el Neminem Laedere (Art. 1717) y la llamada Reparación Plena (Art. 1740).

En efecto, si bien entendemos que las funciones del sistema del responder civil son cinco: prevención, mitigación, reparación, punitiva y precautoria. Las dos últimas por fuerza de la propia consagración del Art. 1709 del CCYCN que otorga prelación normativa a las legislaciones supletorias especiales por sobre las sustantivas del Código Civil y Comercial; las últimas mencionadas, precisamente, surgen de la normativa consumeril (artículo 52 bis ley 24.240) y la ambiental (artículo 4, ley 25.675).

6. EMPLAZAMIENTO CONTRACTUAL Y EXTRACONTRACTUAL DE LA MITIGACIÓN

Si bien hablamos de órbitas del resarcimiento que han visto devaluada la importancia de su disociación en los últimos tiempos, merced al Artículo 1716 del Código Civil y Comercial de la Nación es de suma importancia que el distingo subsiste, tanto como existen etiologías diversas que hablan de un daño surgido de una obligación preexistente (contractual) como de un perjuicio emergente de un acto ilícito (aquiliano o extracontractual). [9]

La mitigación opera en ambos espacios con la misma gravitación.

[9] Artículo 1716 CCYC: "Deber de reparar. La violación del deber de no dañar a otro, o el incumplimiento de una obligación, da lugar a la reparación del daño causado, conforme con las disposiciones de este Código".

7. NATURALEZA JURÍDICA – LA CAUSALIDAD JURÍDICA CIVIL COMO ELEMENTO VALIDANTE DE LA MITIGACION DEL DAÑO POR LA VÍCTIMA

Históricamente vinculado a la Culpa, en general, y a la noción de culpa de la víctima, en particular, la doctrina se inclina en ver a la mitigación del daño como un problema conectado a la relación de causalidad.

El derecho de la responsabilidad civil tradicional, con una culpa reinante, no podía establecer este instituto pues la mirada estudiosa que ofrecía el prisma de la época se asentaba en criterios de imputación subjetivos. Fue, entonces, la *culpa de la víctima*, la que atesoraba las miradas de la doctrina vernácula (Borda, Llambías, etc.) sin reparar en la causalidad jurídica.

Las cosas comenzaron a cambiar en 1968 con la reforma civil de la Ley 17.711 que reformó 200 artículos de un total de 4051, menos de un 5% de ese Código Civil decimonónico. No obstante, la escasa cantidad de artículos reformulados, bajo una nueva letra y perspectiva, no fue el mismo código de leyes. Y el cambio fue *significativo* porque rompió el dique de la culpa y cimentó los factores de atribución objetivos, y con ellos, la causalidad tuvo un soplo vivificante.

No era el mismo código.

8. PRINCIPIO GENERAL EMERGENTE - LA REPARACIÓN PLENA

Cómo se busca establecer la medida exacta a reparar (quantum respondeatur) el principio de reparar plenamente el daño (Art. 1740) adquiere preponderancia. Pues las medidas mitigadoras equilibran la balanza de los daños (jurídicos) a resarcir, llevando dicha estimación a sus justos límites. [10]

La noción de REPARACIÓN PLENA exige un manto de justicia en la reparación del daño: *reparar todo el daño, no más allá del daño, pero sí todo el perjuicio producido* nos hemos escuchado repetir en las aulas universitarias. Muy bien, la plenitud de la reparación exige la *certeza*, no sólo de su acaecimiento sino también del metro de su reparación. Endilgar a

[10] Artículo 1740. "Reparación plena. La reparación del daño debe ser plena. Consiste en la restitución de la situación del damnificado al estado anterior al hecho dañoso, sea por el pago en dinero o en especie."

la empresa o producto dotado de Inteligencia Artificial un daño que podría haberse evitado obrado con la *razonabilidad* que las circunstancias exigían, pareciera tener el sentido que exige la propia norma. En cuanto a su *subsistencia*, queda claro que es subsistente el daño no reparado, pero también el futuro y cierto que puede producirse si no se llevan adelante las medidas mitigadoras.

9. INTELIGENCIA ARTIFICIAL

Desde el concepto a sus múltiples propósitos nada acapara tanto la atención de científicos, juristas, filósofos y escritores de las más diversas ramas que la Inteligencia Artificial. Las opiniones abarcan desde su domesticación científica hasta su regulación, atravesando senderos donde se conjugan el miedo, la incertidumbre y la aprobación entusiasta. Nada ha sido sereno en torno a esta tecnología.

Visiones distópicas como la de Yuval Noah Harari nos lo ha acercado el diario británico The Guardian bajo el título abreviado "Nunca invoques un poder que no puedas controlar" en donde analiza la llegada de una tecnología en pleno proceso evolutivo. Proceso, el cual, según su autor es fruto de una red de cooperación humana en derredor de su desarrollo que nos puede afirmar la falsa idea de un progreso cuando, en rigor, estaríamos generando una jaula con barrotes gruesos con la humanidad como único morador. [11]

10. GESTIÓN DEL DAÑO

La mitigación del daño por el perjudicado aplica a la idea/noción de toda gestión razonable por parte de la víctima del perjuicio en evitar agravar

---

[11] "En las últimas generaciones, la Humanidad ha experimentado el mayor aumento de su historia, tanto en la cantidad como en la velocidad de nuestra producción de información. Cada teléfono inteligente contiene más información que la antigua Biblioteca de Alejandría y permite a su propietario conectarse instantáneamente con miles de millones de personas de todo el mundo. Sin embargo, con toda esa información circulando a velocidades vertiginosas, la humanidad está más cerca que nunca de aniquilarse a sí misma" Harari, Yuval Noah, The Guardian, "Nunca invoques un poder que no puedas controlar": Yuval Noah Harari sobre como la IA podría amenazar la democracia y dividir al mundo" ("Never Summon a power you can´t control": Yuval Noah Harari on how AI could threaten democracy and divide the world" sábado 24 de agosto de 2024, en sitio web https://www.theguardian.com/technology/article/2024/aug/24/yuval-noah-harari-ai-book-extract-nexus

los perjuicios ya sufridos. Gestión que apunta a *disminuir* la magnitud del nocimiento. Lo que puede conllevar gastos que deben ser debidamente probados y considerados en el débito del dañador (vgcia: empresa, producto, servicio que opere con Inteligencia Artificial).

La referencia a la gestión del daño se conecta, de manera insoluble, con la persona razonable que ejerce la misma (razonabilidad). Siendo, esta última, un *"criterio jurídico de ponderación, utilizado por el Juez, el árbitro o el práctico, con el fin de encontrar una solución adecuada o equilibrada respecto a la interpretación, integración y aplicación de la norma, de los principios o estándares jurídicos, vinculados con las circunstancias del caso concreto (tiempo y lugar) y a los valores e intereses en conflicto (ratio decidendi)"* [12]

11. METRO DEL RESARCIMIENTO

El daño (jurídico) ya producido por la intervención de Inteligencia Artificial activa y articula los mecanismos –tanto reparadores como mitigadores del nocimiento- por lo que cuadra entender que frente al daño producido -y lo estimado a producirse- operará la actividad mitigadora del afectado como cierre y conclusión final del número de reparación.

La dimensión del daño jurídico (resarcible) ha roto el cascarón de la doctrina y ha ingresado a la exégesis del Código Civil y Comercial de la Nación (Art. 1739). [13]

Por su parte, los requisitos de *certidumbre* y *subsistencia* se sostienen y afirman en forma contundente en la mitigación del daño por el perjudicado. Pues el daño ya se ha producido (certidumbre) y pervive, no sólo la ausencia de resarcimiento, también un peligro de agravamiento (subsistencia). Por lo que este segundo requisito se reconfigura en un segundo segmento de análisis. Siendo la causalidad jurídica civil el núcleo de su naturaleza jurídica pareciera necesario mencionar que ambos *presupuestos* se conjugan en plenitud en el Instituto mencionado.

---

[12] Larrañaga, L., "El principio de razonabilidad", *Revista y Doctrina de Derecho Civil*, Vol 7, Nro. 7, Montevideo FCU, 2019.-

[13] Artículo 1739 – "Requisitos. Para la procedencia de la indemnización debe existir un perjuicio directo o indirecto, actual o futuro, cierto y subsistente. La pérdida de chance es indemnizable en la medida en que su contingencia sea razonable y guarde una adecuada relación de causalidad con el hecho generador".

De Lege Ferenda:

12. APLICACIÓN PRÁCTICA DEL PRINCIPIO DE MITIGACIÓN DEL DAÑO EN EL ÁMBITO DE LA INTELIGENCIA ARTIFICIAL

Cabe observar que, frente a la posibilidad de encontrarnos con sistemas reguladores de este tipo de actividades, la mitigación del daño por el perjudicado por utilización de Inteligencia Artificial ha sufrido un daño que debe evitar ser maximizado. Por lo que se propone:

a) Necesidad de incluir conductas prohibidas para los usuarios en los manuales de uso

El *principio de mitigación* exige como contrapartida que el acreedor sepa que conductas debe abstenerse de realizar como consecuencia de la actividad riesgosa que implica la Inteligencia Artificial.

El *principio general de buena fe* impone que le sea advertido al *usuario* de esta los perjuicios que puede acarrearle. Es decir, que un comportamiento responsable resulta ser necesario.

b) Necesidad de una canal de comunicación

El llamado *responsable de la organización* de la Inteligencia Artificial debe prever los canales de comunicación adecuados para que el *sujeto/usuario* que ha sufrido un nocimiento pueda avisar el evento acaecido.

Entendemos que la función mitigadora operaría plenamente desde el envío de la citada notificación. Ese lapso temporal marcaría la etapa que el *agravamiento* del daño recibido por la *propia conducta* del acreedor debería ser soportado por él si se encontraba en su esfera de actuación la posibilidad de disminuirlo y no lo hubiera hecho. Es decir, una deficiente plasmación de gestionar su propio daño.

En el supuesto que no existiese la vía de notificación pretendida, entendemos que la *no morigeración* de la extensión del perjuicio debe ser de *interpretación estricta*.

Si el damnificado no lo practica, su omisión de comunicación lo perjudica. La verdadera naturaleza de la mitigación no es un deber ni una obligación, sino que consiste en una carga, con las consecuencias que se derivan de esta.

c) Ponderación del hombre razonable

La reflexión acerca de la *previsibilidad* de la conducta del damnificado en cuanto a que no hace suyo un comportamiento que disminuye el daño debe practicarse teniendo en cuenta la medida del *hombre razonable* (Reasonable Man) perteneciente a la media.

d) Responsabilidad de los gastos – pauta de mensura – enriquecimiento sin causa

Al adoptar el *acreedor/damnificado* una conducta que impide agravar del daño, los gastos que irrogue ello debe ser soportados por el responsable del uso de la Inteligencia Artificial.

La pauta de mensura o métrica de agravamiento (quantum respondeatur) radica en el *enriquecimiento sin causa*. La gestión del daño por parte de la víctima no debe serle exigida con un elevado grado de eficacia en el resultado de la misma, sino, por el contrario, ponderar si es un comportamiento esbozado por una persona razonable (Reasonable Man) de acuerdo a las circunstancias del caso que deberán ponderarse.

e) La inteligencia artificial como actividad riesgosa – aptitudes técnicas no trasladables al usuario

La Inteligencia Artificial implica una *actividad peligrosa* (Art. 1757 CCYCN) [14] que por su propio dinamismo de funcionamiento potencia la ocurrencia de nocimientos; especialmente, si tiene en vistas las de alto o elevado riesgo y la aplicabilidad *multipropósito* de la misma.

No se puede exigir al común de la gente las actitudes técnicas.

f) Necesidad de prever la no adopción por parte del acreedor de conductas morigeradoras en los espacios de prueba antes de su salida al mercado

[14] Artículo 1757 – "Hecho de las cosas y actividades riesgosas. Toda persona responde por el daño causado por el riesgo o vicio de las cosas, o de las actividades que sean riesgosas o peligrosas por su naturaleza, por los medios empleados o por las circunstancias de su realización. La responsabilidad es objetiva."

Debe contemplarse la posibilidad de que el acreedor no lleve a cabo un comportamiento morigerador y que la propia Inteligencia Artificial brinde pautas para *evitarlo* en base a su proceso de toma de decisiones.

Tal aspecto debe ser foco de especial atención en la actividad desplegada en los *espacios de prueba* donde se evalúa la operatividad y gestión de la Inteligencia Artificial ante de su salida al mercado.

13. HACIA UNA ADECUADA REGULACIÓN DE LA MITIGACIÓN DEL DAÑO POR LA VÍCTIMA EN EL CÓDIGO CIVIL Y COMERCIAL DE LA NACIÓN

Más allá de su inclusión en el Artículo 1710, inciso c de nuestro CCYCN estimamos conveniente una doble arquitectura jurídica: la primera, su inserción como función autónoma en el Artículo 1708, juntamente con la función preventiva y la función resarcitoria, dada su autonomía conceptual y científica; lo segundo, en una norma distinta, insertar la función mitigadora con las medidas de ajuste, reembolso por gastos incurridos por la víctima por la gestión del daño sufrido.

En efecto, pareciera más acertado pensar en una regulación ordenada de esta segunda herramienta evitativa de daños mayores que en sostener una regulación dispersa o mal diseñada. Por lo que el planteo sería propender a ingresar a la mitigación del daño dentro del elenco de funciones mencionadas en el Artículo 1708 del Código Civil y Comercial de la Nación, al mismo tiempo, comprender lo señalado en el Inciso c) del Artículo 1710 como un Artículo 1710 bis que la mencione expresamente, dada su autonomía conceptual y científica con relación a la función preventiva.

14. BIBLIOGRAFÍA

Código Civil y Comercial de la Nación (CCYCN)

Convención de Viena sobre Compraventa Internacional de Mercaderías;

Principios del UNIDROIT;

Principios del Derecho europeo de los Contratos

"Enciclopedia de la Responsabilidad Civil - En homenaje a Atilio Aníbal Alterini", Abeledo Perrot, Buenos Aires, Tomo IA, año 1998.

LAMANNA GUIÑAZÚ, Emiliano Carlos, Daño Agravado por el Acreedor. Formas del debido comportamiento de la víctima" Buenos Aires, editorial Astrea, año 2020. -

HARARI, Yuval Noah, The Guardian, "Nunca invoques un poder que no puedas controlar": Yuval Noah Harari sobre como la IA podría amenazar la democracia y dividir al mundo" ("Never Summon a power you can´t control": Yuval Noah Harari on how AI could threaten democracy and divide the world" sábado 24 de agosto de 2024, en sitio web https://www.theguardian.com/technology/article/2024/aug/24/yuval-noah-harari-ai-book-extract-nexus

LARRAÑAGA, L., "El principio de razonabilidad", *Revista y Doctrina de Derecho Civil*, Vol 7, Nro. 7, Montevideo FCU, año 2019.-

PERFILAMIENTOS DIGITALES: LA INTELIGENCIA ARTIFICIAL Y LA BIG DATA COMO AGENTES DE PROFUNDIZACIÓN DE LOS ESTADIOS PSÍQUICOS DE LOS SUJETOS.

Por Gabriel E. Lanzavechia[1]

I. CONCLUSIONES

1. Que el perfilamiento de los sujetos a través de las diversas plataformas digitales puede provocar la persistencia del estadio psíquico de las personas que utilizan las plataformas.

2. Que el ordenamiento jurídico debe brindar la posibilidad de que las personas puedan ser excluidas de un procesamiento masivo de

---

[1] Prof. Mg. Gabriel E. LANZAVECHIA. Abogado, Profesor universitario e Investigador. Funcionario del Poder Judicial de la Pcia. de Buenos Aires. Secretario General de la Asociación de Magistrados y Funcionarios de San Martín. Doctorando en Derecho Civil (UBA). Magister en Derecho del Trabajo y Relaciones Laborales Internacionales (UNTREF). Especialista en Derecho de Daños (UBA – título en trámite). Profesor de grado en "Derecho de Familia y Sucesiones" en la Facultad de Derecho de la Universidad de Buenos Aires y Profesor de grado en "Derecho del Trabajo" en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires. Profesor Titular de grado en "Derecho y Tecnología"; Profesor adjunto de grado en "Derecho de Familia", "Derecho Financiero y Tributario", "Práctica Profesional Civil y Comercial II", "Interpretación del Derecho" y Profesor Adjunto de posgrado en "Taller de Tesis" en la Maestría de Derecho Administrativo de la Universidad Abierta Interamericana. Profesor Titular de grado en "Procedimientos por Medios Electrónicos"; Profesor Titular de grado en "Derecho Procesal y Práctica Profesional II", Profesor Asociado de grado en "Teoría del Proceso" de la Universidad Católica de La Plata. Profesor Adjunto de "Derecho del Trabajo I y II", del Instituto Universitario Escuela Argentina de Negocios. Profesor Asociado de grado en "Derecho Informático" y Profesor adjunto de grado en "Derecho Laboral" y "Metodología de la Investigación" y de Profesor adjunto de posgrado en Maestría de Derecho y Tecnología en la Universidad John F. Kennedy. Profesor en la Diplomatura de 'Derecho a la intimidad en la Empresa por la Universidad Nacional Scalabrini Ortiz. Miembro del Seminario Permanente de Investigación de la Persona Humana, Familia y Sucesiones, por el Instituto Ambrossio L. Gioja de la Universidad de Buenos Aires. Director de la "Revista Argentina de Derecho, Tecnología y Sociedad" y Subdirector de la "Revista Argentina de Derecho Común" de la Editorial IJ Editores. Director del Proyecto de Investigación 'Algoritmos, Sesgos y Género: implicancias legales' por la Universidad Abierta Interamericana. Conferencista y autor de publicaciones sobre temas de su especialidad. Contacto: lanzavechia@gmail.com

datos, existiendo tal como refiere Faliero , la incorporación del 'derecho a no ser perfilado' en el ordenamiento jurídico.

3. Que debe existir delimitación específica de responsabilidad civil para el caso de las plataformas digitales y/o servidores de internet y/o cualquier sistema y/o sujeto que efectúe captación masiva de datos de las personas, generando de este modo perfilamientos digitales, y que conlleven al sujeto a recibir informaciones, productos y/o cualquier aspecto de consumo relacionado a su propio perfil.

II. FUNDAMENTOS

1. INTRODUCCIÓN: LA TECNOLOGÍA Y EL IMPACTO SOCIAL: EL ROL DEL DERECHO.

Liminarmente cabe destacar que la tecnología inevitablemente involucra la aplicación de técnicas destinadas al aprovechamiento del conocimiento científico en un sentido práctico[2], provocando una transformación del mundo que lo rodea.

Así, el conocimiento humano comienza a tener implicancias visibles cuando se aplica a un elemento tangible que puede expresar la cualidad del intelecto humano.

De ello, podemos advertir que a lo largo de la historia de la humanidad se han visto avances en su desarrollo producto del impacto tecnológico que generaron transformaciones inconmensurables a nivel social y que han sido catalogadas como verdaderas revoluciones sociales, más precisamente conceptualizadas como revoluciones industriales.

La revolución industrial hilvana una revolución tecnológica que conlleva necesariamente una transformación social. En la historia de la humanidad pueden advertirse cuatro grandes revoluciones de estas magnitudes.

En el Siglo XVIII, se determina la Primera Revolución Industrial, con la aparición de la máquina a vapor, que generaba energía a partir de la ignición por combustión externa, y que se aplicó a la industria se produjo un incremento en la producción y a nivel social produjo la migración de las

[2] Consultado en RAE www.rae.es, fecha de consulta 22-7-2024.

familias del campo a los grandes aglomerados urbanos, generándose transformaciones de todo tipo: económicas, sociales, laborales, de salud, etc.

Luego, en el Siglo XIX, se advierte la Segunda Revolución Industrial, con la elaboración del motor a combustión interna, el cual es un tipo de motor en donde la ignición se da desde el mismo motor por la energía química contenida en el motor y transformada en energía mecánica; como así también la propagación en el desarrollo de la manipulación de la energía eléctrica y sus derivados. Todo ello, permitió la producción masiva incrementando el fenómeno descripto en la revolución anterior.

Posteriormente, en el Siglo XX, con el surgimiento de la computación y las tecnologías de la información y de la comunicación, que propagaron los fenómenos de la globalización.

Finalmente, parte del Siglo XX y el presente (XXI) con la aparición de las tecnologías exponenciales: biotecnología, nanotecnología, infotecnologías (Inteligencia artificial y robótica) y las cognotecnologías.

Como podemos advertir, los saltos de revolución en revolución cada día se acortan y se profundizan. Es decir, que podemos referenciar un efecto multiplicador y acelerador del impacto tecnológico en nuestras vidas. De allí, deviene la nominación de tecnología exponencial.

Las tecnologías exponenciales se encuentran definidas así en atención al tipo de crecimiento y expansión que tienen en la sociedad actual y que repercuten directamente en ella.

Dentro de estas podemos encontrar la biotecnología, la cual vincula a las ciencias naturales, tales como la química, la biología, la física y la ingeniería, persiguiendo la mejora de la vida del ser humano, teniendo aplicación directa en el campo de la medicina, entre otras. Por otro lado, encontramos la infotecnologías, las cuales involucran la computación a través de la ingeniería del software, y que permite lograr el procesamiento y almacenamiento masivo de datos. De aquí derivan la Inteligencia Artificial y la Big Data También encontramos la nanotecnología, que se enfoca en la manipulación de dispositivos materiales a escala nanométrica, lo cual permite trabajar con elementos atómicos y moleculares con gran precisión. Tiene aplicación en el área de la medicina, computación, etc. Finalmente, la cognotecnología que importa la combinación de la inteligencia artificial con otras áreas científicas, tales como la informática, etc., y que se aplica para profundizar los aspectos y habilitades cognoscentes del ser humano.

En este contexto, encontramos al Derecho regulando relaciones individuales…

Así, el sistema jurídico que se construye a partir del debate singular y simplificado de los agentes que representan al campo. Todos los operadores jurídicos participan de ese debate, construyendo y repensando normas.

Lo cierto, es que las tecnologías exponenciales superan el constructo intelectual humano, por la masividad de su avance.

Es por ello, que es menester reflexionar sobre el impacto de la tecnología en el Derecho, atendiendo a un campo en constante evolución.

En la era digital actual, la tecnología avanza a un ritmo vertiginoso, impactando todos los aspectos de nuestra vida diaria, desde la forma en que nos comunicamos hasta cómo hacemos negocios y protegemos nuestra privacidad. Y como eso influye en nuestra vida.

Consecuentemente, corresponde, parafraseando al Dr. Marcos Córdoba, reflexionar sobre el rol de los juristas, ya que son quienes deben comprender el fenómeno jurídico y asignarle consecuencias jurídicas.

Atendiendo lo expuesto, centraremos el presente análisis sobre la Big Data y el procesamiento masivo de datos a través de la Inteligencia Artificial relacionado estrictamente con el perfilamiento humano en el marco de las plataformas digitales, y como las construcciones algorítmicas pueden generar daño o el agravamiento de situaciones prexistentes.

2. PONENCIA DE LEGE LATA: BIG DATA Y LA INTELIGENCIA ARTIFICIAL: EL PERFILAMIENTO DIGITAL DEL SUJETO Y AUSENCIA DE NORMATIVA ESPECÍFICA.

a) El fenómeno de la Big Data y la Inteligencia Artificial y el procesamiento masivo de datos.

Inserte texto aquí. Tal como ha quedado expuesto precedentemente, la vida de los seres humanos ha quedado frente al impacto de un nuevo proceso de revolución industrial, tecnológica, etc., derivado del crecimiento del poder de cómputo y almacenamiento, la existencia de internet y propagación de las comunicaciones.

Nunca en la humanidad se han generado, procesado y almacenado datos como en la actualidad. Es por ello por lo que podemos afirmar que

hemos ingresado en una era masiva del procesamiento y almacenamiento de datos.

Nótese como muchas casas de altos estudios han profundizado el desarrollo de carreras específicas, sean de grado o posgrado, que aborden la cuestión: la ciencia de datos.

Corresponde, entonces, indagar: ¿qué es un dato? Lo cual, su respuesta inmediata es relativa a la información del mundo que nos rodea, sea material o inmaterial, y traduce un carácter neutral y objetivo, según la pieza informativa.

Cuando procesamos el dato, le otorgamos sentido. Es decir, significamos el dato. Por lo que, ya deja de tener un contenido objetivo para pasar a tener una traducción informativa y con conjugación significante.

Es decir, que el dato es aislado. La significación del dato es el otorgamiento de un carácter simbólico y social de ese mundo. Es por ello, que podemos afirmar que los datos no existen, sin que sea adosado a una idea dispuesta por un sujeto.

Aclaramos que la Big Data descansa sobre tres pilares centrales, representativos en tres V, que se referencian: velocidad, volumen y variedad; entendiendo la inclusión de una cuarta V, que es la veracidad, ya que no podríamos hablar de predictibilidad sin la veracidad del dato. Althabe coincide que la: "*Big data traducido literalmente significa 'datos masivos' y, consiste en la ciencia de predicción basada en grandes masas de datos utilizando algoritmos matemáticos para poder obtener resultados de probabilidad."*[3]

Aquí es donde la computación y el uso de la Inteligencia Artificial, para el procesamiento de dato comienza a tener un rol preponderante en la sociedad, ya que se ha comenzado a utilizar para el procesamiento masivo de datos a fin de captar caracteres y asignarles sentido.

Así, de una base masiva de datos que recopilan elementos concretos y homogéneos, se aplican los sistemas de Inteligencia Artificial a fin de su procesamiento, este procesamiento es masivo y se denomina minería de datos.

---

[3] ALTHABE, María Victoria. 'Big data, un desafío para el derecho a la privacidad', SJA 28-10-2022,1, TR La Ley, AR/DOC/1513/2022.

Entonces, podemos afirmar que estamos frente a un nuevo paradigma en la obtención de datos producto del impacto tecnológico, y afirmar que frente a la aplicación de algoritmos podemos obtener probabilidades sobre determinados eventos o hechos, logrando una gran predictibilidad.

Ahora, ¿Qué sucede si eso puede aplicarse directamente a las personas humanas?

b) El perfilamiento del sujeto: ausencia de regulación específica.

Atendiendo el contexto científico referido antes, claramente nos permite afirmar que el procesamiento masivo de datos permite aplicarlo a las personas y así obtener una caracterización de los sujetos.

Es así, que derivado de estas nuevas tecnologías se advierte una transformación e impacto en el espacio de vida de los seres humanos.

Hoy en día es común participar de la vida digital, ingresando en redes sociales, relacionándonos con amigos, nuevos amigos o incluso desconocidos. La vida del sujeto ha traspasado a un mundo digital, al cual ya podríamos referenciarlo como mundo digital, o nombre que al lector se le ocurra.

En ese nuevo contexto, cada uno de nosotros desarrollamos actividades diarias de la vida cotidiana participando activamente en redes sociales, navegando en páginas de internet, accediendo a cuentas bancarias, efectuando negocios a través de una simple conexión, visualizando películas, escuchando música, leyendo noticias, publicando opiniones, etc.

Cada participación en el mundo digital importa un dato…

Por lo que, dentro de ese devenir cotidiano arrojamos datos por los diversos sistemas de información, lo cual permite a los sistemas efectuar un almacenamiento masivo de ellos, generando así una base de datos que permite posteriormente su procesamiento.

En el marco del procesamiento masivo, podemos generar un perfil digital, estableciendo criterios conductuales del sujeto, identificando así su orden de preferencias, rasgos conductuales, entre otros.

Así las cosas, cada vez que participamos en el mundo digital, cada vez se van caracterizando, según nuestro perfil, los criterios de búsqueda, los gustos, nuestras preferencias. Cada vez, el sistema nos conoce más, y así

nos ofrece infinitamente la reproducción según nuestro perfil. El algoritmo nos conoce mejor que nadie.

Vale la pena invitar al lector a utilizar alguna red social habitual, y advertir que presentaciones, publicaciones, videos, reels, etc., habituales recibe. Y ahora explicitarle que ese direccionamiento involucra el perfilamiento digital captado a través de su participación en el mundo digital.

Cabe reflexionar, entonces, si el perfilamiento digital del sujeto importa una afectación a los derechos personalísimos de los ciudadanos: intimidad, honor, imagen, etc., y si existe marco normativo específico que regule la cuestión; aspecto que ya hemos abordado en trabajos precedentes.

Lo cierto, es que los Derechos Personalísimos se encuentran tutelados en el marco del Código Civil y Comercial de la Nación, en art. 51 y sstes., como así también existen ciertas leyes especiales que permiten la protección de la imagen, tales como el art. 31 de la Ley 11.723, o bien en normativa que regula precisamente los datos personales, como la Nro. 25.326, que establece como objeto primordial: "…la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional…".

Y, sobre la especie, Argentina ha dictado la Ley 27.699 sobre el 'Tratamiento Automatizado de Datos' por la cual se aprobó el Protocolo modificatorio del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, suscripto en la ciudad de Estrasburgo (Francia), del cual se destaca: el preámbulo del convenio, a efectos de delimitar el norte, el cual reza: "…Considerando que resulta necesario asegurar la dignidad humana y la protección de los derechos humanos y libertades fundamentales de cada persona y, dada la diversificación, intensificación y globalización del tratamiento de datos y los flujos de datos personales, la autonomía personal basada en el derecho de una persona a controlar sus datos personales y el tratamiento de tales datos…".

De lo cual, no debe perderse de vista que regular el tratamiento automatizado de datos, es asegurar la dignidad humana y las libertades fundamentales.

Así, pareciera encontrarse un Norte con relación a dicha temática, pero ¿existe suficiencia legislativa?

El protocolo para el tratamiento automatizado de datos conforme expresa la norma, dispone que este debe ser proporcional al fin legítimo que se persigue, encontrando un equilibrio justo entre todos los intereses. Como así también desarrolla la legitimidad del tratamiento del dato, parte de una base esencial: el consentimiento. Este, debe ser voluntario, específico, informado e inequívoco del titular de los datos; todo lo cual sólo comprende aspectos generales sobre el tratamiento. Asimismo, establece una individualización del sujeto que la ley autoriza al tratamiento del dato, al cual denomina 'encargado del tratamiento', resultando aquel una persona física o jurídica, autoridad pública, servicio, organismo o cualquier otro órgano que dé tratamiento a datos personales en nombre del responsable del tratamiento', siendo responsable de todas las medidas de seguridad adecuadas contra riesgos como los de acceso accidental o no autorizado a lo datos, destrucción, pérdida, uso, modificación o divulgación de los mismos; siendo que, a su vez, debe asegurar la transparencia del tratamiento.

Aquí encontramos un elemento esencial en cuanto el objeto de la presente ponencia, y que entendemos que la legislación actual no ha alcanzado la profundidad y análisis suficiente, ya que delimita conductualmente la responsabilidad civil a las medidas de seguridad, sea por acceso incidental o no autorizado a los datos.

Pero ¿se regula el alcance sobre la actividad de procesamiento y la exposición del sujeto a través de su propio perfilamiento? Lo que no se advierte es regulación específica en la materia.

Por ello, podemos advertir que la norma es una ley de alcance general sobre el tratamiento automatizado de datos, estableciendo parámetros y ejes rectores en la materia, pero que ha dejado un tendal de espacios sin resolver.

c) La determinación algorítmica y el sostenimiento de una situación temporal: afección a la esfera psíquica.

Ahora sí, adentrándonos en la situación que se advierte como problema que a través de la determinación del procesamiento automatizado de datos se capte un perfil del sujeto en un contexto específico.

Tal como se referenció oportunamente, los sujetos convivimos con el mundo digital, al cual le otorgamos datos de forma constante y masiva, y que, a través de ese perfilamiento, es el mismo sujeto que inevitablemente se vuelve para la plataforma un producto en sí mismo.

Ahora ¿qué ocurre si el procesamiento masivo y la exposición de datos tiene como suceso un momento particular del sujeto en el que se encuentra atravesando una afectación psíquica? Un ejemplo, podría decirse, un estado depresivo de la persona.

Lo cual, inevitablemente, el proceso de captación del dato y su operacionalización se encontraría enraizado en ese contexto personal. Por lo que, atendiendo el modo de funcionamiento del perfilamiento, los objetos de participación digital ofrecidos en la plataforma tendrían caracteres que se adecúen a ese aspecto.

Es decir, podría ofrecerse publicaciones, visualizaciones, música, etc., que conlleven a cierto entramado de contexto depresivo; entonces ¿cómo hace el sujeto para escapar a ese bucle?

A partir de allí, es que puede advertirse que la participación digital, podría llegar a provocar una profundización de un estado psíquico del sujeto y potencialmente ocasionar o agravar un daño.

Máxime atendiendo la representación y entidad que la persona le otorga a lo que ella misma consume en la plataforma; por lo que podría advertirse responsabilidad civil derivada del consumo indirecto de la Inteligencia Artificial.

Y, más allá de repensar el aspecto derivado de la responsabilidad que podría generar el procesamiento automatizado de datos, y de repensar si el ordenamiento jurídico es suficiente para atribuir responsabilidad a las plataformas, creo que queda consolidada una idea que podría resultar complementaria al presente, que es la posibilidad de escapar al procesamiento automatizado de datos, de no querer ser parte de determinación alguna, de escapar dentro del mundo digital y poder convivir, quizá, con el azar.

Consecuentemente, vemos la necesidad de regulación específica en la materia, que será planteada infra.

3. PONENCIA DE LEGE FERENDA: LA REGULACIÓN DEL PROCESAMIENTO AUTOMATIZADO DE DATOS Y EL DERECHO DE EXCLUSIÓN A SER PARTE DE ESTE

Conforme a los aspectos teóricos tratados, consideramos pertinente que se evalúe la incorporación y/o modificación y/o adecuación de la normativa nacional, a fin de que resulte expresa y claramente:

Que exista la posibilidad de que las personas puedan ser excluidas de un procesamiento masivo de datos, existiendo tal como refiere Faliero[4], la incorporación del 'derecho a no ser perfilado' en el ordenamiento jurídico.

Que exista la delimitación específica de responsabilidad civil para plataformas digitales y/o servidores de internet y/o cualquier sujeto que efectúe captación masiva de datos, generando perfilamientos digitales que conlleven al sujeto a recibir informaciones, productos y/o cualquier aspecto de consumo relacionado a su propio perfil.

4. REFLEXIONES FINALES Y CONCLUSÍON.

Como cierre del presente, es menester dejar una reflexión, más allá del contenido teórico y práctico brindado, como de las propuestas ofrecidas; que está centrada en la idea de la herida narcisista que se basa la obra de Sigmund Freud, significado que representa un daño o trauma emocional que afecta al sentido del autoestima o imagen de sí mismo de una persona.

Freud refería que existían tres heridas narcisistas de la humanidad.

La primera, atribuida a Copérnico, quien esgrimió en un contexto contradictor, de que la Tierra giraba alrededor del Sol, apartándose de la idea hegemónica en que la Tierra era el centro del todo. Es decir, reposicionó a la humanidad en un estadio de insignificancia universal, no siendo más que una pequeña gota en el coloso universal, girando alrededor de una estrella.

La segunda, provocada por Darwin, quien incorporó las teorías de la evolución, derivada de la selección natural, en el que el más apto sobrevive, ya que se adecúa naturalmente al medio, y en su caso, perece. Esta tesitura colocó al sujeto en un estadio de animalidad, ya que no fue elegido por ningún Ente superior para gobernar la tierra, y que su proceso de desarrollo deriva de aspectos evolutivos y adaptación al mundo natural.

Finalmente, la tercera, la propia teoría de Freud, con el desarrollo de la teoría del psicoanálisis, que descubre el inconsciente humano y que representa la idea de que el ser humano no es consciente de sí mismo, ni

[4] FALIERO, Johanna C. Hacia la nueva ley de protección de datos personales en Argentina, 5-sep-2022, Microjuris. MJ-DOC-16776-AR | MJD16776.

puede alcanzar el conocimiento profundo de su propia individualidad, resultando un esclavo del inconsciente.

De ello, podemos reflexionar, como idea simbólica, si actualmente la humanidad no se encuentra frente a la cuarta herida narcisista, devenida del crecimiento exponencial de la tecnología, en la creencia de que podemos controlar lo que hemos creado, que a la luz de la praxis nos supera ampliamente.

Concluyendo así, que esta herida no derivará de un fenómeno natural que ha sido recibido por el Ser Humano desde el Universo, sino que, por el contrario, tendremos participación en ella, resultando así una herida autoinfligida.

Es por ello por lo que resulta vital que todos los operadores, no solo jurídicos, sino también desde las diferentes interdisciplinas participen activamente en la construcción que regule la materia.

DAÑOS DERIVADOS DEL USO DE INTELIGENCIA ARTIFICIAL GENERATIVA: ANÁLISIS Y NORMATIVA ARGENTINA

Por Mario Rodolfo Leal[1], Mario Rossi[2] y Franco Orellana[3]

I. CONCLUSIONES

1. La inteligencia artificial generativa presenta riesgos significativos para la protección de la imagen personal.

2. La legislación argentina actual proporciona un marco de protección, pero no aborda de manera específica los desafíos planteados por la IA generativa.

3. Las IA generativas pueden ser responsables por la reproducción no consentida de imágenes personales utilizadas en su entrenamiento.

4. El uso indebido de herramientas de IA para crear situaciones ficticias vulnera derechos personalísimos y genera daños significativos.

---

[1] Abogado, Juez Vocal de la Cámara Federal de Apelaciones de Tucumán y doctor en Derecho por la Universidad Nacional de Tucumán (UNT) con la máxima distinción Summa Cum Laude. Es Director del Centro de Estudios de Nuevas Tecnologías y Bioderecho del Siglo XX y profesor titular en las cátedras de Derecho Civil y Derecho Privado en la UNT. También es profesor en la Universidad San Pablo Tucumán, donde coordina investigaciones en derecho civil y biotecnología. Ha dirigido numerosos proyectos de investigación y es autor de libros y artículos sobre derecho civil, biotecnología y propiedad intelectual, y ha recibido múltiples premios por su contribución académica y científica.

[2] Abogado especializado en innovación y tecnología. Doctor "honoris causa" por la Federación Iberoamericana de Abogados. Es especialsita en Derecho Procesal Civil y tiene un diplomado en Metaverso, Gaming y Web 3.0 por la Universidad Nacional de Buenos Aires. Actualmente es Director del Laboratorio DYNTEC en la Universidad Nacional de Tucumán (UNT) y funcionario en la justicia laboral de Tucumán. Docente en la Universidad San Pablo Tucumán y la UNT, también coordina el suplemento "Abogacía Práctica Digital" de la Editorial ElDial y es autor de libros sobre innovación legal, incluyendo "Justicia Algorítmica, Metaverso y resolución de conflictos" y "Chat GPT: ¿una IA que revolucionará la abogacía?".

[3] Abogado, diplomado en Metaverso, Gaming y Web 3.0 por la Universidad Nacional de Buenos Aires. Relator en el Juzgado del Trabajo de la 9ª Nominación de Tucumán, es investigador y docente en la UNT. Subdirector del Laboratorio DYNTEC de la Facultad de Derecho y Ciencias Sociales de la UNT, coautor de "Metaverso y resolución de conflictos" y de la "Guía de uso de IA en el aprendizaje práctico del derecho".

5. Existe la necesidad de reformar la normativa vigente para incluir protecciones específicas contra los usos dañinos de la IA generativa.

6. La actualización del marco legal argentino es crucial para garantizar la protección adecuada de los derechos en la era digital.

7. La prevención y reparación de daños causados por la IA generativa deben ser priorizadas en futuras reformas legales.

II. FUNDAMENTOS

1. INTRODUCCIÓN

En la era digital actual, la inteligencia artificial generativa ha surgido como una herramienta poderosa con el potencial de transformar múltiples aspectos de nuestra vida diaria. Desde la creación de contenido visual y auditivo hasta la generación de textos complejos, esta tecnología ha demostrado capacidades sorprendentes. Sin embargo, con este gran poder también vienen grandes responsabilidades y riesgos. El Papa Francisco, en su reciente discurso frente a la cumbre del G7, destacó la dualidad de la inteligencia artificial, señalando que puede ser utilizada tanto para el bien como para el mal. Él afirmó que "la inteligencia artificial es una herramienta fascinante y tremenda al mismo tiempo", subrayando la importancia de su uso ético y responsable[4].

El objetivo de esta ponencia es analizar los daños derivados del uso de inteligencia artificial generativa, distinguiéndola de la IA utilizada para la toma de decisiones. Exploraremos casos específicos donde la IA generativa ha sido utilizada de manera perjudicial, como en la creación de deepfakes y deepnudes, así como en la clonación de artistas sin su consentimiento. Además, evaluaremos cómo estos fenómenos se interpretan dentro del marco normativo argentino, identificando las lagunas legales y proponiendo mejoras para una regulación más efectiva.

Para ello, la ponencia se estructurará de la siguiente manera: primero, se definirá y comparará la inteligencia artificial generativa con la IA

4 Francisco. (2024, junio 14). *Discurso del Santo Padre Francisco en la sesión del G7 sobre inteligencia artificial*. Borgo Egnazia, Apulia, Italia. Recuperado de https://www.vatican.va/content/francesco/es/speeches/2024/june/documents/20240614-g7-intelligenza-artificiale.html

utilizada para la toma de decisiones, destacando sus características y aplicaciones. Luego, se presentarán casos de uso dañino de IA generativa, detallando su impacto social y psicológico. A continuación, se evaluarán los daños resultantes de estos usos y se discutirán las implicancias legales bajo la normativa argentina. Finalmente, se ofrecerán conclusiones y recomendaciones para fortalecer la regulación y proteger a los individuos de los riesgos asociados con esta tecnología.

Al sumergirnos en este análisis, buscaremos arrojar luz sobre los desafíos y oportunidades que presenta la inteligencia artificial generativa, promoviendo un uso responsable que beneficie a la sociedad en su conjunto y prevenga abusos y daños innecesarios.

2. DIFERENCIAS ENTRE IA GENERATIVA Y IA DE TOMA DE DECISIONES

La inteligencia artificial es un concepto complejo y multifacético que abarca una amplia gama de tecnologías y aplicaciones. En términos generales, la IA puede definirse como una rama de las ciencias informáticas que busca desarrollar sistemas capaces de realizar tareas que normalmente requieren inteligencia humana. Estos sistemas intentan reducir el grado de intervención humana, logrando así resultados más eficientes y precisos. La inteligencia artificial ha sido un tema recurrente en la ciencia ficción, donde a menudo se la representa de manera negativa, evocando escenarios en los que las máquinas superan y controlan a los humanos. Un concepto clave en este ámbito es el de la "singularidad", un punto hipotético en el futuro donde las máquinas alcanzarían una inteligencia superior a la humana, transformando radicalmente la sociedad.

a) Definición y características de la inteligencia artificial generativa

La inteligencia artificial generativa es una subcategoría de la IA diseñada para crear nuevo contenido. Utiliza algoritmos de aprendizaje profundo para generar textos, imágenes, música y otros tipos de datos que son originales y no simplemente una reproducción de entradas anteriores. Un ejemplo emblemático de IA generativa es GPT (Generative Pre-trained Transformer), desarrollado por OpenAI. GPT puede generar textos coherentes y contextualmente relevantes a partir de unas pocas palabras o frases de entrada. Su capacidad para comprender y replicar el estilo y el

contenido de un amplio corpus de datos lo hace particularmente útil en aplicaciones creativas y de generación de contenido.

b) Comparación con la IA utilizada para la toma de decisiones

Por otro lado, la IA utilizada para la toma de decisiones, como la que se encuentra en los sistemas de piloto automático de aviones o en los vehículos autónomos, está diseñada para analizar datos y tomar decisiones basadas en ellos. Estos sistemas dependen en gran medida de algoritmos que procesan información en tiempo real para hacer predicciones y tomar decisiones que optimizan ciertos objetivos, como la seguridad y la eficiencia.

Por ejemplo, en los vehículos autónomos, la IA analiza continuamente datos de múltiples sensores, como cámaras, radares y LIDAR, para comprender el entorno del vehículo y tomar decisiones de conducción en fracciones de segundo. Estos sistemas deben considerar una multitud de variables y posibles escenarios, desde la detección de peatones hasta la interpretación de señales de tráfico, para garantizar una conducción segura.

c) Ejemplos de cada tipo de IA en el mundo real

a. IA Generativa:

1. GPT (Generative Pre-trained Transformer): Utilizado en aplicaciones de procesamiento de lenguaje natural, GPT puede redactar artículos, responder preguntas y mantener conversaciones fluidas. Su capacidad para generar texto humanamente convincente lo hace valioso en áreas como la atención al cliente, la creación de contenido y la educación.

2. DALL-E: Otro modelo de OpenAI, DALL-E, genera imágenes a partir de descripciones textuales. Puede crear ilustraciones y gráficos originales basados en descripciones detalladas, lo que es útil en diseño gráfico y arte digital.

b. IA para la Toma de Decisiones:

1. Piloto Automático de Aviones: Los sistemas de piloto automático utilizan IA para mantener el control del vuelo, gestionar la navegación y optimizar el consumo de combustible. Estos sistemas toman decisiones en

tiempo real para ajustar la altitud, la velocidad y la ruta del avión, mejorando la seguridad y la eficiencia del vuelo.

2. Vehículos Autónomos Empresas como Tesla y Waymo han desarrollado vehículos autónomos que utilizan IA para conducir de manera segura y eficiente. Estos sistemas toman decisiones basadas en una combinación de algoritmos de visión por computadora, aprendizaje automático y control predictivo para navegar por las carreteras y evitar obstáculos.

3. CASOS DE USO DAÑINO DE IA GENERATIVA.

a) Explicación de casos de deepfake y deepnude

Uno de los casos más notorios y dañinos del uso de IA generativa es la creación de deepfakes y deepnudes. Estas tecnologías utilizan redes neuronales avanzadas para superponer la cara de una persona en el cuerpo de otra en videos o imágenes, a menudo de contenido sexual explícito. Un ejemplo destacado es el caso de Taylor Swift, quien fue víctima de la difusión de imágenes pornográficas falsas creadas con IA. Estas imágenes circularon en redes sociales, generando una ola de indignación y llevando a Swift a considerar acciones legales contra los responsables[5].

Los deepfakes y deepnudes no solo representan una violación grave de la privacidad, sino que también pueden tener consecuencias devastadoras para las víctimas, incluyendo daño a la reputación, estrés psicológico y amenazas a la seguridad personal. Este tipo de contenido falsificado se difunde rápidamente en internet, lo que dificulta su control y eliminación, exacerbando el daño causado a las víctimas.

b) Análisis de la clonación de artistas y el uso no consentido de su voz

Otro uso perjudicial de la IA generativa es la clonación de artistas y el uso no consentido de sus voces. Un caso prominente es el de Scarlett Johansson y su conflicto con OpenAI. Johansson descubrió que la voz de un

[5] Página/12. (2024, enero 27). Indignación en Estados Unidos por la difusión de imágenes pornográficas falsas de Taylor Swift hechas con IA: La artista iniciaría una demanda. *Página/12*. Recuperado de https://www.pagina12.com.ar/707865-indignacion-en-estados-unidos-por-la-difusion-de-imagenes-po

asistente de IA llamado Sky, desarrollado por OpenAI, sonaba inquietantemente similar a la suya. A pesar de los intentos de OpenAI por obtener su consentimiento, Johansson quedó "conmocionada" por la semejanza y consideró tomar acciones legales. Este caso subraya los riesgos de la clonación de voces y la necesidad de regulaciones claras para proteger los derechos de los individuos sobre su identidad y su imagen.[6]

Un fenómeno similar ocurrió con Taylor Swift, cuando se especuló que un álbum supuestamente filtrado había sido creado por IA. Aunque finalmente se confirmó que las canciones eran genuinas, la situación resaltó cómo la tecnología puede engañar incluso a los fans más leales y generar confusión sobre la autenticidad de las obras artísticas.[7]

c) Impacto social y psicológico de estos casos

El impacto social y psicológico de los deepfakes, deepnudes y la clonación no consentida de voces es profundo y multifacético. Las víctimas de estas prácticas enfrentan una violación significativa de su privacidad y dignidad. La difusión de imágenes y videos falsos puede causar un daño irreparable a su reputación, afectar sus relaciones personales y profesionales, y generar un estrés psicológico intenso.

Desde una perspectiva social, estos incidentes erosionan la confianza en los medios digitales y plantean serios desafíos para la autenticidad de la información en la era digital. La capacidad de la IA para crear contenido extremadamente realista pero falso amenaza con desestabilizar la percepción pública de lo que es real y lo que no lo es, fomentando un ambiente de desconfianza y escepticismo.

Psicológicamente, las víctimas pueden experimentar ansiedad, depresión y otros trastornos relacionados con el estrés debido a la exposición

[6] Hart, R. (2024, mayo 24). El conflicto entre Scarlett Johansson y OpenAI podría generar una guerra de las celebridades contra las empresas de IA. *Forbes Argentina*. Recuperado de https://www.forbesargentina.com/innovacion/el-conflicto-scarlett-johansson-openai-podria-generar-una-guerra-celebridades-empresas-ia-n53413

[7] Watercutter, A. (2024, abril 19). No, el nuevo disco de Taylor Swift no fue creado con IA (pero que creyeras que sí dice algo sobre el mundo en que vivimos). *WIRED*. Recuperado de https://es.wired.com/articulos/nuevo-disco-taylor-swift-no-fue-creado-ia-pero-dice-algo-sobre-mundo-que-vivimos

no consensuada de contenido íntimo o la sensación de haber perdido el control sobre su propia identidad. El caso de Taylor Swift, en particular, destaca cómo las figuras públicas, a pesar de su influencia y recursos, no están exentas de estos problemas y pueden sufrir considerablemente debido a la explotación de su imagen y voz.

4. EVALUACIÓN DE LOS DAÑOS

Los daños derivados del uso de la inteligencia artificial generativa son múltiples y profundos, afectando tanto a las víctimas individuales como a la sociedad en general. Aunque no existen estudios específicos sobre el impacto de la IA en la generación de pornografía, sí hay una vasta cantidad de investigaciones sobre la difusión de imágenes pornográficas no consentidas por internet. Estas situaciones son similares en cuanto al daño causado, aunque en el caso de la IA generativa, no es el cuerpo verdadero de la persona el que se expone, sino una representación que parece auténtica y tiene el mismo potencial de generar daño.

a) Antijuricidad y Daño

La creación de *deepfakes* y deepnudes mediante IA generativa infringe claramente el deber general de no dañar a otro, violando la antijuricidad objetiva establecida en el artículo 1717 del Código Civil y Comercial de la Nación (CCCN). La difusión de estos contenidos sin el consentimiento de la persona afectada constituye una violación grave de su privacidad y dignidad, generando un daño significativo a nivel psicológico, emocional y social.

b) Causalidad

La relación de causalidad en la responsabilidad civil es crucial para determinar quién es el responsable del daño. En el caso de la IA generativa, es fundamental establecer el nexo causal entre el uso de la tecnología y el daño sufrido por la víctima. Esto incluye la prueba de que una imagen o video creado por IA causó directamente la angustia, la pérdida económica o el daño reputacional de la víctima. Por ejemplo, el caso de Taylor Swift, víctima de deepfakes pornográficos, muestra cómo la difusión de estos contenidos puede causar un daño irreparable a su reputación y bienestar emocional.

c) Factores de Atribución

Los factores de atribución en la responsabilidad civil pueden ser objetivos o subjetivos. En el contexto de la IA generativa, la creación de contenido dañino puede ser evaluada bajo estos factores dependiendo de si fue intencional (dolo) o resultado de una falta de diligencia (culpa). La asignación de responsabilidad puede recaer en los desarrolladores de la IA, los usuarios que manipulan la tecnología con fines maliciosos, o las plataformas que permiten la distribución del contenido.

d) Prevención y Reparación

El artículo 1716 del CCCN enfatiza la función preventiva y reparadora de la responsabilidad civil. En el contexto de la IA generativa, esto se traduce en la necesidad de implementar medidas que eviten la creación y difusión de contenido dañino y aseguren que las víctimas reciban una compensación adecuada por los daños sufridos. La reparación puede incluir tanto daños patrimoniales como morales, alineándose con el objetivo de restablecer la situación anterior al daño. Por ejemplo, la necesidad de compensar a víctimas como Scarlett Johansson, cuya voz fue clonada sin su consentimiento por OpenAI, subraya la importancia de la reparación en estos casos.

e) Impacto Social y Psicológico

El impacto social y psicológico de la difusión de imágenes no consentidas es devastador. Las víctimas pueden experimentar ansiedad, depresión y otros trastornos relacionados con el estrés debido a la exposición no consensuada de contenido íntimo. Desde una perspectiva social, estos incidentes erosionan la confianza en los medios digitales y fomentan un ambiente de desconfianza y escepticismo sobre la autenticidad de la información. Psicológicamente, las víctimas como Taylor Swift enfrentan una violación significativa de su privacidad y dignidad, generando un daño profundo a su bienestar emocional y social.

5. INTERPRETACIÓN SEGÚN LA NORMATIVA

En la legislación argentina, el derecho a la imagen personal está regulado principalmente por el nuevo Código Civil y Comercial de la Nación, que establece en su artículo 53 la necesidad de consentimiento para captar o reproducir la imagen o la voz de una persona, salvo en excepciones como la participación en actos públicos o por interés científico, cultural o

educacional. Este marco normativo busca proteger los derechos personalísimos de los individuos, garantizando que su imagen y voz no sean utilizadas sin su autorización y permitiendo su libre revocabilidad. Además, el artículo 55 refuerza que el consentimiento debe ser expreso, no presumido y de interpretación restrictiva, subrayando la importancia de la protección de la identidad y privacidad de las personas.

Las inteligencias artificiales generativas, al ser entrenadas con grandes volúmenes de datos que pueden incluir imágenes personales, pueden ser responsables por el uso indebido de la imagen de personas que no consintieron su uso. Cuando estas IA generan reproducciones fieles de individuos, como en el caso de deepfakes, se produce una vulneración directa de los derechos a la imagen y a la voz. Además, quienes utilicen estas herramientas para crear situaciones ficticias que nunca ocurrieron, pueden incurrir en responsabilidad por los daños ocasionados, dado que estas acciones contravienen lo establecido en relación con la reproducción no ofensiva de la imagen personal. Esto pone en evidencia la necesidad de una regulación más precisa que contemple estos nuevos desafíos tecnológicos.

Aunque las situaciones mencionadas pueden encuadrarse dentro de la normativa existente, sería beneficioso para la protección de los derechos de las personas una reforma normativa que aborde específicamente los usos dañinos de las herramientas de IA generativa. Esta reforma debería incluir disposiciones claras sobre la responsabilidad de los desarrolladores y usuarios de estas tecnologías, así como mecanismos efectivos de prevención y reparación de daños. La actualización del marco legal no solo brindaría mayor seguridad jurídica, sino que también permitiría adaptarse a las rápidas innovaciones tecnológicas, garantizando una protección adecuada y contemporánea de los derechos personalísimos frente a los avances de la inteligencia artificial.

VEHÍCULOS AUTÓNOMOS, SOFTWARE Y RESPONSABILIDAD POR DEFECTOS OCULTOS

Por Lucas P. Leiva Fernández[1]

I. CONCLUSIONES

1. Si existe un defecto funcional, para responsabilizar al fabricante del vehículo autónomo deberá ponderarse si cuenta con el software actualizado. Recién a partir de la actualización del software, correrían los plazos comprendidos en la garantía legal del vicio redhibitorio para poder demandar al fabricante del automotor.

2. Es deseable establecer un tope de responsabilidad respecto de la responsabilidad del fabricante del vehículo autónomo, otorgado por la garantía legal del vicio redhibitorio, la cual correrá para el guardián una vez actualice el software vehicular.

3. Ante cada nueva actualización de software de conducción autónoma realizada por el guardián diligente, renovará la responsabilidad por parte del fabricante de automotor al crear la posibilidad de que exista un vicio redhibitorio si falla dicho software.

4. Si el guardián no realiza las actualizaciones de software pertinentes y éste último falla, no podrá demandar al fabricante del automotor autónomo.

5. La actualización de software en automotores autónomos impide la caducidad del derecho a reclamar por vicios redhibitorios

---

[1] Abogado (Universidad de Buenos Aires). Magíster en Derecho Civil (Universidad Austral) Profesor Adjunto en la Cátedra de "Contratos Civiles y Comerciales" del Dr. Oscar J. Ameal en la UBA. Profesor Adjunto en la Cátedra de "Obligaciones Civiles y Comerciales" del Dr. Ignacio E. Alterini en la UMSA. Profesor y Coordinador en la Maestría de Derecho Civil – Universidad Austral. Profesor en "Curso Regular de Capacitación" en Cam. Nac. Civ.

II. FUNDAMENTOS

1. INTRODUCCIÓN

El 27 de enero de 2017, un informe con recomendaciones sobre "Normas de Derecho civil sobre robótica" dirigido a la Comisión de Asuntos Jurídicos del Parlamento Europeo presentado por Mady Delvaux fue aprobado con 17 votos a favor y 2 en contra[2].

En dicho informe, se establecieron ciertos aspectos éticos los cuales son los siguientes: "1) beneficencia (los robots deben actuar en beneficio del ser humano); 2) no maleficencia (los robots no deben hacer daño al ser humano); 3) autonomía (la interacción humana con robots debe ser voluntaria); 4) justicia (los beneficios de la robótica deben distribuirse equitativamente)"[3].

Allí se establecieron pautas por ejemplo la de establecer una definición europea común de robots autónomos «inteligentes», teniendo en cuenta las siguientes características:

– la capacidad de adquirir autonomía mediante sensores y/o mediante el intercambio de datos con su entorno (interconectividad) y el análisis de dichos datos;

– la capacidad de aprender a través de la experiencia y la interacción;

– la forma del soporte físico del robot;

– la capacidad de adaptar su comportamiento y acciones al entorno.

- A estas características hay que sumarle que supere la prueba del Test de Turing, es decir que demuestre la persona electrónica que tiene consciencia de sí misma. Una aproximación interesante hecha por Stuart M. Shieber, profesor de Harvard especializado en lingüística computacional,

---

[2] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//ES#title10 Consultado el día 19 de junio de 2024

[3] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//ES Consultado el día 19 de junio de 2024

considera al Test de Turing como una prueba interactiva de inteligencia[4] (similar a la que poseemos los humanos para entablar y construir relaciones.)

Y en lo que concierne a la persona electrónica se peticionó en dicho informe, a la Comisión para que se cree una personalidad jurídica específica para los robots denominada "personas electrónicas." "f) crear a largo plazo una personalidad jurídica específica para los robots, de forma que como mínimo los robots autónomos más complejos puedan ser considerados personas electrónicas responsables de reparar los daños que puedan causar, y posiblemente aplicar la personalidad electrónica a aquellos supuestos en los que los robots tomen decisiones autónomas inteligentes o interactúen con terceros de forma independiente."[5]

En el informe también se propuso la introducción de un sistema de registro de robots avanzados que estaría gestionado por una agencia de la Unión para la robótica y la inteligencia artificial. Posiblemente uno de sus atributos de la personalidad, no sea un nombre, sino una identificación.

El robot Sophia, fue reconocido como ciudadano en Arabia Saudita mientras mantuvo una entrevista con el público revelando rasgos de humor y resaltando cualidades derivadas del ser humano.[6]

Es claro que en muchas ocasiones se podrá determinar que, a pesar del comportamiento emergente del robot, él era predecible y por lo tanto cabe responsabilizar a alguien. Muchas veces la responsabilidad será similar a la atribuida a los dueños de animales como garantes de una fuente de peligro.

2. PARTICULARIDADES DE LOS VEHÍCULOS AUTÓNOMOS

En cuanto a los vehículos autónomos, son módulos independientes capaces de transportar a personas y cosas sin la intervención humana en la

---

[4] https://www.eecs.harvard.edu/shieber/Biblio/Papers/turing-aaai-senior.pdf *" I have argued that the Turing Test is appropriately viewed not as a deductive or inductive proof but as an interactive proof of the intelligence of a subject-under-test."* Consultado el día 19 de junio de 2024

[5] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//ES#title10 Consultado el día 19 de junio de 2024

[6] https://www.infobae.com/america/tecno/2017/10/27/sophia-el-primer-robot-en-obtener-una-ciudadania/ Consultado el día 19 de junio de 2024

conducción. Estos perciben el entorno a través de cámaras y sensores que cuentan con una tecnología llamada Lidar (*light detection and ranging*, o detección por luz y distancia) que sirve para saber cuándo cambia el semáforo, o se cruzan peatones o ciclistas, o todo otro dato del entorno del vehículo[7].

Los vehículos autónomos se dividen en dos grandes categorías. Por un lado, los vehículos semiautónomos, que contienen un dispositivo que permite la realización automática de ciertas operaciones de conducción, es decir, la conducción debe estar bajo el control permanente del humano. Por el otro, los vehículos autónomos, que garantizan la totalidad de estas operaciones, por lo que —en los niveles más altos de automatización— el vehículo es capaz de operar sin intervención humana y con la automatización completa también en cualquier carretera y en cualquier condición.

Existen niveles de automatización según Cecilia Danesi[8] los cuales son: 0 (sin automatización), 1 (asistencia de conducción) y 2 (automatización parcial), interviene el conductor humano; mientras que los niveles 3 (automatización condicional), 4 (alta automatización) y 5 (automatización completa).

Según esta autora[9] de los niveles 0 a 3 el rol del conductor es activo, por lo que, se debería aplicar la teoría del riesgo.

En el nivel 4 y 5 no se requiere conductor por lo que es difícil atribuirle responsabilidad, por lo que se haría responsable al titular o al fabricante del vehículo automatizado.

Sostiene que el art. 1769 se aplica a los daños causados por la circulación de vehículos remitiéndose a los arts. 1757 y 1758 de cosas riesgosas por responsabilidad objetivo, siendo amplio el término "circulación de vehículos".

A ello se suma el tema de la actualización del software por parte del guardián. El *Crash Optimization Algorithm* se encuentra presente en automotores autónomos niveles 4 y 5 permitiendo minimizar los daños. Este

---

[7] DANESI, Cecilia C., "Inteligencia artificial y responsabilidad civil: un enfoque en materia de vehículos autónomos", La Ley Online, Cita Online: TR LALEY AR/DOC/2374/2018

[8] Idem.

[9] Idem

algoritmo busca minimizar los daños causados por un accidente de tráfico inevitable. Se encarga de decidir contra qué o contra quién debe impactar. Estas actualizaciones deberían ser realizadas por el guardián.

Da de ejemplo[10] el accidente protagonizado el 7 de mayo de 2016 por un Tesla modelo S semiautomático, el que golpeó y pasó por debajo de un camión que estaba realizando una maniobra de giro, produciéndole la muerte al conductor del vehículo. Las investigaciones arrojaron que, aunque el piloto automático funcionaba como estaba diseñado, no detectó el camión, dado que este estaba cortando el camino del automóvil en lugar de conducir directamente enfrente de él. El sistema no estaba entrenado para reconocer la parte plana del camión como una amenaza. La falta de capacidad de respuesta del conductor del Tesla indicaba una dependencia excesiva de la automatización, por lo que, la autoridad competente concluyó que el choque no fue causado por un defecto específico en el sistema de piloto automático y, consecuentemente, Tesla no fue responsable del accidente. Se señaló que Tesla hizo lo correcto al advertir a sus clientes que el sistema de piloto automático exige su supervisión permanente.

Cuando se discute sobre responsabilidad de vehículos autónomos también debe traerse a colación los graves problemas éticos sobre tomas de decisiones.

El caso ficticio, trata sobre un vehículo autónomo que tiene los frenos desgastados y se encuentra con 5 peatones que cruzan la calle. Las únicas dos opciones que tiene son las siguientes:

1) atropellar a los 5 peatones con la consecuencia de sus fallecimientos.

2) girar bruscamente, colisionar contra una pared, salvar la vida de los 5 peatones pero ocasionar la muerte de los ocupantes del vehículo.[11]

Frente a una situación en la cual se producirá necesariamente un resultado lesivo, el sistema tiene que elegir cuál tendrá lugar. Influenciado por la ideología norteamericana el automotor tendrá que dirigirse allí donde el resultado lesivo sea menor (en cantidad, en calidad o ambas). Influenciado por la filosofía alemana, no podrá doblar y poner en riesgo a sujetos que no

[10] Idem.

[11] https://www.nytimes.com/2016/06/24/technology/should-your-driverless-car-hit-a-pedestrian-to-save-your-life.html?mcubz=1 Consultado el día 19 de junio de 2024

hayan estado anteriormente sometidos a riesgo alguno. El quid, bien se señala es ¿Qué empresa publicitará un automotor que sacrifique a sus ocupantes?[12].

Se cuestiona si el instituto de la responsabilidad por el hecho ajeno (tutores, padres por los hijos, etc.) resulta aplicable para tecnologías como la IA. No es que se pretenda asimilar a los humanos a aquella, sino que al compartir con estos el carácter de autónomos, permite —ante el vacío legal— aplicar ciertos institutos por analogía. También se aborda la corriente que propone utilizar las normas de responsabilidad por los daños causados por animales. Esta se basa en la similitud existente entre la falta de previsibilidad de las acciones de aquellos y la IA, es decir, vinculado al comportamiento autónomo. En ambos supuestos (hecho ajeno y animales), el ordenamiento jurídico argentino determina que la responsabilidad será objetiva (arts. 1756 y 1759 del Cód. Civ. y Com.).

Aun así, entiendo que existe una forma diferente de responsabilidad civil que no es tratada generalmente al analizar los vehículos autónomos. Es la responsabilidad civil producto del vicio redhibitorio.

3. MI PROPUESTA

A través de la garantía por vicios ocultos se garantiza el derecho y el estado físico de la cosa, su aprovechamiento práctico y económico. En Roma, el edil civil encargado de mercados y ferias hacía conocer a los potenciales compradores de esclavos y animales domésticos los defectos ocultos que adolecían.

Evicción y vicios redhibitorios son supuestos de responsabilidad postcontractual de origen legal.

Si la concurrencia de una característica o función específica en la cosa transmitida se establece especialmente por contrato, su ausencia pasa a ser considerada vicio redhibitorio (art. 1052), lo que es lógico porque para la causa común de las partes reviste suficiente entidad como para incorporarla al contrato.

---

[12] VARELA, Agustín, "Los robots autónomos y el problema de la atribución de resultados lesivos", La Ley Online, Cita Online: TR LALEY AR/DOC/3684/2018

Los defectos pueden catalogarse en estructurales o funcionales[13].

El defecto puede ser estructural —como de calidad de materiales, estado de cimientos o de partes no visibles como cañerías, defectos de diseño, etc.— o funcionales cuando, aunque la cosa no tenga defectos de diseño ni de materiales, su funcionamiento resulte ineficaz para el destino natural que deba prestar.

Acá entra el *quid* de las actualizaciones de software de los vehículos autónomos. Si existe un defecto funcional, se deberá tener en cuenta para responsabilizar al fabricante del vehículo que se posea el software vehicular más vigente, es decir, actualizado. Recién a partir de la actualización del software, correrían los plazos comprendidos en la garantía legal del vicio redhibitorio para poder demandar al fabricante del automotor.

Entonces, si hay vicio redhibitorio, el fabricante automotor responderá por saneamiento (art. 1034).

El guardián encargado de actualizar el software podrá:

a) reclamar que se subsane el defecto (art. 1039, inc. a);

b) obtener otra cosa equivalente sin el defecto (íd., inc. b);

c) resolver (íd., inc. c, y 1056) excepto que el defecto sea subsanable, el transmitente haya ofrecido subsanarlo y el adquirente no lo acepte (art. 1057).

A esas acciones se puede sumar la acción por resarcimiento de daños conforme al acápite del art. 1040, incluso en caso de sustitución de la cosa (art. 1057), excepto que se trate de alguna de las situaciones previstas en los incisos del art. 1040 que excluyen la acción de daños

Entonces, a partir de la actualización del software se podrá demandar al fabricante automotor por parte del guardián. Correrá el plazo de caducidad de 6 meses (Art. 1055 CCCN), sumado al plazo de 60 días de aviso de caducidad (aunque este último podríamos decir que el art. 1054 permite eximirse si el actualizador de software conocía o debía conocer el vicio) sumado a que tendrá un año de prescripción conforme art. 2564 inc. a.

De esta forma, concluyo que es sano establecer un tope de responsabilidad respecto de la responsabilidad del fabricante del vehículo

---

[13] LEIVA FERNÁNDEZ Luis F.P., "Tratado de los Contratos. Parte General", Bs. As., 2017,T.II, p. Conf. p. 111

autónomo, otorgado por la garantía legal del vicio redhibitorio, la cual correrá para el guardián una vez actualice el software vehicular.

De más está decir, que, cada nueva actualización de software de conducción autónoma realizada por el guardián diligente, renovará la responsabilidad por parte del fabricante de automotor al crear la posibilidad de que exista un vicio redhibitorio si falla dicho software por la nueva actualización.

Si el guardián no realiza las actualizaciones de software pertinentes y éste último falla, luego no podrá demandar al fabricante del automotor autónomo.

RESPONSABILIDAD DERIVADA DE LA UTILIZACIÓN DE VEHÍCULOS AUTÓNOMOS

Por Leonardo Marcellino[1]

I. CONCLUSIONES

1. Los vehículos autónomos permitirán una reducción en los índices de siniestralidad vial, pero aun así tendremos accidentes en donde, en ocasiones, la causa será una falla en los sistemas informáticos de conducción automatizada.

2. El régimen general de responsabilidad por daños emergentes del Código Civil y Comercial y leyes específicas en materia de accidentes de tránsito son una plataforma jurídica suficiente por el momento para regular los casos de daños provocados por vehículos autónomos.

3. En los casos de accidentes con vehículos autónomos se tratará de una responsabilidad objetiva con fundamento en el riesgo creado que hará responsable al dueño y guardián, pudiendo según la causa eficiente ampliarse la legitimación pasiva a los que participaron en calidad de "proveedores" en la cadena de comercialización del automotor.

4. En los supuestos de siniestros provocados por errores en el sistema de conducción automatizada, el dueño o guardián no podrán eximirse de responsabilidad alegando esa situación como un caso fortuito o que el programador o controlador o diseñador o actualizador o fabricante de ese sistema, sea un tercero por quien no deba responder, sin perjuicio de las eventuales acción de repetición que pueda tener.

II. FUNDAMENTOS

1. INTRODUCCIÓN

En la hora actual y más allá de la concepción personal que se pueda tener sobre el avance de las tecnologías, hoy se presenta como una realidad

---

[1] Abogado (Universidad Nacional de Córdoba). Magíster en Derecho y Argumentación (Universidad Nacional de Córdoba). Doctor en Derecho y Ciencias Sociales (Universidad Nacional de Córdoba). Profesor Titular Experto en la asignatura Privado VIII (Derecho de Daños) e Investigador en la Universidad Siglo 21. Docente Profesor Ayudante en la asignatura Privado VII (Derecho de Daños) en la Universidad Nacional de Córdoba. Miembro del Instituto de Derecho Civil de la Academia de Derecho Córdoba.

innegable la existencia de daños provocados por la inteligencia artificial, en las diversas formas en que aquella puede manifestarse.

Frente a la verificación de ese simple fenómeno fáctico es que ha surgido la necesidad de regular jurídicamente la utilización de la inteligencia artificial, es decir de brindarse herramientas legales adecuadas ante su incorporación a la realidad social y al tráfico jurídico.

Las formas de daños que puede provenir de la inteligencia artificial se muestran como absolutamente diversas, probablemente aun existan manifestaciones de dañosidad que se desconozcan, pero es cierto que estos sistemas de algoritmos artificiales parecen procurar, entre otras cuestiones, disminuir y no incrementar los daños en las actividades donde se ha introducido. Es más, existen estudios estadísticos que dan cuentan justamente de la reducción de siniestros en aquellos casos en los que se ha implementado la inteligencia artificial, en comparación a cuando las tareas eran cumplidas exclusivamente por hombres.

Aun así y aunque se aceptara que la implementación de la inteligencia artificial tiende a recortar posibles daños que los hombres causan, lo cierto que se tratan de daños *"nuevos",* en donde se plantea el debate en torno a si deben o no aplicarse los paradigmas clásicos de la responsabilidad civil.

Resulta difícil identificar al sujeto responsable, ya que detrás de un sistema de inteligencia artificial pueden aparecer un gran número de personas no visibles y la dificultad de imputación de los daños lleva inexorablemente a la problemática de ensayar o plantear un juicio de causalidad que parece escapar a las reglas clásicas de adecuación causal que adopta nuestra legislación a partir de un juicio de previsibilidad.

A lo anterior debe agregar una exigencia de conciencia colectiva, en virtud de la cual todo aquel que sufre un daño no debe resignarse a soportarlos, sino que tiene el derecho a reclamarlos y a que se le reparen, incluso prescindiendo en ocasiones de que se verifiquen los presupuestos legales de responsabilidad y dando lugar a lo que López Mesa denomina la *"ideología de la reparación"*[2].

[2] LÓPEZ MESA, Marcelo, "La ideología de la reparación y la concesión de resarcimientos porque sí", *LL* 2008-B-270.

Por lo anterior entiendo que la aparición de estas formas de daños a partir de la inteligencia artificial requiere de un abordaje jurídico, pero sobre todo de mesura y flexibilidad para que las reglas que se propongan se ajusten a la realidad cambiante, no obstaculicen el progreso de las tecnológicas y al mismo tiempo no incentiven la provocación de daños que pueden evitarse y también contribuyan a garantizar el derecho resarcitorio de las víctimas.

Frente a las diversas modalidades en que pueden presentarse la ocurrencia de daños mediante la utilización de inteligencia artificial en el presente trabajo se abordará los accidentes en lo que participa un vehículo *"autónomo"* y la cuestión a valorar es si realmente es necesario legislar con nuevas normas de responsabilidad que regulen estos daños, o si, por el contrario, es suficiente con las que ya existen, que en todo caso solo debieran adaptarse a este tipo de nuevos daños.

2. INTELIGENCIA ARTÍFICIAL Y VEHÍCULOS AUTÓNOMOS

En general, se destaca la dificultad de brindar un concepto de inteligencia artificial no solo por los diversos aspectos que la misma involucra, sino también porque se trata de un tema en permanente evolución tecnológica, pero más allá de ello, se han podido formular definición de la misma, a partir de algunas características relevantes que presenta.

La R.A.E. define la inteligencia artificial como una *"disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico*". En tanto que la Unión Europea mediante Resolución del Parlamento del 20/10/2020 lo define en su art. 4 a) como *"un sistema basado en programas informáticos o incorporado en dispositivos físicos que manifiesta un comportamiento inteligente, al ser capaz, entre otras cosas, de recopilar y tratar datos, analizar e interpretar su entorno y pasar a la acción, con cierto grado de autonomía, con el fin de alcanzar objetivos específicos*". En términos semejantes se expresó la Propuesta de Reglamento del Parlamento Europeo de 2020 sobre responsabilidad civil. En tanto que la Propuesta de Reglamento de inteligencia artificial de 2021, en el art. 3 la conceptualiza como *"el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I, y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa"*.

Las definiciones brindadas permiten destacar como notas salientes que la misma involucra programas informáticos, los cuales permiten cumplir con diversas actividades de inteligencia de los humanos e incluso con cierto grado de autonomía.

Esta característica de brindar grados de autonomía por parte de estos sistemas tecnológicos que colabora, auxilia y en ocasiones reemplaza a la inteligencia humana, en su aplicación a los vehículos de circulación ha dado lugar a que los mismos presenten una conducción automatizada de diversos niveles.

Así puede hablarse de una conducción automatizada parcial cuando el vehículo puede realizar todas o algunas de las funciones de la conducción conforme a un sistema de programación, pero bajo el control y supervisión del conductor humano; una conducción autónoma o de automatización total, cuando es el propio vehículo el que toma el manejo de la cosa y decisiones conductivas sin intervención humana, conforme a un sistema de programación; y la conducción tradicional en el que las decisiones son exclusivas del humano al volante.

Nos interesa particularmente en el trabajo el caso del vehículo con conducción autónoma, donde la automatización es total, y por lo tanto no hay un conductor humano, sino que el mismo es reemplazado por un sistema informático de inteligencia artificial, y solo se tiene como ser humano al pasajero que no tiene control sobre la conducción del vehículo.

Se ha definido a los vehículos autónomos como *"módulos eléctricos capaces de transportar personas y cosas sin intervención humana en la conducción. Estos perciben el entorno a través de cámaras y sensores que cuentan con una tecnología llamada "Lidar" (Light Detection and Ranging, o detección por luz y distancia) que sirve para saber cuándo cambia el semáforo o se cruzan peatones o ciclistas o todo otro dato del entorno del vehículo"*[3]

Estos vehículos autónomos, que conforme a la clasificación elaborada en 2014 por la Sociedad de Ingenieros de Automoción Internacional (SAE) tiene un nivel 5 de total automatización, ya circulan en

[3] DANESSI, Cecilia C., *Accidentes de tránsito. Daños ocasionados por la circulación de vehículos*, Ed. Hammurabi, Bs. As., 2019, p.400.

diversos lugares del mundo generándose cuestionamientos con relación a los siniestros que pueden ocasionar.

Es de destacar que como se dijo en la introducción que lo que se procura a través de esa mayor y en casos total autonomía artificial, es contribuir a un menor número de accidentes en comparación a los que ocurrirían si el conductor fuera humano.

Y probablemente se logre ese objetivo, si se piensa que se podría evitar al error humano como causante del siniestro vial, ya sea por distracciones o negligencia o impericia al volante, o bien disipando que sean factores externos como animales sueltos en ruta o internos como fallas de frenos, entre otros casos, los causantes de accidentes alertando de esas circunstancias al sistema informático de conducción para impedir colisiones.

Lo cierto es que aun cuando los peligros de accidentes viales puedan reducirse mediante el empleo de vehículos autónomos, en modo alguno podrán eliminarse y de hecho ya hay casos de siniestros en los que se encuentran involucrados autos de este tipo.

De allí que no resulta baladí plantear si en estos casos corresponde que los mismos se resuelvan, en caso de tener lugar en algún momento en nuestro país, con el régimen legal existente, o si por el contrario es preciso otro especial.

3. NORMATIVA REGULATORIA DE ACCIDENTES CON VEHÍCULOS AUTÓNOMOS

Se sabe que la responsabilidad por daños causados en lo que hay una participación de un vehículo en circulación encuentra su régimen normativo en los arts. 1757 y 1758 CCCN a partir de la remisión efectuada por el art. 1769 CCCN. Sea que se lo considere un supuesto de responsabilidad por el riesgo o vicio de la cosa o por el desarrollo de una actividad riesgosa o peligrosa, en cualquier caso, se trata de una responsabilidad de tipo objetiva.

Además de la normativa reseñada, la misma tiene que ser completada con el Régimen Jurídico del Automotor (Decreto-Ley Nº 6582/58, ratificado por la Ley Nº 14.467, y sus modificatorias), así como con la legislación de tránsito aplicable a la materia.

El art. 5 del Régimen Jurídico del Automotor considera como automotores a los vehículos que tengan la capacidad de autopropulsión, es decir que se puedan impulsar por su propia fuerza motriz. Claramente los

vehículos autónomos poseen esa característica y por lo tanto quedan subsumidos en este Régimen.

Si los vehículos autónomos son considerados automotores a los fines de nuestra legislación nacional, entonces no cabe duda de que, en caso de daños causados por su circulación, será de aplicación la remisión del art. 1769 CCCN.

Se sostiene que el fundamento objetivo de esta responsabilidad anida en la teoría del riesgo creado. Dicha teoría explica que la intervención dañosa de ciertas cosas en la realidad fáctica, por las características intrínsecamente activas de la mismas ya que escapan al control absoluto humano, y que además poseen por su naturaleza o modo de uso una potencialidad mayor de daños, hacen responsable al sujeto por esa generación de *"riesgo creado"* en forma objetiva, es decir con absoluta prescindencia a si el mismo obedeció o no a un obrar reprochable de su parte.

Aun cuando se sostuviera y comprobara que la conducción autónoma en reemplazo de la humana va a reducir la siniestralidad vial, no parece haber duda de que la sola circulación en velocidad del vehículo autónomo es en si misma riesgosa o peligrosa.

Con prescindencia a si el conductor es un humano o una máquina, en todos los casos hay un desplazamiento de una cosa a velocidad que escapa al control absoluto humano, más si es totalmente automatizado, y por esa circunstancia tiene la potencialidad o *"aptitud para causar daños frecuentes o graves"*[4], que es lo que denota su peligrosidad y el carácter objetivo de la responsabilidad.

Al respecto se sostiene que el fundamento para aplicar reglas de responsabilidad objetiva a los daños causados por inteligencia artificial es que cuando el sistema es inteligente, ya es capaz de aprender de su entorno y de tomar sus propias decisiones, su utilización implica una creación anormal de un riesgo de producción de daños para terceros[5].

4. LEGITIMADOS PASIVOS

[4] MARCELLINO, Leonardo, "Actividades riesgosas o peligrosas: posibles respuestas a algunos de los interrogantes que plantea su regulación en el Código Civil y Comercial", RCCyC 2020 (marzo), 91 Cita: TR LALEY AR/DOC/4061/2019

[5] ATIENZA NAVARRO, María Luisa, *Daños causados por inteligencia artificial y responsabilidad civil*, Ed. Atelier, Barcelona, 2022, p. 243.

La normativa civil y comercial hace responsable en su art. 1758 CCCN al dueño y guardián en forma concurrente por los daños causados por las cosas.

Tratándose de vehículo autónomos y en virtud de lo explicado anteriormente, no hay impedimento para tener como responsable al dueño, entiendo por tal al sujeto que tiene anotado a su nombre la titularidad dominial del automotor en el Registro Nacional de la Propiedad del Automotor en virtud del carácter constitutivo de la inscripción registral, a tenor del art. 1 del Régimen Jurídico del Automotor.

A su vez nuestra legislación no refiere, como en España, al *"conductor"*, como otro legitimado, sujeto respecto del cual habría sido problemático su determinación tratándose de vehículos autónomos, sino que en forma más amplia refiere al guardián, entendiendo por tal *"...a quien ejerce, por sí o por terceros, el uso, la dirección y el control de la cosa, o a quien obtiene un provecho de ella"*.

El uso importa el hecho de servirse de la cosa en propio interés; la dirección denota la existencia de un poder del sujeto sobre la cosa para que se desplace a su voluntad; el control significa que el guardián puede vigilar o supervisar el uso y manipulación de la cosa; y finalmente la obtención del provecho refiere a que la cosa le debe de reportar alguna utilidad, sea o no de naturaleza patrimonial.

El concepto de guardián es bastante polémico, para algunos[6] reviste esa condición únicamente el sujeto que tiene un poder de hecho sobre la cosa que le permite dirigirla, controlarla o gobernarla, se sirva o no de la misma;

---

[6] PICASSO, Sebastián y SÁENZ, Luis R. J., *Tratado de derecho de daños*, T. II, Ed. La Ley. Bs. As., 2019, p. 159. LÓPEZ MESA, Marcelo, *Código Civil y Comercial de la Nación. Comentado. Anotado*, T. 10-B, Ed. Hammurabi, Bs. As, 2019, p.268. LUCCHESI, Mauro D., y SÁENZ, Luis R. J., *Código Civil y Comercial de la Nación y normas complementarias. Análisis doctrinal y jurisprudencial*, T. 3F, Dir. Bueres, Ed. Hammurabi, Bs. As., 2018, p.631. GALDÓS, Jorge M., *La responsabilidad civil. Análisis exegético, doctrinal y jurisprudencial: Arts. 178 a 1780, CCCN*, T. III, Ed. Rubinzal Culzoni, Santa Fe, 2021, p. 260/262. GALDÓS, Jorge M., *Código Civil y Comercial de la Nación. Comentado*, T. VIII, Dir. Lorenzetti, Ed. Rubinzal Culzoni, Santa Fe, 2015 ,p. 595 y ss. SAGARNA, Fernando A., *Código Civil y Comercial explicado. Doctrina-Jurisprudencia. Responsabilidad Civil*, Dir. Lorenzetti. Ed. Rubinzal Culzoni, Santa Fe, 2021, p. 262.

mientras que para otros autores[7] admiten que además de los anteriores son guardianes (guardia conjunta) lo que obtienen un beneficio de la cosa, a pesar de no tenerla bajo su custodia.

Ahora bien, aun cuando se sostenga que el rasgo fundamental para que pueda hablarse de guarda, es que el sujeto tenga el poder de control o vigilancia completo sobre la cosa, y de este modo posibilidad de evitar que cause un daño, se acepta que basta que ese poder se tenga en forma táctica o potencial[8].

Lo propio del vehículo autónomo es que el sujeto que es transportado no tiene la conducción del mismo que se realiza en forma independiente, con lo cual podría decirse hay una ausencia de poder efectivo de control y dirección de la cosa. Sin embargo, subsiste un poder potencial de supervisión sobre la cosa, en la medida que la persona humana en cualquier momento pueda dejar de ser pasajera y tomar la conducción tradicional del automotor. Ese control potencial nos parece es suficiente para considerar guardián al sujeto transportado, e impedir que pueda alegar su eximición de esa condición por no revestir la calidad de conductor del vehículo. Además, en todos los casos este pasajero tendrá un provecho del transporte.

Ahora bien, la responsabilidad de estos sujetos mencionados en el art. 1758 CCCN no excluye la posibilidad de imputar responsabilidad a otros legitimados pasivos, como podría ser un principal respecto del cual el dueño o guardián reviste la condición de dependiente en los términos del art. 1753 CCCN, pero sobre todo en los casos en los cuales la causa del siniestro se deba a una falla del software de *"sistema de conducción automatizado"*, podrá ser de aplicación la normativa consumeril, y hacerse responsable a una pluralidad de sujetos, sea en forma directa por la víctima o por vía de regreso en caso de condena del propietario o guardián, a todos aquellos que participaron en la cadena de comercialización del producto e incluso, cuando sea posible de identificar, a los propios programadores o creadores del software así como los encargados de su control y actualización (incluso hay

---

[7] PIZARRO, Ramón D., "Tratado de la responsabilidad objetiva", T. I, Ed. La Ley, Bs. As., 2015, n°77, p.521. KEMELMAJER DE CARLUCCI, Aida, "Código Civil y leyes complementarias", T. 5, Dir. Belluccio y Coord. Zanoni, Ed. Astrea, Bs. As., 1984, n°18, p.470/471. CAZEAUX, Pedro N., y TRIGO REPRESAS, Félix A, "Derecho de las obligaciones", T. V, 4ª ed., Ed. La Ley, Bs. As., 2010, n°2749, p.281/282.

[8] ZAVALA DE GONZÁLEZ, Matilde, y GONZÁLEZ ZAVALA, Rodolfo, *La responsabilidad civil en el nuevo Código*, T. III, Ed. Alveroni, Cba., 2018, p.731.

doctrina[9] que le asigna a ellos el carácter de guardián técnico o intelectual del rodado) y a fabricantes del hardware del sistema de inteligencia artificial aplicado al vehículo.

5. EXIMENTES PARTICULARES

Se entiende que un gran número de los siniestros provocados por vehículos autónomos se provocaran por defectos de los automóviles, con lo cual puede haber un desplazamiento de las reglas de responsabilidad del propietario y guardián hacia los integrantes de la comercialización del producto.

Sobre el particular el planteo es si en el caso de determinarse que la causa del accidente en el que participó un vehículo autónomo fuera una falla en el sistema informático de conducción, ello puede ser alegado por el propietario o guardián para liberar su responsabilidad, sosteniendo o bien que en estos casos el vehículo fue utilizado en contra de la voluntad expresa o presunta de aquéllos (art. 1758 CCCN); o bien que los diseñadores o programadores del software que provocó la falla, o el fabricante, o vendedor, u otros sujetos que participación en la cadena de comercialización pueden ser tenidos como terceros por quien el dueño y guardián no deba responder (art. 1731 CCCN).

Personalmente me pronuncio decididamente en contra de dicha eximición de responsabilidad de parte del dueño y guardián del vehículo autónomo en esos casos.

Primeramente, la eximente referida al uso de la cosa en contra de la voluntad expresa o presunta no puede tener cabida aquí, ya que como sostiene Pizarro[10] la misma requiere de un desapoderamiento o apropiación indebida del vehículo y que esa circunstancia no le sea imputable al dueño o guardián.

En el caso de los vehículos autónomos, por las propias características que justamente definen esta clase de automotores, tanto el que lo adquiere en propiedad, como aquel que lo usa y obtiene un provecho del mismo, han de algún modo consentido la delegación de la conducción vehicular en el

---

[9] DANESSI, Cecilia C., *Accidentes de tránsito. Daños ocasionados por la circulación de vehículos*, Ed. Hammurabi, Bs. As., 2019, p.408.

[10] PIZARRO, Ramón D., *Tratado de la responsabilidad objetiva*, T. I, Ed. La Ley, Bs. As., 2015, n°81, p.549.

sistema informático del rodado, y ello importa asumir los riesgos de esa situación. El mero hecho de ocurrir una falla técnica en la conducción no importa un desapoderamiento del vehículo o que el uso del mismo haya sido contra la voluntad del sujeto transportado o dueño, aun cuando no haya llegado al destino programado.

En segundo término y con relación a la eximente del hecho de un tercero por quien no se debe responder, debe recordarse que ahora el art. 1731 CCCN contempla que para su configuración debe reunir los caracteres del caso fortuito (arts.1730 y inc. e 1733 CCCN), esto son la imprevisibilidad e inevitabilidad y además la ajenidad.

El carácter de exterioridad o ajenidad que debe revestir el *casus* respecto al obrar del sindicado como responsable *"supone que se produzca fuera de su esfera de actuación, sin que haya colocado ningún antecedente causalmente idóneo que haga posible el suceso lesivo sobreviniente"*[11].

Este recaudo implica que la ocurrencia del hecho imprevisible o irresistible, no puede constituir una contingencia propia del riesgo de la cosa o de la actividad desarrollada. Así como la rotura o falla del mecanismo de frenos de un automotor con conducción tradicional no puede ser alegado

[11] PIZARRO, Ramón D. y VALLESPINOS, Gustavo C., *Tratado de Responsabilidad Civil*, T. I, Ed. Rubinzal-Culzoni, Santa Fe, nº154, p. 519. ALTERINI, Atilio A., AMEAL Oscar J. y LÓPEZ CABANA, Roberto M., *Derecho de obligaciones civil y comerciales*, 4ª ed., Ed. Abeledo-Perrot, Bs. As., 2009, n°835, p. 407. MOSSET ITURRASPE, Jorge, "Las eximentes en general", en *Responsabilidad civil*, Dir. Jorge Mosset Iturraspe, 2ª reimpr., Ed. Hammurabi, Bs. As., 1997, n°54, p.128. MEIJIDE, Marcela, "Las eximentes de la responsabilidad", en *Responsabilidad y Derecho de Daños*, Dirs. Carlos Alberto Ghersi y Celia Weingarten, Ed. Nova Tesis, Rosario, 2016, p.198. PICASSO, Sebastián, *Código Civil y Comercial de la Nación comentado*, T. VIII, Dir. Ricardo Luis Lorenzetti, Ed. Rubinzal-Culzoni, Santa Fe, 2015, p. 435. BUSTAMANTE ALSINA, Jorge, *Teoría General de la Responsabilidad Civil*", 9va ed., Ed. Abeledo-Perrot, Bs. As., 1997, n°714, p. 317. AZAR, Aldo M. y OSSOLA, Federico A., *Responsabilidad Civil*, en "Derecho Civil y Comercial", Dir. Julio César Rivera y Graciela Medina, Ed. Abeledo-Perrot, Bs. As., 2016, p. 366 y ss. ZAVALA DE GONZÁLEZ, Matilde y GONZÁLEZ ZAVALA, Rodolfo, *La responsabilidad civil en el nuevo Código*, T. II, Ed. Alveroni, Cba., 2018, p.312 y ss. ALFERILLO, Pascual A., *Código Civil y Comercial comentado. Tratado exegético*, T. VIII, Dir. Jorge H Alterini., Coord. Ignacio E. Alterini, Ed. La Ley, Bs. As., 2015, p.110/111. MAZEAUD, Henry, Jean y Léon y CHABAS, François, *Derecho civil*, T.2, traducción Luis Andorno, Ed. Zavalía, Bs. As., 2006, nº577, p.296. CAZEAUX, Pedro N. y TRIGO REPRESAS, Félix A., *Derecho de las Obligaciones*, T. I, 4ª ed., Ed. La Ley, Bs. As., nº456, p. 545. ZAVALA DE GONZÁLEZ, Matilde, *Resarcimiento de daños. Presupuestos y funciones del derecho de daños*, T. 4, Ed. Hammurabi. Bs. As., 1999, n°39, p. 304/305.

como caso fortuito frente a la víctima, lo mismo sucederá cuando el error provenga del programa informático de conducción autónoma del automotor, incluso si el mismo se deba a un hackeo realizado por un tercero (*"pirata informático").*

En consecuencia, *"cuando el daño sea debido a una decisión autónoma del sistema inteligente, la autonomía no será considerado un caso de fuerza mayor, puesto que esa posibilidad del sistema de tomar decisiones independientes es algo interno e inherente a la propia actividad de este tipo de vehículos"*[12].

Entonces el dueño o guardián por el solo hecho de haber hecho un aporte de riesgo a la sociedad, no pueden liberar y descargar su responsabilidad por fallas en el sistema conducción autónoma del vehículo, frente a la víctima, con aquellos participaron en la comercialización del producto (fabricante, diseñadores, programadores del sistema, vendedor, etc.).

En contra de lo anterior se ha sostenido que *"cuando, a pesar de la vigilancia del sujeto, el software no reacciona o no lo hace oportunamente, ello desliga la responsabilidad de la persona* ("transportada") *que se vio impedida de ejercer una guarda eficiente, y se traslada a los técnicos"*[13]. No se comparte lo anterior, no solo porque pone en cabeza de la víctima una prueba de causalidad de enorme dificultad, esto es probar que la causa fue un error en el sistema de conducción automatizada, sino principalmente porque no tiene en cuenta que la persona transportada ha sido la que introdujo la cosa riesgosa en el medio que provoca el daño.

Ahora bien, lo anterior no significa que la víctima no tenga posibilidad, en los casos de ser esa falla en el software de conducción la causa del daño, de efectuar su reclamo resarcitorio en forma concurrente al dueño y guardián y también a los que intervinieron en calidad de *"proveedor"* del producto como responsables solidarios en los términos de la ley consumeril. Y también que, en caso de ser demandado el dueño y guardián en forma exclusiva por el damnificado, éstos tengan también la

---

[12] ATIENZA NAVARRO, María Luisa, *Daños causados por inteligencia artificial y responsabilidad civil*, Ed. Atelier, Barcelona, 2022, p. 352.

[13]BARICCO PRATS, Macarena, "Vehículos autónomos y su impacto en el sistema de responsabilidad civil argentino", EBOOK-TR 2022 (Alterini), 608.Cita: TR LALEY AR/DOC/1225/2022

posibilidad de citar como terceros a los proveedores comerciales participantes para ejercitar las acciones de repetición pertinentes.

6. CONCLUSIÓN FINAL

Los vehículos autónomos con seguridad lograran una reducción considerable en los niveles de siniestralidad, pero no serán infalibles y lamentablemente se sucederán accidentes en los que se encuentren involucrados esta clase de automotor en los cuales el conductor no sea una persona humana.

Cuando ello suceda, se considera que el actual régimen de responsabilidad por daños de accidentes (fundamentalmente los arts. 1757 y 1758 CCCN) deviene aplicables y son suficientes para regular los siniestros viales que involucren a vehículos autónomos, más allá de las adaptaciones particulares al caso concreto que habrá de efectuarse en atención a las características de estos vehículos y al impacto progresivo que la tecnología tenga en estos casos.

RESPONSABILIDAD CIVIL POR LOS DAÑOS DERIVADOS DE VEHÍCULOS AUTÓNOMOS

Por Bárbara Alejandra Martínez[1]

I. CONCLUSIONES

1. La responsabilidad civil en siniestros viales protagonizados por vehículos autónomos debe enmarcarse dentro de un régimen de responsabilidad objetiva.

2. El deber de responder pesa sobre el propietario y el guardián del vehículo.

3. El conductor, ya sea cuando tiene el control del sistema de modo principal como cuando actúa supervisando el vehículo, será responsable en su calidad de guardián.

4. Otros sujetos, tales como el controlador del software, el programador, el encargado del mantenimiento y de las actualizaciones del software, pueden encuadrar en la categoría de guardián, en la medida que ejerzan un control sobre el vehículo.

5. La responsabilidad ha de extenderse al fabricante, en los supuestos de accidentes ocasionados por defectos de fabricación, diseño o de advertencias insuficientes del producto, supuesto en el que ha de aplicarse el art. 40 de la Ley 24.240.

II. FUNDAMENTOS

1. INTRODUCCIÓN

La irrupción de los vehículos autónomos, es decir aquellos que pueden conducir sin intervención humana, mediante sistemas avanzados de inteligencia artificial (IA), representa un cambio disruptivo en la movilidad

---

[1] Abogada. Auxiliar Letrada en el Juzgado en lo civil y comercial N°4 de Dolores (Provincia de Buenos Aires). Jefe de trabajos prácticos en la cátedra de derecho procesal civil y comercial y de obligaciones en la Facultad de Abogacía de la Universidad Atlántida Argentina, sede Dolores. Maestranda en Maestría de derecho Civil en la Universidad Austral. Con el aval de Daniel J. Bonino.

y plantea nuevas cuestiones jurídicas, especialmente en el ámbito de la responsabilidad civil.

Esta ponencia analiza cómo se configuraría la responsabilidad civil en Argentina ante siniestros viales ocasionados por la intervención de vehículos autónomos, en particular lo relativo al fundamento del deber de reparar y a los sujetos sobre quienes recae esa atribución de responsabilidad.

El objetivo es determinar si el estado actual de la legislación en la materia da respuesta a las hipótesis dañosas que podrían presentarse o si sería necesario la adaptación de aquella normativa, a fin de abarcar una realidad que cada vez se vuelve más palpable.

2. VEHÍCULOS AUTÓNOMOS

a) Definición. Características.

Inserte Se define como vehículo autónomo aquel que puede circular sin intervención humana por vías que no han sido diseñadas específicamente para ese tipo de automóviles y por las que circulan ciclistas, peatones y otros usuarios de vehículos convencionales. Emplean sistemas de automatización que llevan a cabo total o parcialmente la llamada "tarea de conducción dinámica" (DDT o Dynamic driving task)[2].

Los coches autónomos perciben el entorno a través de cámaras y sensores que cuentan con una tecnología llamada LIDAR (Light Detection and Ranging, o detección por luz y distancia) que sirve para saber cuándo cambia el semáforo, o se cruzan peatones o ciclistas, o todo otro dato del entorno del vehículo[3].

Además, están equipados con sistemas de posicionamiento, sistemas de comunicaciones, sistemas avanzados de control, sistemas de aprendizaje automático (machine learning), algoritmos complejos, controladores y actuadores, así como unidades de control con potentes procesadores para

[2] BUSTAMANTE DONAS, Javier, "Dilemas éticos de los vehículos autónomos: Responsabilidad ética, análisis de riesgo y toma de decisiones", disponible al 23/6/2024 en https://institucional.us.es/revistas/argumentos/25/09Art.pdf

[3] DANESI, Cecilia Celeste, "La responsabilidad civil en la era de la inteligencia artificial", La Justicia Uruguaya, T.156, DA-39, noviembre-diciembre 2018.

ejecutar software y transformar los datos recabados por los sensores en acciones sobre el volante, acelerador, freno, etc.

Con estas tecnologías, los vehículos automatizados pueden medir distancias, monitorear vehículos, peatones y obstáculos, detectar los bordes de la calzada, identificar y seguir las líneas de los carriles o leer las señales de tráfico[4].

b) Clasificación

Previo a adentrarnos en el análisis de la responsabilidad civil por los daños derivados de la intervención de los vehículos autónomos, es conveniente hacer una referencia a sus distintos niveles de autonomía para determinar, en base a ello, qué grado de intervención humana existe en la conducción de cada uno de ellos.

La Sociedad de Ingenieros de Automoción (SAE), entidad encargada de regular y estandarizar la movilidad en ingeniería aeroespacial y automoción, publicó en el año 2014 el estándar J3016[5], que es el documento que describe los sistemas de automatización de conducción de vehículos que realizan parte o la totalidad de la tarea de conducción dinámica (DDT) de forma sostenida. Proporciona una taxonomía con definiciones detalladas para seis niveles de automatización de la conducción, en función del nivel de atención e intervención del humano en la conducción.

Estos niveles son los siguientes:

- Nivel 0: conducción manual
- Nivel 1: conducción asistida
- Nivel 2: automatización parcial
- Nivel 3: automatización condicionada
- Nivel 4: automatización alta
- Nivel 5: automatización total

---

[4] Dirección General de Tráfico de España, disponible al 25/6/2024 en https://www.dgt.es/muevete-con-seguridad/tecnologia-e-innovacion-en-carretera/vehiculos-de-conduccion-automatizada/

[5] Su última revisión data del 30/04/2021. Disponible al 24/06/2024 en https://www.sae.org/standards/content/j3016_202104/

La intervención humana dependerá del nivel de automatización del vehículo de que se trate.

Así, en los niveles 0, 1 y 2 hay un humano conduciendo el vehículo que debe supervisar constantemente las funciones de asistencia, por ejemplo, el control de velocidad crucero, el asistente de estacionamiento, el centrado de carril, entre otras.

En el nivel 3 el conductor puede ceder el control al sistema autónomo aunque, en caso de emergencia, cuando el sistema detecta que se enfrenta a condiciones que lo superan, avisa para que el conductor vuelva a tomar el control, es decir que el humano debe mantenerse expectante durante todo el trayecto.

Por otra parte, en el nivel 4 el sistema realiza todas las tareas de conducción, incluso si el conductor humano no responde adecuadamente a una solicitud de intervención

Finalmente, en el nivel 5 el sistema realiza todas las tareas en todas las condiciones posibles. En este supuesto, el vehículo puede prescindir incluso de la figura del conductor, del volante y de los pedales.

3. RESPONSABILIDAD CIVIL POR DAÑOS DERIVADOS DE LOS VEHÍCULOS AUTÓNOMOS

a) Marco Legal

Si bien en nuestro país ha habido recientes intentos de adaptar la legislación a fin de introducir este tipo de tecnologías[6], lo cierto es que hasta el momento, no existe en el ordenamiento jurídico argentino una regulación específica sobre esta temática.

Abordando puntualmente el tema de la responsabilidad civil, entonces, habremos de recurrir a las normas generales, a efectos de evaluar si las mismas brindan el andamiaje adecuado para una realidad cada vez más cercana, o si, por el contrario, resulta necesaria una reforma legislativa.

---

[6] "La Ley Ómnibus autoriza los autos autónomos en Argentina: ¿un guiño para Tesla y Elon Musk?", publicado en https://www.lanacion.com.ar/autos/la-ley-omnibus-de-javier-milei-autoriza-los-autos-autonomos-un-guino-para-elon-musk-nid27122023/, disponible el 24/06/2024.

En tal sendero, he de señalar en primer lugar que, siempre que medie un transporte en automotor, ya sea convencional o autónomo, el riesgo opera como factor de atribución. Así, tratándose de accidentes de tránsito, resultará aplicable al caso el art. 1769 del CCyCN, que remite a las normas referidas a la responsabilidad derivada de la intervención de cosas, esto es, al art. 1757 del mismo cuerpo legal[7].

No hay dudas de que los vehículos autónomos son una cosa riesgosa, y que los daños que con su uso se causen, generan una presunción de responsabilidad en cabeza de su dueño o guardián.

La responsabilidad, entonces, será objetiva, pues, tal como ha sido señalado doctrinariamente, "quien se sirve de cosas que por su naturaleza o modo de empleo generan riesgos potenciales a terceros, debe responder por los daños que ellas originan"[8].

En cuanto a los sujetos responsables, están mencionados en el art. 1758 del CCyCN que determina que responden de manera concurrente el dueño y el guardián.

Con respecto al guardián, la norma establece que se considera tal a quien ejerce por sí, o por terceros, el uso, la dirección y el control de la cosa, o a quien obtiene provecho de ella. Se agrega que el dueño y el guardián no responden si prueban que la cosa fue usada en contra de su voluntad expresa o presunta.

b) Sujetos responsables

No hay dudas respecto de la responsabilidad que pesa sobre la figura del dueño o propietario del vehículo autónomo, derivada del riesgo creado por su puesta en circulación.

En cuanto al "guardián", en este tipo de automóviles, resulta más complejo determinar quien ocupa ese rol.

---

[7] Art. 1757 CCyCN: "Hecho de las cosas y actividades riesgosas. Toda persona responde por el daño causado por el riesgo o vicio de las cosas, o de las actividades que sean riesgosas o peligrosas por su naturaleza, por los medios empleados o por la circunstancia de su realización. La responsabilidad es objetiva. No son eximentes la autorización administrativa para el uso de la cosa o la realización de la actividad, ni el cumplimiento de las técnicas de prevención".

[8] PIZARRO, Ramón Daniel, "Responsabilidad civil por el riesgo o vicio de las cosas", Ed. Universidad, Buenos Aires, 1983, pág. 38

En primer lugar, se incluye dentro de aquella categoría al conductor. Obviamente, en los niveles 0, 1 y 2 aquél es quien tiene el control del vehículo, por lo que resultan aplicables las normas comunes sobre responsabilidad civil.

Asimismo, los niveles 3 y 4 demandan su presencia, de modo que el conductor es quien puede tomar la decisión final, imponiendo su voluntad sobre la del software.

Recordemos que conducir no es sólo manejar el volante, sino que también implica supervisar la conducción. Aquel que debe supervisarla (el conductor de respaldo) es quien genera el riesgo al introducir un vehículo automatizado en las vías y asumir su supervisión, y por este riesgo debe responder[9]. Encontrarse al mando de un vehículo implica un nivel de dirección y control que trasciende de la mera manipulación del volante. Así, conductor es quien responde del correcto control del vehículo y de las maniobras encaminadas a garantizar ese control, sin que sea condición "sine qua non" que la tarea mecánica se realice directa y personalmente. Es de esta dimensión de la conducción de donde se concluye que el conductor de respaldo es el conductor responsable de la conducción, aunque su intervención en la misma sólo sea a través de la supervisión.

En el nivel más alto de autonomía (nivel 5) el escenario es más complejo, en virtud de que nos encontramos frente a la posibilidad de que sea el software quien decida por si mismo contra qué conviene estrellarse, en la hipótesis de una colisión inevitable.

Si bien en este caso podría no existir la figura del conductor de respaldo como tal, la responsabilidad habrá de recaer sobre quien introdujo el vehículo totalmente automatizado en la vía pública, por haber puesto en peligro a los demás al poner en circulación el sistema autónomo, ya sea que se trate del propietario o de otro tipo de operador que, por ejemplo, controle el software.

---

[9] ZORNOZA SOMOLINOS, Alejandro (2021). "Vehículos automatizados y seguro obligatorio de automóviles: estudio de derecho comparado" (ed.). Madrid, Dykinson. Disponible al 24/6/2024 en https://elibro.net/es/ereader/bibliouaustral/189570?page=117 pág. 135

En estos tres últimos niveles, se hace necesario, además, poner atención sobre los nuevos actores que pueden llegar a tener participación activa en el hecho generador de responsabilidad, como los fabricantes, programadores y encargados del mantenimiento y de las actualizaciones del sistema.

Pensemos, por ejemplo, en la hipótesis de que alguno de los sensores del vehículo falle, de modo que no detecte la presencia de un peatón en su camino e impacte contra él, ocasionándole heridas graves. En tal caso, será posible dirigir la acción contra el fabricante, toda vez que el daño ha sido causado como consecuencia de un vicio o defecto del vehículo. El basamento de la responsabilidad lo encontraremos en el estatuto consumeril, en particular en la responsabilidad por producto defectuoso, prevista en el art. 40 de la Ley 24.240[10].

Son muchas las hipótesis de daños que podrían derivar del uso de estas tecnologías. Una de las que más preocupación genera es la posibilidad que tiene el sistema autónomo, de elegir a qué persona embestir, cuando existe más de una vida en juego. En este supuesto, sería de singular importancia analizar la tarea del programador, por ser quien aporta los datos al sistema autónomo. Si bien es cierto que el "machine learning" o aprendizaje automático de estas máquinas puede ser más o menos supervisado, en esa supervisión residirá la posibilidad de imputarle responsabilidad a tal sujeto, en su calidad de "guardián". Cuanto mayor sea la supervisión, mayor será el deber de responder, atento el poder de dirección que tal sujeto detenta sobre la cosa.

No es menor el papel que desempeñan las personas encargadas del mantenimiento y de las actualizaciones del software, atento que dicha tarea permite detectar errores, corregirlos y perfeccionar el sistema, a fin de dotar de mayor seguridad a estas tecnologías. Se trata de personas que deben actualizar, reparar, incorporar nuevas rutas, nuevas normas viales, señalizaciones, etc.

---

[10] ARTICULO 40. — Responsabilidad Solidaria. Si el daño al consumidor resulta del vicio o defecto de la cosa o de la prestación del servicio responderá el productor, el fabricante, el importador, el distribuidor, el proveedor, el vendedor y quien haya puesto su marca en la cosa o servicio. El transportista responderá por los daños ocasionados a la cosa con motivo o en ocasión del servicio. La responsabilidad es solidaria, sin perjuicio de las acciones de repetición que corresponda. Sólo se liberará total o parcialmente quien demuestre que la causa del daño le ha sido ajena.

Quienes ocupen estos roles ejercen un control sobre el vehículo y, por lo tanto, deben ser incluidos dentro de la categoría de "guardianes". Deberán responder en aquellos supuestos de siniestros viales producidos como consecuencia de errores, que han sido previamente superados por actualizaciones no instaladas en el vehículo.

4. CONCLUSIÓN

La revolución que han generado las nuevas tecnologías, en particular aquellas en las que se involucra el empleo de sistemas de inteligencia artificial, nos lleva a reflexionar sobre las viscisitudes que ocasionaría su implementación en nuestro medio, de cara a las eventuales responsabilidades que podrían surgir ante la posibilidad de daños derivados de su utilización.

En primer lugar y, tal como se adelantó al inicio de esta ponencia, el factor de atribución en esta materia ha de ser objetivo. Ello se justifica por la naturaleza de estas tecnologías. Los vehículos autónomos operan principalmente mediante algoritmos y sistemas de inteligencia artificial (IA), que pueden actuar de manera impredecible y sin intervención humana directa, convirtiéndolos, de tal modo, en cosas riesgosas.

Por otra parte, se advierte que la redacción de las normas vigentes en materia de accidentes de tránsito, en particular el art. 1769 del CCyCN, cuando se refiere a la "circulación de vehículos", resultan lo suficientemente amplias como para abarcar los siniestros viales que se produzcan como consecuencia de la utilización de los vehículos autónomos.

En consecuencia, la responsabilidad será objetiva y habrá de recaer sobre el propietario y guardián. En el caso de los niveles de conducción en los que resulta necesaria la intervención de un conductor humano, ya sea de modo principal o supervisando la conducción, no hay dudas de que éste califica como guardián. No obstante ello, será posible incluir en dicha categoría a otros operadores del sistema tales como los programadores y encargados del mantenimiento y de las actualizaciones del sistema, en virtud del control y dirección que ejercen sobre la cosa.

Finalmente, en aquellos supuestos en aquellos supuestos en que los daños sean causados por defectos en la fabricación, diseño o advertencias insuficientes del producto, la responsabilidad se trasladará al fabricante y devendrá aplicable la responsabilidad por producto defectuoso, contemplada en el art. 40 de la ley 24.240.

RESPONSABILIDAD CIVIL E INTELIGENCIA ARTIFICIAL

Por María José Motta[1]

I. CONCLUSIONES

Hacemos llegar las siguientes propuestas a la Comisión de daños de las JNDC:

En líneas generales decimos:

1. En Argentina, el marco regulatorio de la IA enfrenta varios retos. Primero, la legislación existente no aborda específicamente las cuestiones que plantea la IA, lo que genera lagunas jurídicas. Por ejemplo, la protección de datos personales es una cuestión crucial, especialmente con la aprobación de la Ley de Protección de los Datos Personales (Ley 25.326) en 2000, que debe ser actualizada para abordar los retos que presenta la IA (Ministerio de Justicia y Derechos Humanos, 2020). En segundo lugar, la transparencia y responsabilidad de los algoritmos de IA son cuestionamientos frecuentes. La opacidad en los modelos de IA dificulta la trazabilidad de las decisiones, lo que puede afectar derechos

2. En cuando a la aplicación del derecho de la responsabilidad civil ante daños acaecidos en el marco de la IA, y sin dejar de mencionar que existen diversos casos en los que pude verse subsumido el sistema de algoritmos, entendemos que:

3. La antijuridicidad debe ser analizada ex pos facto, es decir una ver producido el hecho (art. 1717 del CCCN),

4. El factor de atribución debería ser objetivo basado en el correcto uso de la IA (art. 1722 del CCCN), pero no debemos olvidar que la CSJN en el caso RODRIGUEZ, dio las pautas de la aplicación de la responsabilidad subjetiva para google (situación que podría ser aplicable a estos casos).

5. En cuando a la relación causal, en Europa se ha indicado que puede establecerse una causalidad presumida, y no resulta descabellado, si entendemos que el uso y destino en donde se aplica la IA resulta claramente determinado, por lo tanto la variación de ese destino o resultado, hace presumir la relación causal con el daño.

---

[1] Abogada, Titular de Legal Link, Diplomada en Litigación Penal (UCES). Especialización en Cibercrimen y Evidencia Digital (UBA).

6. Con relación al daño, no hay mucho que señalar, ya que deber ser acreditado por quien lo invoca (art. 1744 del CCCN),

7. En cuanto a la legitimación pasiva, en principio podemos referir que la misma reposa en quien tiene el dominio de la IA, su uso, o quien obtiene un provecho o se beneficia de la misma. Ante la concurrencia de estos supuestos la responsabilidad debe ser solidaria.

8. La aplicación de la LDC y su marco de responsabilidad también resultan plausibles como herramientas normativas cuando el daño es producido por quien ha adquirido el bien que emplea IA, y este le causa un daño propio o a su grupo familiar. También en los daños contra tercero el consumidor tendrá una acción de regreso basa en el estatuto del consumo en casos de daños producidos por el uso de la IA.

II. FUNDAMENTOS

1. INTRODUCCIÓN Y GENERALIDADES

La inteligencia artificial (IA) ha irrumpido en la sociedad moderna con una fuerza transformadora, impactando en diversos sectores y planteando nuevos desafíos legales y éticos. Este artículo explora las generalidades de la IA, su creciente ámbito de aplicación, el marco regulatorio nacional e internacional que se está gestando, y las principales problemáticas que surgen en torno a su desarrollo y uso responsable. Se busca brindar una visión crítica y actualizada sobre la IA desde una perspectiva jurídica, con el objetivo de contribuir al debate sobre su regulación y el establecimiento de un marco ético que garantice su desarrollo responsable.

La inteligencia artificial (IA) ha dejado de ser un concepto futurista para convertirse en una realidad palpable que está transformando la sociedad a pasos agigantados. Su capacidad para imitar la inteligencia humana, realizando tareas que requieren razonamiento, aprendizaje y percepción, ha revolucionado diversos sectores, desde la salud y la banca hasta la educación y la industria. Su desarrollo se basa en algoritmos y modelos matemáticos que procesan datos y detectan patrones, permitiendo a las máquinas realizar tareas que antes solo podían ser ejecutadas por humanos. Este avance sin precedentes ha generado una ola de entusiasmo e interés, pero también ha planteado una serie de desafíos legales y éticos que requieren una atención urgente.

2. GENERALIDADES DE LA IA

La IA se puede clasificar en dos categorías principales: IA débil o estrecha: está diseñada para realizar tareas específicas, como el reconocimiento de imágenes, la traducción automática o la recomendación de productos. Algunos ejemplos de IA débil son los asistentes virtuales como Siri o Alexa, los sistemas de recomendación de Netflix o Spotify, o los filtros de spam en los correos electrónicos. Estos sistemas, aunque pueden ser muy sofisticados, están limitados a su tarea específica y carecen de la capacidad para comprender o razonar de manera general.

IA fuerte o general: busca emular la inteligencia humana en su totalidad, con la capacidad de aprender, resolver problemas y adaptarse a nuevas situaciones de manera similar a un ser humano. Esta categoría aún se encuentra en una etapa temprana de desarrollo, con la investigación enfocada en el desarrollo de sistemas de IA que puedan comprender y razonar sobre información compleja. Se aspira a que la IA fuerte tenga la capacidad de resolver problemas complejos, aprender de nuevas situaciones y tomar decisiones basadas en la lógica y el razonamiento, de manera similar a como lo haría un humano.[2]

3. ÁMBITO DE APLICACIÓN DE LA IA

La IA está expandiendo rápidamente su presencia en diversos sectores, revolucionando la forma en que se llevan a cabo las actividades en diferentes áreas. Sus aplicaciones abarcan una amplia gama de sectores:

Salud: la IA está transformando la medicina, mejorando el diagnóstico de enfermedades a través del análisis de imágenes médicas, el desarrollo de tratamientos personalizados, la gestión de datos médicos, la robótica quirúrgica y la creación de nuevas herramientas para el análisis de datos genéticos. [3]

Banca: la IA se utiliza para detectar fraudes, analizar riesgos crediticios, gestionar carteras de inversión, brindar atención al cliente automatizada y mejorar la eficiencia de las operaciones financieras.

---

[2] Russell, S., & Norvig, P. (2020). Inteligencia Artificial: Un Enfoque Moderno (4ª ed.). Pearson.

[3] Topol, E. J. (2019). Medicina de alto rendimiento: la convergencia de la inteligencia humana y artificial. Medicina de la Naturaleza, 25(1), 44-56

Comercio electrónico: la IA se emplea para ofrecer recomendaciones personalizadas de productos, analizar el comportamiento de los clientes, optimizar los precios, gestionar los inventarios, desarrollar chatbots para atención al cliente, y mejorar la experiencia del usuario en línea.

Educación: la IA permite crear sistemas de aprendizaje personalizado, automatizar la evaluación, generar contenido educativo, desarrollar plataformas de tutoría virtual y analizar datos educativos para mejorar las estrategias de enseñanza.[4]

Manufactura: la IA se utiliza para optimizar los procesos de producción, automatizar el control de calidad, implementar el mantenimiento predictivo, gestionar la robótica industrial, y analizar datos de producción para mejorar la eficiencia y la productividad.

Transporte: la IA impulsa el desarrollo de vehículos autónomos, optimiza la gestión del tráfico, mejora la planificación de rutas, y optimiza la logística en la cadena de suministro.

Justicia: la IA se está aplicando al análisis de datos jurídicos, la predicción de sentencias, la gestión de casos, la detección de fraudes, y la creación de sistemas de inteligencia artificial para la asistencia legal.[5]

Seguridad: la IA se utiliza para el reconocimiento facial, la detección de amenazas, la vigilancia, el análisis de imágenes de seguridad y el desarrollo de sistemas de seguridad cibernética.[6]

Entretenimiento: la IA se utiliza para generar música, crear contenido, desarrollar juegos, generar efectos especiales, y personalizar la experiencia del usuario en el entretenimiento.

Análisis de comportamiento del cliente: Utilización de la IA para comprender cómo los clientes interactúan con un sitio web o una aplicación, y optimizar la experiencia del usuario.

---

[4] Holmes, W., Bialik, M., Fadel, C. (2019). Inteligencia Artificial en la Educación. Boston: Centro para el Rediseño Curricular.

[5] Surden, H. (2014). Aprendizaje automático y derecho. Washington Law Review, 89, 87-115.

[6] Liu, Y., Xiang, Y., Sun, L., Zhang, J., & Mei, T. (2019). Comprender la reutilización efectiva de características profundas para el reconocimiento automático de imágenes artísticas de alimentos. Revista Internacional de Aprendizaje Automático y Cibernética, 10(8), 2021-2035.

Optimización de precios: Algoritmos que analizan datos del mercado y la competencia para determinar los precios óptimos para los productos.

Gestión de inventarios: Sistemas de IA que predicen la demanda de productos y optimizan los niveles de inventario para evitar faltantes o exceso de stock.

Educación: la IA permite crear sistemas de aprendizaje personalizado, automatizar la evaluación, generar contenido educativo, desarrollar plataformas de tutoría virtual y analizar datos educativos para mejorar las estrategias de enseñanza. Algunos ejemplos específicos incluyen:

Sistemas de aprendizaje personalizado: Plataformas de aprendizaje que adaptan el contenido y el ritmo de aprendizaje a las necesidades individuales de cada estudiante.

Evaluación automatizada: Utilización de la IA para evaluar tareas y exámenes de forma rápida y eficiente.

Creación de contenido educativo: Herramientas de IA que ayudan a generar contenido educativo como textos, videos o simulaciones.

Plataformas de tutoría virtual: Sistemas de IA que brindan tutoría personalizada a los estudiantes en diferentes áreas del conocimiento.

Manufactura: la IA se utiliza para optimizar los procesos de producción, automatizar el control de calidad, implementar el mantenimiento predictivo, gestionar la robótica industrial, y analizar datos de producción para mejorar la eficiencia y la productividad. Algunos ejemplos específicos incluyen:

Optimización de procesos: Utilización de la IA para identificar y eliminar cuellos de botella en los procesos de producción.

Control de calidad automatizado: Sistemas de IA que inspeccionan productos durante la producción para detectar defectos y garantizar la calidad.

Mantenimiento predictivo: Utilización de la IA para predecir cuándo es probable que falle un equipo y programar el mantenimiento preventivo.

Robótica industrial: Robots controlados por IA que realizan tareas repetitivas o peligrosas en la producción.

Transporte: la IA impulsa el desarrollo de vehículos autónomos, optimiza la gestión del tráfico, mejora la planificación de rutas, y optimiza la logística en la cadena de suministro.

4. MARCO REGULATORIO

La IA plantea nuevos retos para el marco jurídico, ya que no existen normas específicas que regulen su desarrollo y uso. Sin embargo, se están dando pasos para crear marcos regulatorios que aborden las diversas problemáticas que plantea la IA.

5. LA RESPONSABILIDAD CIVIL

La responsabilidad civil adquiere dos variables en el CCCN, la preventiva y la resarcitoria, en cuanto a la preventiva se configura como una herramienta hábil en cuanto a la previsibilidad de daños acaecidos en lugares donde la tecnológica fue implementada y provocó menoscabos

a) La antijuridicidad

El art. 1717 del CCCN incorpora un cimero paradigma, pues admite la protección de intereses simples, que no se encuentran registrados expresamente en la ley, pero que constituyen justas expectativas del hombre medio sobre el ordenamiento jurídico, las cuales, si resultan a su vez respetables y serias, deben ser atendibles y consideradas por el judicante en el caso concreto, siempre que no contraríen el orden público.

La protección de ese tipo de intereses cambia de enclave la partitura originaria escrita por el derogado Código, pues se genera una nueva concepción del derecho de daños, siendo la nota tipificante que decide la resarcibilidad del daño su carácter de injusto.

Entonces el daño es injusto en la medida que derive de la lesión de intereses merecedores de tutela jurídica, que son todos aquellos que la sociedad y los valores comúnmente aceptados muestran como dignos y respetables, aunque no tengan cabida en las normas. Lo jurídico no se agota en lo legal, la injusticia del daño no supone reconocimiento normativo del interés lesionado. En base a este razonamiento, cualquier interés de una

persona siempre que sea serio y digno se hará acreedor a la tutela jurídica, pues será injusto lesionarlo.[7]

El daño injusto no presupone un deber legal preestablecido, sino que lo antijurídico surge de cotejar el ordenamiento jurídico entendido en su totalidad (especialmente tratados internacionales y Constitución Nacional), para determinar si existe un interés que puede verse afectado en el caso concreto, el cual en la medida que merezca tutela jurídica por su razonabilidad deberá ser indemnizado.[8]

En los daños producidos por IA, la antijuridicidad se analiza producido el daño, si el mismo es "injusto" por lesionar intereses merecedores de tutela jurídica, también es antijurídico.

b) El factor de atribución

En cuanto al factor de atribución, la CSJN en el caso RODRIGUEZ c/ GOOGLE dijo que era subjetivo, y sería de aplicación al caso, no obstatne nos resistimos a sostener esta posición y creemos que el mismo es objetivo, pues la aplicación de la IA no deja de ser un factor de riesgo incorporado a la sociedad (art. 1757 del CCCN)

c) La relación causal

La conexión causal apunta al enlace material entre un hecho antecedente y un hecho consecuente y supone establecer el ligamen existente entre un acto y sus consecuencias. Se trata de un elemento autónomo del supuesto de hecho que genera la responsabilidad que está llamado a aprehender jurídicamente el encadenamiento que existe entre una situación antecedente (acción u omisión), y su resultado: el daño.[9]

---

[7] ZAVALA DE GONZALEZ, Matilde. Resarcimiento de daños. Tomo IV. Ed. Hammurabi. Pág. 124. JALIL, Julián Emil. Derecho de Daños Aplicado. Ed. Grupo Ibañez. Bogotá. 2013. Como asimismo: JALIL, Julián Emil. Tratado de la Responsabilidad Civil. Ed. El Zahir. Buenos Aires. 2012.

[8] Ver: JALIL, Julián Emil, "Daño moral derivado de la disolución del matrimonio o de las uniones convivenciales en el Código Civil y Comercial. A propósito de las conclusiones de las Jornadas Nacionales de Derecho Civil de Bahía Blanca, 2015", DFyP 2016 (mayo), 16, AR/DOC/1126/2016.

[9] GOLDEMBERG, Isidoro, La Relación de Causalidad en la Responsabilidad Civil, La Ley, Buenos Aires, 2000, 2da ed., ampl. y con actualización Jurisprudencial,

En esta materia existe una relación de causalidad presumida basada en los resultados certeros que debe producir la aplicación de la IA empleada en sus diferentes facetas. Es decir, el resultado esperado no es aleatorio, sino claramente determinado, cualquier modificación en ese destino hace presumir la causalidad.

d) El daño

En cuanto al daño no hay mayores cuestionamientos solo que deber ser probado por quien lo alega (art. 1744 del CCCN), y que se debe determinar su autoría, en este marco entendemos que pueden ser responsables: el titular del domino de la cosa a la que se aplica la IA, quien la usa, o quien percibe un beneficio o provecho. [10]

pág.39/40. SAMMARTINO, Patricio M. E., "La relación de causalidad en la responsabilidad del Estado", en AA.VV., Cuestiones de responsabilidad del Estado y del Funcionario Público, RAP, Buenos Aires, 2008, pág. 437.

[10] Ver: JALIL, Julián Emil, Resarcimiento de daños. Ed. Hammurabi. Tomo I. 2023. JALIL, Julián Emil. Indemnizaciones derivadas de daños y perjuicios. Ed. Hammurabi. Buenos Aires. 2020

PRINCIPIOS Y VALORES EN LA RESPONSABILIDAD POR DAÑOS DERIVADOS DE LA IA

Por Nicolás J. Negri[1]

I. CONCLUSIONES

1. La responsabilidad civil de la IA es un tema complejo (como la autonomía y la opacidad), que se halla en constante evolución y expansión, lo cual requiere de suma prudencia en su regulación e interpretación jurídica, para garantizar un desarrollo y uso responsable de la IA que proteja los derechos de los hombres.

2. El principio de no dañar a otro debe ser ponderado, en sus funciones preventivas y resarcitorias, en el uso y/o aplicaciones prácticas de bienes o servicios con IA.

3. El principio de no dañar a otro deber ponderado con otros principios jurídicos, en especial, el principio *pro homine*, junto con otros más especiales como: el principio de precaución, transparencia, no discriminación, privacidad y seguridad.

4. Por el momento, no considero conveniente la aplicación de los presupuestos tradicionales de la responsabilidad civil: antijuridicidad, factores de atribución, relación de causalidad adecuada y daño resarcible (arts. 1716 y ss., CCCN).

El grado de evolución tecnológica y los continuos cambios, llaman a la prudencia en la aplicación de los factores subjetivos y objetivos de atribución de responsabilidad civil.

Lo mismo en orden a la determinación de la relación causal, según el criterio brindado por la doctrina de la "relación causal adecuada", receptada por nuestro ordenamiento jurídico.

---

[1] Doctor en Ciencias Jurídicas (UNLP). Profesor Titular de Derecho de las Obligaciones (UCALP). Profesor Adjunto (UNLP). Profesor Adjunto (UNLP). Profesor Titular de Derecho Civil Parte General (UP). Juez de 1ª Instancia en lo Civil y Comercial (Pcia. de Bs. As., La Plata).

EL DERECHO DE DAÑOS FRENTE A LA INCORPORACIÓN DE IA EN EL SERVICIO DE SALUD (RECONOCER EL CAMBIO IMPLICA REVISAR LA NORMA)

Por Gabriela A. Nucciarone[1]

I. CONCLUSIONES

1. La responsabilidad por los daños que se generen en el sistema sanitario a los usuarios del mismo debe ser regulada en el Código Civil y Comercial de la Nación en un apartado especial y especifico.

2. La utilización de la IA en la prestación del servicio de salud, en determinados supuestos implica considerar que el factor de atribución aplicable es el objetivo.

3. Es insuficiente lo regulado por el art. 1768 del CCCN -in fine- para reparar los daños generados en la atención médica por el uso de la IA, pues no solo podrían ser consecuencia de un defecto o vicio de diseño/fabricación sino generarse por la propia y común contingencia de errar de la IA.

4. Sin perjuicio de que subsista el factor de atribución subjetivo para determinados supuestos de mala praxis médica, las modificaciones que se identifican en la forma de prestar el servicio de salud dan cuenta que el mismo queda reducido a la excepción y no a la regla.

5. La aplicación del factor de atribución objetivo, entre otras cuestiones, implica dejar de poner el foco en la conducta del sujeto "dañador", descomprimiendo a los profesionales en ejercicio de su profesión.

6. A mayores beneficios generalmente aumentan los riesgos, ergo es necesario considerar, al factor de atribución objetivo desde una valoración riesgo creado/riesgo provecho, en los supuestos de intervención de la IA en la prestación del servicio de salud.

---

[1] Abogada (Universidad de Buenos Aires). Especialista en Contratos y Derecho de Daños (USAL). Profesora adjunta regular por concurso de Contratos Civiles y Comerciales Facultad de Derecho UBA. Coordinadora del Programa para la Protección de Usuarios y Consumidores de la Procuración General de la Nación.

7. Se requiere incorporar al sistema normativo la obligatoriedad del seguro médico. La cobertura debe abarcar específicamente los daños generados por la utilización de la IA.

8. El seguro médico obligatorio, implicaría entre otras cuestiones, dar un marco de mayor seguridad en el ejercicio de la profesión, evitando lo que se ha denominado el ejercicio de la medicina defensiva.

9. El contexto y la forma en que se presta el servicio de salud, se modificó exponencialmente en los últimos veinte años. Ello requiere una revisión del actual régimen de responsabilidad civil en los supuestos de mala praxis médica.

10. Los cambios más relevantes se dieron en la modalidad relacional médico/ paciente; la forma de organización del sistema/prestadores/laboratorios; el aumento de la edad promedio de esperanza de vida; incorporación de tecnología, robótica e IA; incremento de datos, entre otros.

11. La incorporación de IA al sistema sanitario aporta beneficios distintivos en aspectos económicos (reducción de costos para las entidades públicas y privadas), organizacionales, preventivos, medicina de precisión, diagnóstico y seguimiento de patología crónicas, entre otros.

12. Frente a los cambios sustanciales en la prestación del servicio de salud, se requiere de nueva reglamentación y modificación de las normas que regulan el actual sistema de responsabilidad médica para una mayor seguridad jurídica.

13. El marco regulatorio debe alinear la estructura de incentivos de los distintos participantes del sistema para facilitar el desarrollo, financiación, prevención, con especial respeto a los derechos personalísimos.

14. El derecho debe considerar que según vaya avanzando y cambiando la sociedad y la IA surgirán nuevos derechos susceptibles de protección.

II. FUNDAMENTOS

1. SORDO, CIEGO Y MUDO ¿QUÉ NOS OBLIGA A REVISAR EL ACTUAL REGIMEN DE RESPONSABILIDAD CIVIL APLICABLE A LOS DAÑOS GENERADOS EN LA PRESTACIÓN DEL SERVICIO DE SALUD?

Apelando a la brevedad expositiva que nos demanda la propuesta en análisis, debemos decir que cuando nos representamos la asistencia sanitaria no podemos describirla solamente en un escenario con la presencia de un/a profesional de la medicina en soledad frente al paciente. Por el contrario, el despliegue que se activa es dentro de un sistema, donde converge estructura edilicia, tecnológica, farmacológica, laboratorios, personal administrativo, de higiene, especialidades, robótica, inteligencia artificial, aplicaciones, profesionales medicas/os, pacientes, empresas. Es por ello que comenzamos por aclarar por qué hacemos foco en el "sistema sanitario" y no en la individualidad o singularidad del profesional médico.

Aun cuando la intención de este aporte se reduzca a la incidencia de la IA en la prestación del servicio médico, lo cierto es que el contexto en el que se desarrolla tal actividad, debe ser considerado para valorar el régimen de responsabilidad civil aplicable.

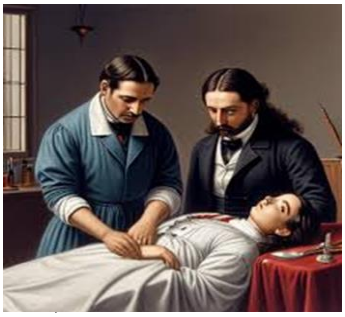
En las últimas dos décadas la evolución y transformación que sufrió el servicio asistencial de la salud, fueron y siguen siendo de tal magnitud que no pueden ser desoídos por el derecho.

No es una novedad, pero vale la pena recordar que el progreso de la nanotecnología nos revela que la ciencia avanza más rápido que el Derecho. Pero también nos permitimos afirmar que muchas veces aún frente a la obviedad del cambio y la obsolescencia de la norma, la comunidad jurídica -y en particular el legislador- se mantiene inerte y prefiere continuar con lo conocido.

Ahora bien, si creemos que desde mitad del siglo XX el centro de tutela normativa es la persona humana, entonces ese es el objetivo jurisdiccional a alcanzar.

Algunos de los hechos que pueden individualizarse como relevantes para forjar esa transformación en el sistema sanitario, tiene estrecha vinculación con: el aumento exponencial de la esperanza de vida y el correlativo crecimiento de la población adulta mayor; el cambio de paradigma en la relación médico paciente, migrando de una relación paternalista a una de autodeterminación; los avances económicos empresariales en la actividad; la convivencia de diversos sistemas, público, mixtos y privados, la incorporación de tecnología, robótica e inteligencia artificial -en adelante IA-

Para ilústralo nos parecen ejemplificativas estas imágenes:



Excepcionalmente nos encontraremos frente a un profesional médico que realice un diagnóstico y proponga un tratamiento sin verse influenciado por el contexto laboral, sin valerse de análisis, estudios de precisión, interconsultas con otros/as colegas especialista, o bien por un diagnóstico producido por la IA.

Veamos entonces algunos fundamentos en los que se enmarca la presente propuesta.

2. LOS AVANCES DISTINTIVOS DE LA INCORPORACIÓN DE LA IA AL SISTEMA SANITARIO

Seguramente cuando el lector avance sobre estos párrafos, estos ejemplos de utilización de IA en la prestación del servicio de salud, ya hayan sido superados, ampliados o modificados. Hecha esa advertencia reflejamos algunos supuestos concretos de la utilización de la IA.

Si bien no existe una definición consolidada de la IA, hay un consenso en que se trata de emular la inteligencia humana en sistemas informáticos.[2] Se la conceptualizó, con meridiana simpleza como aquella que consiste en hacer predicciones futuras basándose en datos, *muchos datos*, del pasado. Esas predicciones las realizan algoritmos que tienen la capacidad de aprender de patrones que se encuentran en los datos. Por eso se afirma que sin datos no existe la IA y de ahí que se los considere el petróleo de nuestra era.[3]

---

[2] SANTARELLI, Fulvio G. "La Madeja de la Inteligencia Artificial. En Busca de la Punta del Hilo" LA LEY 16/09/2022, 1 E, 345

[3] DANESI, Cecilia., *El imperio de los algoritmos* 1ra edición, Galerna editorial, Ciudad Autonoma de Buenos Aires, 2022 p. 40

En la sanidad se utiliza para el campo del diagnóstico o bio marcadores de ciertas enfermedades. En esta área, de la salud, la IA fue pionera debido a su aptitud para "predecir el futuro" se la considera una gran aliada para pronosticar enfermedades como así también para la primera atención médica.[4]

Solo mencionaremos algunos ejemplos para brindar un panorama, aunque parcial y reducido, de la implementación de la IA en la prestación del servicio de salud. Comenzamos por destacar el provisto por empresas argentinas que desarrollaron IA para la atención primaria o diagnóstico por imágenes con los sistemas "Entelai Doc" y "Etelai Pic". En el primer supuesto se utiliza para la atención primaria y de acompañamiento del paciente, y el segundo es un software para el análisis de imágenes médicas que asiste a los actores del sistema de salud en cuatro tipos de estudios: demielinizantes, volumetría, mamografía y tórax.[5]

Otro caso es el de la empresa "Teckel Medical", que dedicada a desarrollar software médico mediante IA creó la aplicación "Mediktor", "el primer evaluador de síntomas avanzado del mundo, capaz de reconocer lenguaje natural para que el usuario exprese cómo se siente con sus palabras".[6]

Mediante otro proyecto llamado "DeepMind", -propiedad de Google Alphabet Inc. desde 2014- se realizan diagnósticos de enfermedades oculares tan o incluso más efectivos que los desarrollados por los humanos, o la propuesta de un protocolo digital para el tratado y cuidado de lesiones renales agudas en los ingresos hospitalarios de emergencias[7].

---

[4] Idem p. 46

[5] Idem p. 47. La autora, Danesi, explica y remite donde podrán ampliar sobre el desarrollo y tipos de reporte que realizan los softwares mencionados.

[6] SERRANO GUTIÉRREZ, Laura, "Ética e Inteligencia Artificial en le ámbito de la Medicina" abril 2021, Ed Comillas Universidad Pontificia Madrid citando a "Barzallo Cueva, S., & Barzallo Cabrera, P. (Diciembre de 2019). La Inteligencia Artificial en Medicina. *Revista Médica Ateneo, 21*(2), 81.

[7] SERRANO GUTIÉRREZ, Laura, "Ética e Inteligencia Artificial en le ámbito de la Medicina" abril 2021, Ed Comillas Universidad Pontificia Madrid citando a Connell, A., Montgomery, H., Martin, P., Nightingale, C., Sadeghi-Alavijeh, O., King, D., Emerson. (2019). Evaluation of a digitally-enabled care pathway for acute kidney injury management in hospital emergency admissions. *Nature Partner Journal, 2*(67).

Recientemente se difundieron dos proyectos argentinos para diseñar soluciones que mejoren la atención del sector público. Estos proyectos surgieron en el marco de una convocatoria internacional para dar con aplicaciones basadas en investigación responsable mientras surgen a diario nuevos potenciales o se comunican buenos resultados en tareas que van desde la gestión de turnos, urgencias, insumos hasta la asistencia a especialistas en el análisis de imágenes u otras pruebas diagnósticas.[8]

En otra área de la medicina que es muy relevante la incidencia de la IA es en la identificación de embriones en una instancia preimplantacional.[9]

A esta altura sabemos que la IA puede facilitar el diagnóstico de enfermedades como cánceres de cuello uterino o mama y endometriosis a través de diagnóstico por imágenes y uso de algoritmos; asistir a personas embarazadas en el seguimiento, el parto y el posparto y brindar información. Al contar con un sistema que almacena la información, los trabajadores sanitarios y prestadores de servicios médicos en general, pueden acceder a los mismos para tomar decisiones teniendo en cuenta las características de los pacientes y sus necesidades.

A partir, entonces, del magnífico y potencial desarrollo de la IA en la prevención, diagnóstico y tratamientos médicos se abren una serie de interrogantes que van desde cuestiones éticas, prácticas y también de responsabilidad frente al acaecimiento del daño.

Sólo a modo de inquietud, entre tantos interrogantes en torno al derecho a la igualdad, acceso al servicio, nos preguntamos ¿las instituciones que no cuenten con sistemas de IA podrán ser demandadas por deficiencia en la prestación del servicio? ¿El sistema se encuentra preparado para asegurar el acceso inmediato y adecuado al tratamiento que surja a partir de la utilización de la IA?

---

[8] CZUBAJ, Fabiola "A fin de año va a ser otra realidad" Dos proyectos argentinos en la carrera contra el tiempo para incorporar la IA en salud., Diario la Nación 3 de agosto de 2024. https://www.lanacion.com.ar/sociedad/a-fin-de-ano-va-a-ser-otra-realidad-dos-proyectos-argentinos-en-la-carrera-contra-el-tiempo-para-nid03082024/

[9] TAGLIANI, María Soledad, Responsabilidad médica derivada de las técnicas de reproducción humana asistida a partir del nacimietno y la muerte de un hijo afectado con fibrosis quística. La Ley 29/12/2020 RCYS2021-II, 66

La transversalidad del tema nos compele a abordarlo desde sus distintos vértices y en conjunto con diversas disciplinas. No obstante, de momento resulta evidente que la aplicación de IA en el sistema sanitario aporta beneficios e implica riesgos que los operadores jurídicos debemos comenzar a analizar.

3. ¿QUIÉN DEBE ABSORBER LOS RIESGOS QUE IMPLICA LA UTILIZACIÓN DE LA TECNOLOGÍA, EN ESPECIAL DE LA IA?

Frente a la implementación de la IA en el sistema sanitario, queremos avanzar sobre la inquietud que venimos teniendo desde hace un tiempo atrás relativa a las respuestas que debería brindar el derecho, por los daños que se puedan experimentar por la utilización de la IA en los supuestos mencionados.

Sabemos que es un gran desafío contar con normas que estén a la altura de transformaciones sociales, económicas y tecnológicas constantes.[10]

Por otra parte, el andamiaje normativo se construye a partir de los cimientos preexistentes y nos parece necesario afrontar ese desafío aún con temor a equivocarnos, porque creemos que es la única forma de avanzar, crecer y mejorar.

A esta altura sabemos que no podemos paralizarnos, por más que tengamos sensaciones encontradas sobre el avance tecnológico en tanto es un hecho que no se detiene ni mucho menos espera que los legisladores dicten normas, reglamentos para seguir desarrollándose.[11]

---

[10] TARELLO, Giovanni "La interpretación de la Ley" 2da edición. Palestra Editores S.A.C. Perú febrero 2018. Pag. 297 "Las leyes interpretativas han suscitado en el pasado, y suscitan hoy, muchos problemas, muy debatidos en doctrina y cuyas soluciones son de gran relevancia práctica. Problemas en orden: a) a su naturaleza; b) a su legitimidad y a le extensión de su legitimidad; c) a su eficacia; d) a su interpretación y a los poderes que los órganos de aplicación tienen en el atribuirá ellas un significado; e) a su oportunidad"

[11] GALVÍN GORDILLO, Marina en "Análisis legal del uso de los robots en la medicina" de junio de 2023 IUS ET SCIENTIA • 2023 Vol. 9 • Nº 1 • pp. 129-151 explica que el carácter positivo o negativo de la tecno ciencia depende del destino que se le da (teoría de la neutralidad valorativa, Oliver.L, 2021) siendo por tanto imposible garantizar la total seguridad, pero la existencia de posibles riesgos imprevisibles no pueden provocar la parálisis de la investigación científica que ha logrado y está logrando importantes beneficios para la humanidad.

Existe suficiente evidencia que el uso de las máquinas dotadas con IA, representan beneficios de apoyo al sector de la salud, pero la pregunta que nos formulamos al inicio es ¿quién debe asumir el costo de las reparaciones de los daños por la introducción de esta tecnología?, bien sea porque su defectuoso funcionamiento haya sido consecuencia del obrar culposo humano en su diseño, programación, operación y/o mantenimiento, o bien porque simplemente al margen de lo anterior, suele presentarse la contingencia propia y común de fallar de toda máquina, y que constituye el riesgo intrínseco de su funcionamiento.

Cuando se plantea el resultado dañoso o lesivo para el paciente como consecuencia o a razón de la utilización de la IA nos parece adecuado que el sistema le permita una reparación integral ágil y que no sea él quien absorba tales riesgos. Por ello un sistema basado en el factor de atribución subjetivo, surge a priori inadecuado.

4. EL SISTEMA DE RESPONSABILIDAD CIVIL ACTUAL

Por algunas razones, quizás afianzadas en el academicismo conservador, intereses corporativos u otras, que difícilmente puedan explicase en estas breves líneas, no existe en el código civil y comercial un apartado específico que regule la mala praxis médica y la reparación de daños generados por el sistema sanitario.

Si bien es conteste la doctrina sobre el avance que significó incorporar al ordenamiento de fondo el art. 1768 del CCCN, para los supuestos de mala praxis en general, a nuestro entender la complejidad del sistema sanitario, el volumen de casos y la especificidad de cada uno, donde pueden converger en el paciente daños que trae por su patología con posibles daños generados en el ecosistema sanitario, requerirían de regulación específica. Y si a ello le sumamos la incorporación de IA en la prestación del servicio, creemos que no debería existir resistencia a pensar en un apartado especial para dar tratamiento a la temática planteada.

El punto de partida, esos cimientos a los que nos referíamos, es el esquema actual. Repasemos entonces el contenido del art. 1768 “La actividad del profesional liberal está sujeta a las reglas de las obligaciones de hacer. La responsabilidad es subjetiva, excepto que se haya comprometido un resultado concreto. Cuando la obligación de hacer se preste con cosas, la responsabilidad no está comprendida en la Sección 7ª, de este Capítulo, excepto que causen un daño derivado de su vicio. La

actividad del profesional liberal no está comprendida en la responsabilidad por actividades."

Bajo este esquema y respecto de los daños generados por la utilización de la IA en la asistencia sanitaria y en particular en la prestación médica, podríamos decir que, si la maquinaria que utiliza IA tiene un vicio o defecto de fabricación, el factor de atribución aplicable es el objetivo.

Ahora bien, para nosotros, como ya adelantamos esta normativa es insuficiente y obsoleta frente al actual contexto.

Creemos que aun cuando el daño no sea producto del vicio de la IA pero el resultado dañoso sea causado por la utilización de la misma, estamos frente a una cosa riesgosa (aún en distintos grados). Valorando además la figura del riesgo creado o riesgo provecho.

En el derecho comparado encontramos un avance sobre la regulación, protocolos o reglamentación que resumidamente vamos a contar en los próximos párrafos, pero antes nos permitimos una nueva "reserva" u "aclaración". Así como nos referimos a la importancia sustancial que tiene el contexto donde se despliega el ecosistema sanitario, con ese mismo criterio debemos saber que no es lo mismo lo que sucede en Europa o Estados Unidos tanto a nivel, económico, social, cultura y por supuesto del avance tecnológico que en nuestra región. Ergo, no debemos cometer el error de "importar" normativa que fue pensada y aplicada en un escenario diverso. Ello no quita que sea un disparador que nos enriquezca para pensar nuestro derecho interno y/o regional.

Citamos algunas de estas referencias:

En el 2017 la Unión Europea aprobó la Resolución del Parlamento Europeo (PE) con recomendaciones a la Comisión Europea (CE) sobre normas de Derecho civil sobre robótica[12]. En 2020, se publicó el Libro Blanco[13] que propone tres componentes que deben ser acumulativos en sistemas de IA: a) lícita, que cumpla con la ley relacionada con la responsabilidad médica y que asegure una compensación justa cuando se

12 Confr. DÍEZ ROYO, Mario, "Cuestiones de responsabilidad civil de los sistemas de Inteligencia Artificial en las Propuestas de Directivas europeas de 28 de septiembre de 2022", Revista de Estudios Jurídicos y Criminológicos, n.º 8, Universidad de Cádiz, 2023, pp. 253-276, DOI: https://doi. org/10.25267/REJUCRIM.2023.i8.09.

13 Libro Blanco, COM (2020) 65 final, Bruselas, 19 de febrero de 2020, se puede consultar en la URL https://eur-lex.europa.eu

produzca un efecto adverso, b) ética, que garantice el respeto a los principios y valores, y c) robusta, basada en la supervisión humana y gestión de la privacidad de los datos y la no discriminación; por consiguiente no podemos olvidar los principios y valores más importantes relacionados con la asistencia sanitaria y la IA.

A ello debemos agregarle el Informe de la CE al PE, al Consejo, y al Comité Económico y Social Europeo sobre seguridad y responsabilidad civil de la IA, el internet de las cosas (IoT) y la robótica.[14]

Más recientemente -en el año 2023- se aprobó el Reglamento de Inteligencia Artificial (IA) cuyo texto se acordó a fines de 2023 y ha sido aprobado por el PE en 2024.[15] Entre sus ejes centrales existe una distinción de escala de riesgos de la IA y otro sobre manipulación de datos. Dependiendo del grado de riesgos, se va de un factor objetivo con especial énfasis en el aporte probatorio a uno subjetivo.

5. REDONDEAMOS, AUNQUE SABEMOS QUE HAY MUCHO MAS QUE PENSAR Y DEBATIR.

Frente a este escenario, nuestro propósito es poner en evidencia que existe una necesidad imperiosa de avanzar con un régimen de responsabilidad específica, en el ámbito de los daños que se produzcan en la prestación del servicio de salud, que se distinga del resto de las responsabilidades profesionales.

Debemos añadir aquellas cuestiones relativas a la utilización de la IA en la prestación del servicio y la reparación de los daños que de ella se pueda derivar.

La tarea no es sencilla, pero requiere de un debate que no pierda de vista que, en la actualidad imperante, debemos bregar por la tutela de persona humana que enfrenta un mundo complejo y convive con otra inteligencia que no es la de su especie, es artificial.

14Confr.https://eurex.europa.eu/legalcontent/ES/TXT/PDF/?uri=CELEX:52020DC0064

15Confr.https://www.europarl.europa.eu/news/es/pressroom/20240308IPR19015/la-eurocamara-aprueba-una-ley-historica-para-regular-la-inteligencia-artificial

EL FACTOR DE ATRIBUCIÓN APLICABLE EN LOS DAÑOS DERIVADOS DEL USO DE INTELIGENCIA ARTIFICIAL POR LOS PROFESIONALES LIBERALES

Por María Agustina Otaola[1]

I. CONCLUSIONES

De lege lata

1. Corresponde descartar la aplicación del factor subjetivo de atribución en el ámbito de la responsabilidad por daños ocasionados a través del uso de inteligencia artificial (en adelante IA), ya que, si bien la culpa es el factor residual, no es posible realizar un test de culpabilidad cuando se trata de daños derivados del uso de IA.

2. En el caso de los profesionales liberales que hacen uso de la IA para ejercer sus funciones, corresponde apartarse de la regla general de factor subjetivo de atribución prevista en el CCyCN para la responsabilidad de los profesionales, aplicándose el factor objetivo de atribución cuando el profesional delega totalmente la función en una aplicación o herramienta de IA, sin ejercer el debido control.

3. La IA, en tanto herramienta potencialmente dañosa, reviste los caracteres de una cosa o actividad riesgosa, y por lo tanto el factor de atribución aplicable debe ser el factor objetivo, basado en el riesgo o vicio de la cosa.

De lege ferenda

4. Corresponde legislar de *lege ferenda* la responsabilidad civil de los profesionales liberales que hacen uso de la IA para ejercer sus funciones, con basamento en el factor objetivo de atribución, cuando el

---

[1] Abogada por la Universidad Nacional de Córdoba (UNC); Doctora en Derecho y Ciencias Sociales por la Universidad Nacional de Córdoba (UNC); Magister en Derecho y Argumentación Jurídica (UNC); Master en Derecho de los Negocios Internacionales por la Universidad Complutense de Madrid, Ex Becaria de Posgrado CONICET, Docente adjunta de la Universidad Católica de Santiago del Estero SEDE JUJUY; Socia- directora en Estudio Jurídico "Otaola y Asociados"; Directora provincial de energía de la Secretaría de Energía de la provincia de Jujuy.

daño ocasionado a un tercero tiene nexo adecuado de causalidad con el uso de IA.

II. FUNDAMENTOS

1. INTRODUCCIÓN

La presencia de la Inteligencia Artificial avanza e irrumpe en todos los ámbitos de la vida humana. Siendo que el derecho no es ni será ajeno a ello, se plantean numerosos interrogantes que tienen que ver con la interrelación entre la IA y el derecho: eficacia y falibilidad de los sistemas de IA para la resolución de casos jurídicos (qué temas o casos pueden resolverse o valerse de la IA); voluntad e información en los casos de contratación por medio de IA; derechos de autor; protección de datos personales; responsabilidad por daños derivados del uso de IA, entre otros.

Este trabajo versa sobre este último tópico, centrado en la responsabilidad civil del profesional liberal que se vale de la IA para el ejercicio de su profesión o función. Desde luego, el tema reviste interés a partir de que el uso de la IA resulte nexo adecuado de causa de un daño a un tercero, momento en el que cabe preguntarnos si el profesional puede atribuir una decisión o acción profesional que es señalada como "mala praxis" a una herramienta de IA. Asumiendo que no puede hacerlo, corresponde preguntarnos qué factor de atribución resulta aplicable, lo que tendrá incidencia en la carga de la prueba y los eximentes de responsabilidad aplicables al caso.

En términos generales, la inteligencia artificial puede definirse como un campo de la ciencia y la ingeniería que se ocupa de la comprensión, desde el punto de vista informático, de lo que se denomina comúnmente comportamiento inteligente. También se ocupa de la creación de artefactos que exhiben este comportamiento[2]. Es aplicable a cualquier ámbito de la actividad intelectual humana y su origen se remonta a una conferencia sobre informática teórica de 1956 en EEUU. Desde entonces, existen

[2] PINO DÍEZ, Raúl, GÓMEZ GÓMEZ, Alberto, ABAJO MARTÍNEZ, Nicolás, Introducción a la inteligencia artificial: sistemas expertos, redes neuronales artificiales t computación evolutiva, Universidad de Oviedo, servicio de publicaciones 2001, pp. 5-8.

innumerables desarrollos de IA que resultan de utilidad para los más impensados ámbitos de la vida humana.

La IA se encuentra presente en nuestra vida cotidiana, inadvertida y sigilosa, en servicios como Google, YouTube, Spotify, Facebook, Netflix. Empresas, profesionales, y personas físicas en general hacen uso de las herramientas predictivas que funcionan mediante IA para ejecutar tareas especializadas, creativas, entre otras.

No caben dudas que la IA seguirá transformando nuestras vidas, adoptando formas más evolucionadas que a su vez traerán aparejada nuevas formas de dañosidad; lo que nos presenta grandes desafíos, ya que la IA involucra numerosos interesados y componentes, tales como hardware, software, manipulación de datos, lo que dificulta distribuir la responsabilidad entre todos los intervinientes. Asimismo, novedosos sistemas de IA son capaces de aprender sin dirección o supervisión humana y de tomar decisiones autónomas, lo que representa un enorme reto a la hora de regular las responsabilidades derivadas del uso de la IA.

Ante el vacío legal generado por estas nuevas tecnologías, será necesario legislar la responsabilidad por los daños ocasionados por el uso de IA por parte de profesionales liberales.

A grandes rasgos, acudiendo a los principios generales de la responsabilidad civil, son dos las posibilidades: endilgar responsabilidad en base a un factor subjetivo u objetivo de atribución.

El *quid* de la cuestión, estará en determinar si el daño causado por una IA puede ser atribuido a título de culpa a alguien o si se trata de un supuesto de responsabilidad objetiva o qué regulación jurídica le corresponderá; ya que una vez definido esto, resultarán de aplicación los principios generales de la responsabilidad civil para cada tipo de atribución.

Dada la amplitud del tema, me centraré a aquellos supuestos en los que un profesional liberal se vale de uso de IA como herramienta para optimizar sus funciones, tema que a su vez nos plantea una primera dificultad: la responsabilidad de los profesionales ya cuenta con una regulación específica en nuestro ordenamiento civil y comercial, que no parece adecuada para responder a los nuevos escenarios que se presentan con el uso creciente de la IA.

2. PROFESIONALES DEL DERECHO Y EL USO DE LA IA

La Inteligencia artificial aplicada al derecho comprende la automatización del razonamiento jurídico y de la solución de problemas jurídicos.

Este específico uso de la IA nos plantea un primer interrogante, referido a la ética sobre el uso de la IA entre operadores jurídicos, tema que no será abordado en el presente, el que se centra en la atribución de responsabilidad por daños derivados del uso de IA.

Un profesional del derecho o un funcionario de la justicia podrán valerse de la IA para la ejecución de sus tareas; a modo de ejemplo, en el primer caso, para elaborar una demanda; en el segundo supuesto, para redactar una sentencia. Como anticipé, el primer escollo está en determinar si el uso de dicha herramienta se condice con los códigos de ética aplicables a la profesión, tema que debe ser objeto de otro estudio específico.

El segundo interrogante tiene que ver con lo antes planteado: cuál será el elemento axiológico que permita atribuir responsabilidad, por ejemplo, al abogado litigante o al funcionario judicial que se valga de IA para el ejercicio de su profesión en el primer caso, y de su función en el segundo supuesto.

El uso de IA no es ajeno al ejercicio de las distintas profesiones liberales, y los profesionales del derecho no son ni serán la excepción. Distintas aplicaciones se han desarrollado y seguirán ideándose que permitan dar respuesta automática a consultas jurídicas, redacción de cartas documentos, redacción de demandas, contestaciones, e incluso sentencias. Como premisa, debemos considerar que, hasta la fecha, ningún sistema de IA ha demostrado infalibilidad para dar respuesta en el ámbito jurídico.

Si tomamos los modelos basados en la lógica computacional clásica, en los años 80 se vieron los primeros trabajos de automatización en lo que se refiere a la representación lógica de las disposiciones legales. Expone Navas Navarro: "*se pensaba entonces que la IA tendría un gran impacto en el ámbito jurídico, pero no sucedió así, más bien lo contrario. La razón de ello venía principalmente del hecho de que el razonamiento basado en la lógica no era capaz de representar de forma adecuada las reglas legales, en la medida en que estas pueden admitir diferentes interpretaciones, presentan ambigüedades, se redactan como cláusulas de carácter general, se emplean conceptos jurídicos indeterminados o pueden existir proposiciones jurídicas contradictorias y el razonamiento basado en la lógica se centra en afirmaciones de verdadero o falso sin apenas admitir*

matices"[3]. Lo mismo ocurre con los sistemas basados en la automatización, que pueden resultar de utilidad para algunas cuestiones, mas no sustituyen la labor del profesional.

Quien se vale de IA sin dudas obtiene un beneficio de ello: optimización de tiempo de trabajo, ahorro en mano de obra, difusión y publicidad a gran escala, entre otras. En esta primera manifestación de voluntad del profesional que se vale del uso de una herramienta automatizada, subyace un elemento volitivo que tiene que ver con la decisión de ejercer su función o profesión a través de IA. El móvil de dicha decisión será la mayoría de las veces optimizar tiempo de trabajo, ahorrando esfuerzo investigativo e interpretativo, como así también de escritura. Si pensamos específicamente en la labor de un profesional del derecho, la misma implica la elaboración de extensos documentos (demandas, contestaciones de demandas, contestación de traslados, alegatos escritos, sentencias, entre otros). Dando por asumido que es moral y permitido el uso de IA, resta por evaluar si el profesional puede confiarse en la respuesta otorgada por una aplicación de IA, y una vez que ello ocasione un planteo de mala praxis, eludir su responsabilidad invocando el uso de dicha herramienta. Se impone la respuesta negativa, y ello nos lleva ineludiblemente a replantearnos las bases del actual sistema de responsabilidad contenido en el CCyCN para el supuesto de los profesionales liberales.

La respuesta, al no encontrarse una legislación específica, dependerá del uso de herramientas interpretativas disponibles, a la luz del ordenamiento jurídico integralmente considerado.

En el específico supuesto de los profesionales del derecho que se valen de la IA para el ejercicio de su profesión, superado (o no) el escollo moral, habrá que replantearse las reglas generales de la responsabilidad civil. Pero como anticipé, debemos asumir como premisa la falibilidad de los distintos sistemas desarrollados hasta la fecha. Supongamos un amparo de salud, donde se plantea una cuestión en la que la vida de una persona dependa de una autorización judicial que deba resolverse en cuestión de días u horas. Consideremos que ninguna herramienta de IA es capaz de detectar la urgencia y especificidad planteada; y que el funcionario a cargo se vale

[3] NAVAS NAVARRO, Susana, Inteligencia artificial. Tecnología Derecho. Tirant lo Blanch, Valencia 2017, p. 28.

de determinada aplicación computarizada para redactar un primer proveído cuando ingresa a su ámbito de conocimiento una demanda categorizada como "amparo de salud". Me encuentro en condiciones de afirmar que cualquier aplicación o herramienta de IA hoy es incapaz de detectar semejante urgencia, a la vez que damos por sentado que adolece de "sensibilidad humana". Entones, ¿quién debe responder ante la falta de una respuesta judicial expedita, tal como lo ameritaba el caso en cuestión?. No parece lógico indagar qué persona, sociedad o ente ideó dicha aplicación falible. Existe un funcionario o profesional que optó por hacer uso de esa herramienta y obtuvo un "provecho" de ella, o al menos tuvo en miras dicho provecho[4].

3. MOTIVOS PARA AOPYAR LA RESPONSABILIDAD OBJETIVA DEL PROFESIONAL LIBERAL QUE OCASIONA UN DAÑO CON IA

En el contexto vigente, la índole del problema es el creciente número de tecnologías de IA que causan daños, sea a la persona, a la sociedad o a las cosas, sin que una persona humana pueda ser reputada como responsable, dada la naturaleza imprevisible de estos entes[5]. Es por eso que este trabajo se centra en un uso específico, referido al uso de la IA como herramienta para facilitar la labor de los profesionales liberales.

La actual regulación, basada en el factor subjetivo de atribución no parece adecuada para dar una respuesta ante el supuesto planteado. El artículo 1768 del CCyCN regula específicamente la responsabilidad de los profesionales liberales, estableciendo que la actividad del profesional liberal está sujeta a las reglas de las obligaciones de hacer, aclarando enfáticamente

---

[4] De la experiencia habida hasta la fecha, se conoce un caso en Estados Unidos de un profesional que hizo uso de IA sin controlar ni verificar el contenido. El Comité de Quejas del Tribunal de la Florida concluyó que el abogado "*no había ejercido la debida diligencia razonable requerida y su conducta iba más allá de una falta de debida diligencia, ya que algunos precedentes que invocaba eran completamente inventados*".

En el informe presentado, se expuso que "*si bien entendemos que la inteligencia artificial se está convirtiendo en una nueva herramienta para la investigación jurídica, nunca podrá reemplazar la responsabilidad de un abogado de cumplir con su deber de diligencia razonable de proporcionar al tribunal unos precedentes precisos que respalden un argumento legal válido*".

[5] YOSHIKAWA, Jin, "Sharing the Costs of Artificial Intelligence: Universal No-Fault Social Insurance for Personal Injuries", Vanderbilt Journal of Entertainment and Technology Law, vol. 21, n. 4, 2019, p. 1155 (consultado el 29/06/2024).

que la responsabilidad es subjetiva, excepto que se haya comprometido un resultado concreto.

A su vez, en el específico tópico de estudio, se establece: *"Cuando la obligación de hacer se preste con cosas, la responsabilidad no está comprendida en la Sección 7a, de este Capítulo, excepto que causen un daño derivado de su vicio. La actividad del profesional liberal no está comprendida en la responsabilidad por actividades riesgosas previstas en el artículo 1757".*

La realidad cambiante nos impone replantear la letra del código, cuando un profesional liberal se vale totalmente de herramientas de IA para el cometido de sus funciones.

Es por ello que, ante un supuesto de mala praxis, acreditado que el profesional se valió del uso de IA suplantando totalmente su accionar profesional por una herramienta artificial, corresponde endilgarle responsabilidad en base a un factor objetivo de atribución, con las consecuencias en la carga de la prueba y eximentes que ello implica. Tal como lo define el artículo 1722 del CCyCN, el factor de atribución es objetivo cuando la culpa del agente es irrelevante a los efectos de atribuir responsabilidad.

Cuando estando vigente el Código de Vélez Sarsfield, se presentó una realidad en la que desbordaron los supuestos de daños ocasionados con cosas o actividades riesgosas, hubo que replantearse el sistema de responsabilidad basado en la culpa. Entonces, proliferaron los supuestos de daños basados en un factor objetivo de atribución que permitió dar respuesta al nuevo escenario. Hasta ese momento, se plantearon ficciones de culpa (culpa *in eligendo*, culpa *in educando*, entre otras), ya que parecía impensable atribuir responsabilidad sin un elemento volitivo reprochable en el agente. La solución se abrió camino a través de replantearse el artículo 1113 de dicho Código Civil, que receptó la responsabilidad objetiva.

El camino recorrido parce válido ahora, cuando pensamos en los daños ocasionados a través del uso de IA, siendo necesario distinguir los supuestos de daños ocasionados "con" la cosa, o "por" la cosa. Es decir, un profesional liberal puede valerse de la IA como herramienta, lo que es válido siempre y cuando la utilice con responsabilidad y diligencia debida (controlando la información obtenida), o bien puede delegar su labor en una herramienta de IA. Ejemplo de esto último, es un abogado consultado por un trabajador despedido, que utiliza una herramienta de "Chat GPT" para

redactar un primer telegrama, copia y pega el resultado obtenido, y a raíz de ello no intima debidamente al empleador a abonar todos los rubros establecidos en la legislación vigente, privando a su cliente de percibir una indemnización integral. A raíz de ello, se deriva un daño a ese trabajador, y nos preguntamos cómo se aplican al caso concreto los presupuestos de la responsabilidad civil. Lo mismo puede decirse de un ingeniero civil que se vale de IA para efectuar un cálculo de estructura y a raíz de ello se derrumba una construcción, o de un médico que efectúa un diagnóstico erróneo mediante el uso de IA.

En los ejemplos expuestos, corresponde esclarecer la atribución de responsabilidad ante la mala praxis del profesional que se valió de IA, siendo ésta la causa adecuada del daño ocasionado al cliente. Una primera respuesta, es acudir al artículo 1768 del CCyCN vigente, y presuponer que el simple hecho de confiarse en una herramienta artificial es demostrativo de la omisión de diligencia debida por parte del profesional. Sin embargo, imponer al cliente dañado la carga de acreditar la reprochabilidad (dolo o culpa) parece irrazonable en los ejemplos propuestos.

a) La diligencia debida y el uso de la IA

El factor de atribución es el elemento axiológico o valorativo, el motivo que elige el legislador para erigir como fundamento del deber de responder. Cuando se dispone expresamente la aplicación de un factor objetivo de atribución, ello no significa que en el caso concreto no pueda existir una conducta negligente, dolosa o culposa (en muchos casos la hay); sino que el derecho prescinde de indagar la subjetividad, disponiendo que esa persona debe responder por el hecho de hacer uso de una cosa riesgosa, por ejemplo. El legislador "elige" determinada regulación por considerarla la más adecuada para dar una respuesta acorde a derecho en el contexto vigente. El contexto en el que se sanciona una determinada norma es cambiante, y es lo que sucede actualmente con el ejercicio de las profesiones liberales, donde la proliferación de herramientas de IA nos enfrenta a nuevas formas de ejercer las distintas profesiones liberales.

Pues bien, un profesional liberal que se vale de IA para ejercer sus funciones o su profesión, bien conoce o debe conocer que dicha herramienta es falible. El justiciable o el cliente confían en un profesional que se ha preparado para la función encomendada. Lo contrario implicaría aceptar el ejercicio de la profesión por parte de legos que tienen a su alcance una computadora con una aplicación de IA.

Hasta la fecha, ninguna herramienta de IA ha superado el test de Turing, según el cual, una máquina presentaría un comportamiento inteligente en la medida en que fuese capaz de mantener una conversación con un humano sin que otra persona pudiera distinguir quién es el humano y quién la máquina[6].

Entonces, como se dijo, si bien el hecho de que un profesional liberal opte por valerse de una herramienta de IA sin el debido control de la información arrojada, es demostrativo de una conducta cuanto menos negligente, el factor objetivo de atribución parece más adecuado para dar respuesta al problema expuesto.

[6] NAVAS NAVARRO, Susana, Inteligencia artificial. Tecnología Derecho. Tirant lo Blanch, Valencia 2017, p. 25.

ASIGNACIÓN DE INCENTIVOS PARA EL DESARROLLO DE LA IA Y LA PROTECCIÓN DEL USUARIO

Por Valentín G. Papp[1][2]

I. CONCLUSIONES

1. En el ámbito de los daños derivados de la inteligencia artificial generativa, la responsabilidad civil **objetiva** restringe el desarrollo de la industria tecnológica.

2. En el ámbito de los daños derivados de la inteligencia artificial generativa, la responsabilidad civil **subjetiva** afecta el derecho de los damnificados a una indemnización integral.

3. La generación de *deepfakes* es una actividad peligrosa en los términos del art. 1757 del Código Civil y Comercial por su naturaleza.

4. Se propone, de lege lata, que todos los que intervienen en la generación de contenido *deepfake* (desarrollador, proveedor y usuario que proporciona el *prompt*) responden por un factor objetivo de atribución en los términos del art. 1757 del Código Civil y Comercial.

II. FUNDAMENTOS

1. EL DESAFÍO DE LA INTELIGENCIA ARTIFICIAL

En palabras del CEO de Alphabet (la empresa madre de Google), Sundar Pichai, "la IA es el mayor salto tecnológico de la humanidad, más profundo que el fuego, la electricidad o cualquier cosa que hayamos hecho en el pasado"[3].

---

[1] Abogado (UNC). Maestrando en Derecho y Economía (UTDT). Adscripto a las Cátedras de Derecho Privado VII (Daños) (UNC), Economía (UNC) y Derecho Privado II (Obligaciones) (UCC). **Ponencia avalada por el Prof. Dr. José Fernando Márquez**, Titular de Derecho Privado VII (Daños) (UNC).

[3] Interpretación libre del texto original: "AI as the most profound technology humanity is working on. More profound than fire, electricity, or anything that we have done in the past", entrevista a Sundar Pichai disponible en:

En el escenario actual, la inteligencia artificial (IA) se ha convertido en un fenómeno omnipresente: utilizamos recursos laborales y académicos potenciados por inteligencia artificial (por ejemplo, búsqueda de doctrina y jurisprudencia, relación de sentencias de determinado Tribunal sobre un tema específico, explicación de conceptos, ideas o autores, etc.); desarrollamos nuestras actividades cotidianas con ayuda de ella (organización del calendario, aprender sobre nuevos temas o consumir contenido audiovisual en plataformas), así como también interactuamos socialmente en el entorno digital con herramientas de IA.

Así como cada nuevo progreso tecnológico ha tenido riesgos para la humanidad (pensemos en los medios de producción modernos, los medios de transporte, la industria farmacéutica, entre tantos otros), los hemos aceptado y tolerado considerando los beneficios que obtenemos de ellos. Esto lo logramos a partir de una regulación legal más o menos eficaz, de modo que podamos reducir e internalizar los riesgos a la vez que aprovechamos sus beneficios.

La Inteligencia Artificial implica un nuevo desafío para el Derecho en materia contractual, de igualdad y de derechos personales y fundamentales. El Derecho de Daños tiene la belleza de ser el encargado de concurrir transversalmente en todas esas áreas a prestar auxilio: generalmente a modo de reparación, a veces con un fin de prevención.

Las innovadoras formas de dañar a partir de la Inteligencia Artificial demandan no solo la sanción de nuevas leyes que regulen particularmente la IA, sino también la reinterpretación o adaptación de las normas actuales.

2. EL FACTOR DE ATRIBUCIÓN

En el ejercicio de determinar la responsabilidad civil de los daños, el Código Civil y Comercial tiene disposiciones específicas para atribuir el hecho dañoso a un sujeto jurídico: el factor de atribución.

El factor de atribución puede ser examinado a partir de los incentivos que genera.

Por ejemplo, podría decirse que un factor objetivo por riesgo puede disuadir a las empresas de invertir en el desarrollo de una tecnología. Si a la

---

https://www.cbsnews.com/news/google-artificial-intelligence-future-60-minutes-transcript-2023-04-16/.

empresa se le imputara a priori cualquier daño derivado de su utilización, no tendría incentivos para introducir esa tecnología al mercado. Asimismo, un factor objetivo incrementaría los costos derivados de su uso (por ejemplo, en proyecciones de indemnizaciones futuras y seguros).

No es absurdo plantear, entonces, que un factor objetivo ralentizaría el progreso tecnológico en el corto y mediano plazo (a largo plazo se espera que las empresas inviertan más en hacer sus productos más seguros, dado el factor objetivo de atribución).

Por otro lado, un factor subjetivo de atribución podría desproteger a los damnificados de sistemas de inteligencia artificial. La necesidad de demostrar la culpa o el dolo pone la prueba en cabeza del damnificado y favorece el desarrollo de la tecnología. Sin embargo, la complejidad del sistema, la opacidad algorítmica (esto es, no poder conocer los pasos de la secuencia lógica que llevó al resultado), la dificultad para predecir el contenido o respuesta y la multiplicidad de sujetos involucrados pueden dificultar la determinación del reproche subjetivo.

Estas circunstancias hacen que un factor subjetivo de responsabilidad afecte el derecho de los damnificados a una indemnización integral.

3. LA IA GENERATIVA DE *DEEPFAKES* COMO ACTIVIDAD PELIGROSA

Los contenidos *deepfakes* son falsificaciones hiperrealistas de la imagen o la voz de una persona real utilizando inteligencia artificial, de modo que parezca que esa persona está haciendo o diciendo algo que, en realidad, nunca hizo o dijo.

Existen sistemas dedicados de Inteligencia Artificial Generativa (o también llamados de IA creativa) que generan este contenido nuevo a partir de voz o imágenes de una persona real, cuyo objetivo es dar apariencia de realidad, es decir, que quien escucha o ve ese audio o video crea que es auténtico.

El objetivo declarado de confundir al oyente u observador para que un contenido falso parezca real debe considerarse un peligro ínsito de la actividad generativa. Se busca hacer indistinguible lo verdadero de lo falso.

Los *deepfakes* afectan especialmente derechos personalísimos como el honor, la reputación y la propia imagen, protegidos por el plexo normativo supranacional (v. gr., art. 12, Declaración Universal de Derechos Humanos)

y por el ordenamiento interno (arts. 52 y 53, Código Civil y Comercial). Esto es así porque el contenido falso puede hacer parecer a la persona cuya voz o imagen se imita como ridícula o mentirosa, o bien colocarla en situaciones criminales o vergonzantes.

La Real Academia Española define el término "falso" como "fingido, simulado; incierto, contrario a la verdad", mientras que la acepción de "peligro" es "situación en que aumenta la inminencia del daño".

En ese marco, va de suyo que el contenido falso, que simula una realidad que no existe, es más susceptible de ocasionar daños que si fuera verdadero.

En principio, las personas controlan sus propios actos y resulta menos probable que se coloquen en una situación criminal o vergonzante o publiquen contenido que las perjudica. En todo caso, estarán preparadas para actuar sobre situaciones reales en tanto conocen que ocurrieron, mas no sobre las infinitas creaciones ficticias que pueden generarse.

Así, la situación de riesgo (v. RAE, definición de "riesgo": "contingencia o proximidad de un daño") es notablemente mayor cuando se utiliza la IA generativa de *deepfakes*.

Por consiguiente, este peligro propio de la generación de *deepfakes* es una actividad peligrosa en los términos del art. 1757 del Código Civil y Comercial por su naturaleza.

En los casos en los que los daños se producen sobre derechos personalísimos, su reparación es compleja y la posibilidad de hacerlo, improbable.

La viralización de *deepfakes* que afectan el honor, la reputación o la propia imagen implica volcar en internet contenido que probablemente circulará para siempre y verán un número indeterminado de personas. El problema es que, aunque se busque una reparación, la rectificación o información sobre la falsedad del contenido difundido no tendrá alcance suficiente, el daño ya estará hecho y su reparación será casi imposible.

Por ello, la mejor alternativa es atacar el contenido *deepfake* desde la prevención, desincentivando directamente tanto al desarrollador y proveedor de la tecnología como al usuario que da la instrucción para crear el contenido potencialmente dañoso.

El factor objetivo de atribución, en tanto permite al damnificado prescindir de la prueba de la culpa, es más eficiente para prevenir daños,

pues el desarrollador del sistema buscará impedir su mal uso y el potencial dañador evitará ocasionarlo para obviar ser pasibles de la imputación.

Por ello, considerando **(1)** la potencialidad dañina de la generación de *deepfakes*, **(2)** la compleja e improbable reparación del daño causado a derechos personalísimos y **(3)** que un factor objetivo es más eficiente que uno subjetivo para prevenir daños, se propone, de lege lata, que todos los que intervienen en la generación de *deepfakes* (desarrollador, proveedor y usuario que proporciona el *prompt*) responden por un factor objetivo de atribución, en tanto es una actividad peligrosa en los términos del art. 1757 del Código Civil y Comercial.

DAÑOS, INTELIGENCIA ARTIFICIAL Y ALGORITMOS

Por Matilde Pérez[1]

I. CONCLUSIONES

De lege lata

1. El principio precautorio permite facilitar la transparencia algorítmica y, con ello, evitar daños en contextos de especial incertidumbre como es el caso de las llamadas *cajas negras* o *black box.*

2. La opacidad u oscuridad de los modelos se refleja en la falta de información adecuada, veraz, completa y clara; en la falta de conocimiento de los modelos o criterios utilizados para las tomas de decisiones que se traducen en agentes generadores del daño.

3. La transparencia en el desarrollo de los modelos algorítmicos es un mecanismo para la gestión de la incertidumbre científica acerca de los procesos de *input* y *output* que permite evitar o mitigar daños, así como establecer desde el diseño, procesos algorítmicos que eviten la generación de sesgos negativos.

De lege ferenda

4. Es necesario establecer estándares en materia de transparencia y privacidad desde el diseño.

5. Se debe propiciar, de acuerdo al estado de los conocimientos científicos, el *itinere* algorítmico implementado.

II. FUNDAMENTOS

1. INTRODUCCIÓN

La llamada Revolución 4.0 se caracteriza por innovaciones tecnológicas que, al igual que las Revoluciones precedentes, produce un

[1] Abogada (UCA). Jefa de Trabajos Prácticos por la Universidad Argentina de la Empresa (UADE) en las asignaturas: “Obligaciones y Contratos” e “Introducción al Derecho”. Autora de diversos trabajos de doctrina y miembro de equipos de investigación jurídica aplicada. Email: moreyrap.cs@gmail.com.

cimbronazo en el modo de vivir, de pensar o llevar adelante actividades o procesos donde la incertidumbre y la fascinación imperan por doquier.

El Derecho como ciencia y como orden social justo no escapa a ello. Conceptos consolidados como persona, consentimiento, hecho y acto jurídico, contrato o certezas construidas a partir de normas o principios parecen no serlo tanto.

Hay una incertidumbre que es propia del desarrollo e implementación de estas nuevas tecnologías que producen transformaciones respecto de las cuales no siempre pueden medirse o establecerse los impactos.

Surge el desafío de decidir en entornos de incerteza. La seguridad jurídica muta hacia un ámbito donde la balanza puede moverse entre la arbitrariedad, la prudencia, la discrecionalidad o la ineficacia.

El vertiginoso avance de las ciencias vinculadas a la informática en todas las áreas de la vida humana, abre el debate sobre la incidencia de la utilización de sistemas de automatización y si éstos pueden ser programados de manera que se sustituya la voluntad humana en pos de mayor celeridad, mayor ganancia, mayor poder, mayor eficiencia o mayor bienestar, entre otros.

Desde que se comenzó a utilizar la expresión inteligencia *artificial* apareció la idea de emular o superar la inteligencia humana. Las ideas de una inteligencia artificial débil y fuerte se plasmaron en diversas investigaciones, ensayos y desarrollo de diversos sistemas. En el caso de la inteligencia artificial débil en el sentido de contribuir con las actividades mentales del ser humano, a diferencia de la inteligencia artificial fuerte que busca la sustitución de las capacidades humanas y se la identifica con la inteligencia artificial generativa.[2]

Es en este contexto y, en especial, en los últimos cinco años en que su crecimiento y expansión hace que el semáforo se coloque en amarillo ¿ Todo es válido en el planeta IA? En forma rotunda, se afirma que no debiera ser así.

En el mientras tanto ¿ qué soluciones son posibles frente a los daños causados por los sistemas de IA? ¿ Es viable la aplicación del sistema

[2] López de Mántaras Badía, R.; Meseguer González, P. *¿ Qué sabemos de Inteligencia Artificial?* Ed. CSIC Los libros de la Catarata, Madrid, 2017, p. 5.

jurídico argentino? ¿ En el ámbito de la responsabilidad civil, cuál es la naturaleza jurídica de la inteligencia artificial como elemento central para la determinación de la existencia de presupuestos para reparar? ¿ Es viable una función preventiva del daño para evitar o mitigar los impactos?

Lo cierto es que la sociedad civil en su conjunto debe trabajar para preservar los derechos y libertades, así como la dignidad intrínseca de nuestro ser humano.

Temas todos ellos que convocan en las XXIX Jornadas Nacionales de Derecho Civil en homenaje a ese gran jurista y excelsa persona, Dr. Jorge H. Alterini.

2. LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL: UN ENGRANAJE COMPLEJO

La inteligencia artificial es un sistema tecnológico que está preparado para resolver problemas puntuales con múltiples definiciones.

La Unión Europea la define como "un sistema programado para poder analizar el entorno y pasar a la acción con cierto grado de autonomía para alcanzar objetivos específicos".[3]

Esta definición de la Comisión aporta varios elementos que son el punto de partida para la búsqueda de marcos éticos y regulatorios diversos que permitan crear certezas jurídicas acerca de todo el *itinere* seguido por el sistema de IA desde su diseño hasta su aplicación práctica.

Los algoritmos, son procedimientos para hallar soluciones a un problema a través de su reducción a un conjunto de reglas; es también, cualquier procedimiento formalizado en una serie de pasos para solucionar un problema o conseguir un resultado.

Ambos interactúan para resolver un problema específico en un contexto que está informatizado y que requiere de un marco normativo

[3] Comisión de la Unión Europea. COM (2018) 237 final. Bruselas 25/404/2018.Disponible en http://www.saij.gob.ar/0-internacional-com-2018-237-ue-inteligencia-artificial-para-europa-lnt0007528-2018-04-25/123456789-0abc-defg-g82-57000tcanyel?&o=5&f=Total%7CTipo%20de%20Documento/Legislaci%F3n%7CFecha/2018%5B20%2C1%5D%7COrganismo/categoriavacia%7CPublicaci%F3n%7CTema/Parlamento%20Europeo%7CEstado%20de%20Vigencia/Vigente%2C%20de%20alcance%20general%7CAutor%7CJurisdicci%F3n&t=6, consultado 20/05/2024.

mínimo sea de carácter público o privado (autorregulación, *compliance*), o sustentado en principios éticos. [4]

Esa interacción permite poner en marcha diversos sistemas con características y finalidades distintas. Las ventajas en muchas áreas como la medicina predictiva, la portabilidad de las historias clínicas, la simplificación de procesos de toma de decisiones en la actividad administrativa, legislativa o judicial, la agilización y seguridad del tráfico económico financiero, la utilización de la tecnología digital para la identificación de personas o bienes a través de la biometría o las cadenas de bloques, entre otras colabora en el bienestar y seguridad.

Junto a esas ventajas, crecen las preocupaciones acerca de cómo estas inteligencias artificiales pueden afectar la dignidad humana, la libertad y autonomía de la voluntad, los procesos de tomas de decisiones la soberanía e independencia de los países en especial, cuando los sistemas pueden tener autonomía decisional como en el caso de los drones o en los vehículos inteligentes.

En efecto, dentro de las críticas a estos sistemas aparecen las posibilidades de merma de las habilidades cognitivas, sociales o de supervivencia e influir en cuestiones vinculadas a la privacidad, el uso de datos personales o la exclusión derivada del uso de sesgos de discriminación negativa.[5]

La " materia prima" de los sistemas de IA son los algoritmos que se alimentan de grandes volúmenes de datos. Es preciso indagar cómo las máquinas pueden utilizar el lenguaje, realizar abstracciones y conceptos, resolver problemas de los seres humanos y automejorarse. En su esencia está que se comporte de manera tal que se lo llame " inteligente".[6]

---

[4] Vestri, G. " La inteligencia artificial ante el desafío de la transparencia algorítmica. Una aproximación desde la perspectiva jurídico-administrativa". Revista Aragonesa de Administración Pública, Nro. 56, 262, 2021, pp. 369-370. Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=7971161, consultado 20/05/2024.

[5] Anderson, J.; Rainnie, L.; Luchsinger, A. *Artificial Intelligence and the future of Humans.* Pew Research Center, Diciembre 2018. Disponible en www.pewresearch.org, consultado 17/06/2024.

[6] Mc. Carthy, J. " *A proposal for Darthmouth Summer Research Project on Artificial Intelligence*". Documento suscripto el 31 de agosto de 1955. Disponible en dartmouth.dvi(standford.edu), consultado el 16/06/2023, p.2.

Se abre entonces un debate sobre el uso e impacto de las mejoras en los algoritmos, el crecimiento de la disponibilidad de recursos computacionales, así como el incremento de volúmenes de datos que pueden ser utilizados para su análisis.

Estos desarrollos se ven favorecidos por tipos específicos de inteligencia artificial, como, por ejemplo, la *machine learning* o la inteligencia artificial generativa.

En idéntico sentido, la expansión de las aplicaciones para todo propósito trae como resultado planteos que impactan de lleno en el derecho constitucional y, también, en el derecho de daños. [7] Si se piensa en la cantidad de datos que se suministran en el quehacer diario se percibe que son los que mueven a gobiernos, industrias y, también, a muchos fantasmas escondidos tras el *clic* o el acepto.

Y en particular, el avance de la inteligencia artificial generativa en la que se engloba a aquella tecnología capaz de tomar elementos del mundo digital y " crear" algo nuevo como textos, imágenes, fragmentos de texto, desarrollo de texto, inventar jurisprudencia. En el caso de los ChatGPT o el creador de texto a imagen Stable Diffusion, absorben una gran cantidad de datos inconmensurables desde la racionalidad humana, en los que el aprendizaje profundo desarrolla conexiones que son volcadas en expresiones de aparente veracidad. [8]

Es por ello, que se torna necesaria la mejora de la cooperación digital como una estructura piramidal en cuya cúspide se halle el ser humano en todos estos procesos de transformación, lo que implica aspirar a sistemas de inteligencia artificial " empáticos" de manera que se puedan anticipar, mitigar o reparar eventuales daños causados por ellos.

Ello por cuanto, tienen aptitud para la mejora de su desempeño de acuerdo a las capas de redes neuronales que puedan establecer lo que se puede hacer de manera automática, con la asistencia de los seres humanos o a través del aprendizaje o modificación de los modelos de aprendizaje (LLM); interactúan con el entorno y lo influencias como sucede con los

---

[7] Carsten Stahl, B., Schroeder, D., Rodrigues,R. *Ethics of Artificial Intelligence. Case Studies and Options for Addressing Ethical Challenges.* Ed. Springer, 2023.

[8] Simonite, T. " Inteligencia artificial. La Guía completa WIRED", Rev. WIRED, 12 de febrero de 2023. Disponible en Inteligencia artificial: la Guía completa

chatbot, los elementos de uso cotidiano ligados en el Internet de las Cosas (IoT).[9]

La ley europea de inteligencia artificial del 13 de marzo de 2024 normativiza los sistemas algorítmicos con base a la calificación del riesgo en un rango que va del extremo al riesgo mínimo. Esta escala se basa en el grado de impacto en lo individual o lo social, pero en modo alguno puede ser entendido como una escala de mayor a menor dañosidad.

Si se analiza el rango de riesgo mínimo, encontramos en ella a los ChatGPT. En este punto es necesario un análisis en lo intrínseco y lo extrínseco.

Desde el interior del software o el hardware usado como continente el sistema puede ser más o menos inocuo.

Desde la perspectiva de su impacto social, este tipo de sistemas pueden significar un choque entre la verdad y la mentira; la realidad y lo inventado; la creación de realidades virtuales que no tienen soporte real y que pueden generar daños cuya masividad lejos está de ser prevista.

Es entonces que, para establecer la responsabilidad civil ante los daños producidos por la intermediación de sistemas de inteligencia artificial, se debe ir más atrás, al propio algoritmo.

En la génesis, producción, desarrollo e interacción del algoritmo pueden estar presentes los presupuestos del responder para dar lugar a la reparación del daño; pero también, en una mirada puesta en la función preventiva desde la perspectiva de los principios de precaución y prevención, así como en la aminoración de la posibilidad de una ulterior responsabilidad derivada de los riesgos del desarrollo.

3. EL DAÑO INJUSTO EN LA RUTA DE LOS ALGORITMOS

a) El daño injusto: reparar y prevenir

Se define al daño injusto como aquél que no existe el deber jurídico de soportar.

---

[9] Comisión Europea. Grupo independiente de expertos de alto nivel sobre inteligencia artificial. *Directrices para una IA fiable.* 08/04/2018. Completar datos y resumen de los puntos

En ese sentido, el art. 1737 CCC establece que existe daño cuando hay una lesión a un derecho o un interés no reprobado por el ordenamiento jurídico sea tanto en la persona o su patrimonio, así como a un derecho de incidencia colectiva.

Esta es la base de la construcción del moderno derecho de daños donde existe un eje en equilibrio sustentado en los principios de buena fe y en principio de no dañar a otro.

La ruptura de alguno o de ambos principios hace que ese eje se corra y, por tanto, surja el deber de reparar.

Los algoritmos pueden ser considerados cosas riesgosas en el marco de lo establecido en el art. 1757 del CCC dada su naturaleza, así como la forma de su utilización. Es entonces que la responsabilidad será de carácter objetivo.

Empero, esta afirmación es contundente y simple en apariencia pues el algoritmo trasunta por diversas zonas grises donde no siempre es posible establecer el agente dañador, la relación de causalidad o el marco jurídico que sustenta al sistema de reparación.

En una retrospectiva de la segunda mitad del siglo XIX en los que la electricidad y la automoción aparecen como grandes inventos y como grandes dañadores, pasaron años para que la normativa, la doctrina y la jurisprudencia reconocieran la existencia de nuevos factores de atribución de carácter objetivo, en particular, la teoría del riesgo.

La producción masiva, el reconocimiento de los derechos de los consumidores incorporan otros criterios como la obligación de seguridad, el deber de garantía, la equidad que conviven con los criterios de atribución subjetiva.

En este estudio, pareciera que la ciencia pierde su autonomía al confundirse con la técnica. A la par, se crean certezas para afrontar y neutralizar el riesgo que se crea. Ese riesgo, nace de una incertidumbre científica y se busca evitarlo o aminorarlo ante la posibilidad de generar daños masivos e irreparables.

En todo ello, el principio de precaución en el marco de la función preventiva del daño es un mecanismo por analizar como modo de gestionar

los riesgos acerca de las consecuencias de los procesos de toma de decisiones automatizadas generadas por algoritmos.[10]

b) La ruta de los algoritmos

Es una constante de este tiempo que las operaciones, decisiones y elecciones que antes se dejaban a los seres humanos, hoy se delegan cada vez más en algoritmos que pueden asesorar, o decidir, acerca de cómo deben interpretarse los datos y acciones a seguir en consecuencia lo que incide en las formas como los individuos y grupos pueden gestionar sus intereses.

El algoritmo es un procedimiento de cálculo que consiste en completar un camino ordenado y finito de instrucciones sobre unos datos específicos para arribar a la solución de un problema planteado. Se apropian de esos datos para alcanzar un determinado objetivo. Esos datos masivos o *big data* son los grandes activos empresariales que permiten que los algoritmos tengan cada día una mayor complejidad atento un crecimiento exponencial de sus finalidades.

Si se analiza su evolución, en sus inicios se basaban en sistemas expertos en los cuales los programadores trasladaban punto por punto las normas y criterios previstos para lograr conclusiones.

En la actualidad, el aprendizaje automático pretende simular el funcionamiento del cerebro humano para lo cual, el diseño y puesta en marcha del algoritmo está en cabeza del programador, aunque existen algoritmos que pueden generan modelos a partir de los datos disponibles.[11]

Esta situación surge de la naturaleza del algoritmo como elemento basilar en la construcción de una inteligencia artificial. Se desarrolla y convive a través de diversas técnicas de aprendizaje como la *machine learning*, el *deep learning* o el árbol de decisiones o *decisión tree* por lo que

---

[10] Barone, A. " *Amministrazione del rischio e intelligenza artificiale". Europe Review of Digital Administration & Law,* ERDAL, 2020, Vol. 1, Junio-diciembre, p. 63-67. Disponible en https://www.erdalreview.eu/free-download/97888255389606.pdf, consultado 20/05/2024.

[11]Cerrillo Martínez, A. " Com obrir les caixes negres de les administracions públiques? *Transparència i rendició de comptes en l´ós dels algoritmes".* Revista Catalana de Dret Oúblic Nº 58, 2019, pp. 13-29. Disponible en https://www.raco.cat/index.php/RCDP/article/view/357191, consultado el 20/05/2024.

es necesario indagar sobre el alcance de una acción que es tomada de manera automatizada.

En los programas de aprendizaje automático el denominador común es la aptitud para reconocer y clasificar patrones a través de las denominadas redes neuronales que son parte de los aprendizajes supervisados en que los sistemas aprenden a clasificar sobre la base de datos de entrenamientos ya conocidos.

Con este sistema conviven los llamados aprendizajes de refuerzo en que el algoritmo aprende a partir de interactuar con acciones previas o por selección aleatoria de las acciones posibles a través de prueba y error.

En el caso de los algoritmos de minería de datos, pueden dar sentido a los flujos emergentes de datos de comportamiento generados por el internet de las cosas (IoT), esto es, obtenidos a través de elementos que utilizamos en la vida cotidiana como puede ser la computadora, el celular, la aspiradora o los asistentes virtuales sin que los usuarios puedan acceder a esos algoritmos de filtrado y personalización.

Al estudiar los algoritmos de aprendizaje automático o *machine learning*, el foco de la atención debe estar en la identificación desde su creación de los posibles conocimientos engañosos, sesgados o inexactos. Ello por cuanto estos algoritmos están cargados de sesgos o valores determinados por los desarrolladores y configurados por los usuarios tomando en cuenta los resultados deseados en que se privilegian unos valores o intereses en demérito de otros.

Sin embargo, no siempre elegir determinada información o forma de incorporación de datos en estos algoritmos puede ser aceptables desde una perspectiva ética en lo que hace a la protección de la persona humana en su dignidad. Tampoco desde lo jurídico, pues pueden ser mecanismos de conculcación de los derechos fundamentales, así como a su entidad como posible agente generador de daños en detrimento del destinatario final del sistema de IA que se vale de estos algoritmos.

Extraer patrones a partir de los datos existentes sin que los programadores puedan crear de forma intuitiva y precisa cómo funcionan. Estos algoritmos funcionan sobre la correlación entre datos y no sobre la base de una relación causal, se producen más predicciones a medida que se disponen de nuevos datos. Ello se hace de forma ininteligible para la mayoría

de los usuarios porque los datos y resultados están relacionados de una manera compleja y no lineal.[12]

Es difícil poder determinar el impacto dañoso potencial y real de un algoritmo. Por una parte, identificar la subjetividad humana en el diseño y la configuración del algoritmo por cuanto en muchos casos se requiere investigar procesos de desarrollo multiusuario a largo plazo. Por la otra, aún con los recursos suficientes, los problemas y los valores subyacentes sólo emergerán frente a la causación efectiva del daño. [13]

De ello se puede deducir que la determinación de una responsabilidad subjetiva de quién o quiénes desarrollan y configuran el algoritmo se torna dificultosa, en especial, desde la perspectiva de aquellos que sufren un daño tanto individual, colectivo o masivo.

A ello debe añadirse que estos desafíos son mayores en la medida que los algoritmos aumentan su complejidad e interactúan con los resultados de cada uno para las tomas de decisiones.

¿Será entonces centrarse en cuánta incertidumbre es admisible para poner en marcha estos algoritmos vinculados al aprendizaje profundo? Esa incertidumbre, ¿se puede tolerar en aquellas situaciones en que pueden tomar decisiones debido a su aptitud para mejorar los parámetros operativos y las reglas de tomas de decisiones en su elemento?

Esta incertidumbre, ¿ puede ser considerada un riesgo y, por ende, ser gestionada para su prevención? ¿ al ser un riesgo, la responsabilidad es objetiva y de todos los actores que intervienen en la cadena causal?

En todas estas preguntas, planea la idea de una brecha entre el funcionamiento de los algoritmos con la comprensión de las implicaciones éticas y jurídicas.

---

[12] Cerrillo Martínez, A. " Com obrir les caixes negres de les administracions públiques? *Transparència i rendició de comptes en l´ós dels algoritmes".* Revista Catalana de Dret Oúblic Nº 58, 2019, pp. 13-29. Disponible en https://www.raco.cat/index.php/RCDP/article/view/357191, consultado el 20/05/2024.

[13] Mitteldstadt, B.; Allo,P.; Floridi, L. "*The Ethics of Algorithms: mapping the debate*". *Big Data & Society*, 3 (2), 2016, pp. 1-21. Disponible en DOI: 10.1177/2053951716679679, consultado el 20/05/2024.

Es en este sentido, que el algoritmo como esencia de la inteligencia artificial como producto a analizar desde su diseño requiere de la adopción de medidas para la gestión de la incertidumbre en la que el principio de transparencia tiene un rol central.

4.

a) La transparencia aplicada al ámbito de la IA

Transparencia es una palabra polisémica tanto en el lenguaje coloquial como en el jurídico. En el caso del binomio transparencia-ciencias vinculadas a la inteligencia artificial, impacta de manera transversal a distintas ramas del derecho, las ciencias de la administración, económicas o sociales.

En 2017, el Parlamento europeo dicta las normas de derechos civiles sobre la robótica para actualizar y completar la normativa de la Unión Europea a través de directrices éticas que orienten el desarrollo, la producción, usos y modificaciones de los robots.

Entre sus principios, la transparencia significa entender las razones por las que ante cualquier decisión tomada con la ayuda de la inteligencia artificial puede influir en la vida de las personas, debe ser posible que los procesos del sistema puedan ser legibles por el ser humano. [14]

b) La opacidad algorítmica

La opacidad algorítmica es una de las cuestiones centrales a solucionar en estos sistemas. El diseño, desarrollo y producción en estas tecnologías deben tener como punto de partida la transparencia de los procesos de manera que se pueda acceder a esos tipos de informaciones por los consumidores, los usuarios y los actores sociales en general, en un lenguaje claro y veraz.

---

[14] Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)) (2018/C 252/25). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017IP0051&from=EN, consultado el 20/05/2024.

La opacidad algorítmica puede impactar en la eficiencia de un sistema y en la posible causación de daños, así como impedir que se pueda hacer una rendición de cuentas sobre la actuación o el cumplimiento de los estándares disponibles ante la posibilidad de tener su fuente en razones técnicas, jurídicas y organizativas.

Las causas técnicas pueden obedecer a la complejidad o al carácter dinámico del algoritmo. En algunos casos, es difícil conocer en detalle su funcionamiento y los datos que tienen en cuenta para producir un determinado resultado que no siempre puede ser el buscado o previsto por el desarrollador.

En la opacidad jurídica, pueden existir normas o cláusulas contractuales que limitan el acceso a la información para la protección de otros bienes o derechos, la protección de datos personales o razones de seguridad jurídica.

En las causales organizativas, las razones son múltiples. La más común, la ausencia de información sobre los algoritmos, lo que muchas veces está relacionado en el hecho que el código fuente está en manos de quién terceriza el servicio al Estado.

La posibilidad de explicar el proceso de creación de un algoritmo y cómo funciona hacen la diferencia en lo que hace a la confiabilidad y seguridad de los sistemas de IA. En este sentido, la puesta en marcha de leyes y técnicas de aprendizaje automático diseñadas para abordar el problema de las decisiones inescrutables son mecanismos para que los científicos informáticos puedan levantar ese manto oscuro o ayudar a la compresión de los denominados " patrones extraños" que aparecen en un *output* que no es correcto ni incorrecto, sino que no se corresponde con los datos suministrados en los procesos de *input.* Fuera de las cajas negras, también debe analizarse cómo se desarrolla y se usa un proceso de aprendizaje automático.

Esto es, en ese itinerario algorítmico dentro del sistema de inteligencia artificial no siempre pueden ser explicados los procesos de ingreso de datos y egreso de decisiones, lo que se conoce como " cajas negras" o *black box*, lo que da lugar a planteos de carácter ético, jurídico y social acerca de los sistemas atravesados por esta opacidad.

En ellos, la transparencia permite establecer el respeto por la legalidad, deshace el anonimato y posibilita la exigencia de responsabilidades, así como el acceso de los ciudadanos a la información sobre los procesos algorítmicos

En efecto, hay partes de los modelos de aprendizaje automático (ML) que no aparecen en los modelos, pero pueden servir para contextualizar su funcionamiento, por qué el sistema elige un camino y no otro. En definitiva, apuntar a un proceso de trazabilidad de los modelos en forma análoga a los procesos establecidos en materia de productos elaborados como un mecanismo de gestión de riesgos a través del principio de transparencia.[15]

El principio de transparencia es un principio de raíz filosófica que ya se esboza en la Grecia Clásica, que suele vincularse con el buen gobierno y acceso a la información pública en el sector público y con los procesos de control de calidad de gestión, de procesamiento de datos, códigos de buenas prácticas, normas de autorregulación o *compliance* corporativo.

En cualquiera de sus formas, se puede afirmar que el principio de transparencia abreva en el principio general de buena fe por lo que se aplica en aquellos procesos que, derivados de la opacidad algorítmica, se pueden generar daños derivados del algoritmo *per se*, del proceso algorítmico, del sistema de IA o del impacto de este sistema en los diversos actores sociales y con gran relevancia en aquellas operaciones que pueden llegar a ser intangibles.

5. TRANSPARENCIA Y PRINCIPIO DE PRECAUCIÓN. UNA PROPUESTA

El principio de precaución puede ser utilizado para facilitar la transparencia algorítmica frente a información deficiente, los datos suministrados y los diversos procesos de aprendizaje, así como gestionar los riesgos.

---

[15] Selbest, A.; Barocas, S.*" The intuitive Appeal of Explainable Machine". Fordham Law Review,* 87, (3), 2018 p. 1089-1090. Disponible en https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5569&context=flr, consultado el 20/05/2024.

El principio de precaución se centra en la incertidumbre científica y en la necesidad de tomar decisiones ante la amenaza de daños masivos e irreversibles. Ese "humo de peligro" se manifiesta en las correlaciones, el reconocimiento de parones o la multiplicación exponencial del uso de los datos. Estos modelos, como se señalara, son abstractos, se auto entrenan y generan esos *outputs* opacos propios de las cajas negras.

La utilización del principio colabora en la determinación de cuánta transparencia es posible al colaborar en los procesos para acceder a los datos, a la información y al conocimiento del entorno de la inteligencia artificial, esto es, el itinere algorítmico.

EL PRINCIPIO DE PRECAUCIÓN, LOS RIESGOS DE DESARROLLO: SU APLICACIÓN A LA INTELIGENCIA ARTIFICIAL

Por Matilde Pérez[1]

I. CONCLUSIONES

De lege lata

1. La gestión de la incertidumbre científica tiene en el principio de precaución y en los riesgos de desarrollo dos herramientas en el marco de las funciones preventiva y resarcitoria del derecho de daños en miras a la gestión de riesgos y reparación de los daños derivados de la utilización de sistemas basados en IA.

2. Los Estados tienen una obligación legal de adoptar medidas adecuadas para evitar la producción de daños evitables o potenciales en contextos de gravedad inusitada o irreparabilidad.

3. La IA es un camino sinuoso en el que se bifurcan la certeza de sus bondades para el progreso humano y los peligros para su dignidad humana, la preservación del medio ambiente y la convivencia democrática.

4. Los sistemas basados en IA deben ser considerados como un producto elaborado y, por lo tanto, amparados por las normas derivadas del estatuto de defensa de los consumidores, así como el régimen de responsabilidad civil.

De lege ferenda

---

[1] Abogada (UCA) Doctora en Ciencias Jurídicas (UCA). Especialista en Derecho Administrativo (UNLa Plata). Profesora titular de las asignaturas Obligaciones Civiles y Comerciales, Derecho de Daños y Derechos Reales en la Facultad de Derecho de la Universidad Católica Argentina. Profesora en el Doctorado en Ciencias Jurídicas y en la Maestría de Derecho Civil Patrimonial de esta Universidad, miembro del Comité Asesor del Doctorado en Ciencias Jurídicas y miembro de la Comisión de Abogacía Digital (UCA). Profesora asociada en las asignaturas Derecho de las Obligaciones y Derecho de Daños en Universidad Austral. Profesora invitada en Universidades nacionales y extranjeras. Coordinadora del Suplemento " Derecho, Innovación y Desarrollo Sustentable" en Editorial El Derecho. Autora de libros, capítulos de libros y ponencias. Correo electrónico matildeperez@uca.edu.ar . ORCID 0009-0008-2189-701X

5. Es necesario propiciar un marco normativo que permita inscribir estos institutos como protectorios de la dignidad humana en los sistemas basados en IA.

6. Se debe impulsar la creación de organismos con responsabilidad y sensibilidad ética.

7. Se propicia que los riesgos de desarrollo sean incluidos en el sistema jurídico argentino en el marco de la responsabilidad por productos.

II. FUNDAMENTOS

1. INTRODUCCIÓN

En 1956, en la Conferencia de Dartmouth, un grupo de científicos dirigidos por J. McCarthy proponen introducir un estudio sobre la inteligencia artificial (IA). Ellos consideran que cada aspecto del aprendizaje o cualquier otra característica de la inteligencia, en principio, debe ser descripto con tanta precisión que pueda hacerse que la máquina lo simule. Se debe indagar cómo estas máquinas pueden analizar el lenguaje, formar abstracciones y conceptos, resolver problemas reservados a los seres humanos y, además, automejorarse.

Todo este proceso es movido por el proceso de lograr que esa máquina se comporte de modo tal que se pueda llamar inteligente. De allí la idea de " inteligencia artificial".[2]

Esta definición de inteligencia artificial como un análogo de la inteligencia humana es modificada con los avances científicos y tecnológicos por lo cual desde hace años que se vienen impulsando diversas iniciativas con el objeto de definir qué es la inteligencia artificial, cómo opera, cuál es el impacto en la sociedad, así como en los ordenamientos jurídicos.

A la par, el crecimiento exponencial de los distintos sistemas, procesos o productos que se valen de la inteligencia artificial para el

[2] McCarthy, J. " A proposal for Dartmouth Summer Research Project on Artificial Intelligence". Documento suscripto el 31 de agosto de 1955. Disponible en http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf , consultado el 30/06/2024

cumplimiento de su finalidad hace que ese impacto se traslade a todas las áreas del conocimiento y surjan nuevos planteos y búsqueda de soluciones.

Temas como el futuro de las relaciones laborales, la prestación de los servicios de salud y educación, los vehículos y drones de conducción autónoma, la pérdida de la privacidad en pos de la comodidad entre muchos otros, revelan la necesidad de proteger los derechos y garantías de las generaciones actuales y de las venideras y fijar marcos éticos y regulatorios de protección de la dignidad humana.

Se debe redefinir cuál es el rol del Estado: espectador o, por el contrario, ser garante de la seguridad, la transparencia, la seguridad y la protección ante las nuevas tecnologías que puedan llevar implícitos sesgos discriminatorios, manipulación de opinión pública o ante la posibilidad de aparición de daños de carácter masivos y de difícil reparación.

Las respuestas, lejos están de ser unánimes.

No obstante, la realidad tecnológica avanza a una velocidad en la que el derecho parece correr varios miles de kilómetros atrás.

Es entonces, donde surge la pregunta acerca de la posibilidad de analizar los sistemas de IA desde la óptica del principio de precaución en estos contextos de incertidumbre científica y posible daño masivo, así como una eventual responsabilidad fundada en los riesgos de desarrollo cuando la ausencia de toma de decisiones o de gestión de los riesgos hace que los daños se manifiesten mucho tiempo después como daño tardío o como daño a futuro.

2. EL DERECHO Y LA IA

En este camino de regulación de la IA, se destacan los siguientes instrumentos:

a) Consejo de Europa

El 17 de mayo de 2024 en Estrasburgo se firma el tratado regulatorio de la IA, que vincula jurídicamente a los Estados miembros y abierto a la firma de países no europeos Se aplica a la totalidad del ciclo de vida de los sistemas de IA, con el eje puesto en la innovación responsable y en los riesgos que pueda entrañar. Desde una mirada de prevención del daño, obliga a los Estados signatarios a poner en marcha medidas para identificar,

evaluar, anticipar y atenuar los posibles riesgos incompatibles con el respeto de la dignidad y los derechos humanos.

Por otro lado, también establece como misión que la IA pueda ser utilizada para atacar las instituciones y los procesos democráticos, haciendo hincapié en el respeto de los principios de separación de poderes.

El tratado recoge la labor de dos años del Comité integrado por los miembros del Consejo junto con los representantes de otros países, entre los que se encuentra Argentina, así como representantes de diversos sectores públicos y privados. [3]

b) Unión Europea

Reglamento de inteligencia artificial de la Unión Europea. El 13 de marzo de 2024, el Consejo aprueba el reglamento sobre inteligencia artificial.

Esta norma adopta el enfoque basado en el riesgo, a mayor riesgo, normas más estrictas. Es la primera de este tipo que se adopta a nivel global y se estima que puede ser adoptado como estándar normativo en países extracomunitarios.

La IA es categorizada siguiendo esta impronta y los criterios de transparencia algorítmica. Los de riesgo bajo o limitado esa obligación es atemperada a diferencia de los sistemas de alto riesgo que estarán permitidos con la condición de cumplir con los requisitos y obligaciones que se fijen para acceder al mercado de la Unión.

Aquellos sistemas que puedan significar la manipulación del comportamiento cognitivo y la puntación social, están prohibidos por ser un riesgo inaceptable. Se prohíbe, además, el uso de vigilancia predictiva basada en perfiles y los sistemas que utilizan datos biométricos para categorizar a las personas de acuerdo a determinadas características como raza, religión, estrato social u orientación sexual.

c) UNESCO

[3] Council of Europe Framework convention on artificial Intelligence and human rights, democracy, and the rule of law. Disponible en https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680afb11f, consultado el 02/07/2024.

Marco ético sobre inteligencia artificial. La totalidad de los Estados miembros aprueban este marco ético que establece principios y valores éticos comunes que deben ser la guía para el desarrollo responsable de la IA.

Con esta Recomendación se busca realizar un aporte a la sociedad y reducir los riesgos que conlleva la IA. En esta línea, sostiene que las transformaciones digitales deben promover los derechos humanos, contribuir a la consecución de los Objetivos de Desarrollo Sostenible (ODS) a través de la transparencia, la rendición de cuentas, la privacidad, la acción sobre gobernanza de datos, educación, cultura, trabajo, economía o asistencia sanitaria.

En materia de protección de datos, la transparencia es uno de los temas centrales aunada al derecho a acceder cada persona a sus datos e, incluso, borrarlos. En lo que hace a los marcadores sociales y la vigilancia masiva, se prohíbe el uso de estas tecnologías por ser invasivas, violar los derechos y libertades fundamentales y generar daños masivos y de difícil remedio. La evaluación y supervisión de los sistemas debe estar signada por la transparencia a lo largo de su itinere vital.[4]

d) Declaración de Montreal

En 2018 se suscribió la Declaración de Montreal para un desarrollo responsable de la inteligencia artificial, fruto del trabajo de varios expertos. Tiene como objetivo establecer un marco ético para el desarrollo e implementación de la IA. Se establecen como principios el bienestar social de todos; la autonomía en los procesos de toma de decisiones; justicia a través de una IA imparcial y que no perpetue discriminación o sesgos; privacidad de datos personales y no injerencia en la vida privada; democracia como mecanismo para potenciar la participación ciudadana; excelencia técnica; cooperación global y sostenibilidad ecológica.

Se destaca la responsabilidad como principio aplicable a los creadores de la IA.

e) Vaticano

[4]UNESCO. Marco ético sobre la inteligencia artificial. Disponible en https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa, consultado el 02/07/2024.

Su Santidad Francisco desde hace tiempo viene promoviendo diversas iniciativas acerca del uso de la IA. Desde una perspectiva jurídica se destacan:

e.1. La Llamada de Roma para una IA Ética: Tiene como objetivo garantizar un futuro en el que la innovación digital y el progreso tecnológico estén al servicio del genio y la creatividad humana y no su sustitución gradual, en el que el desarrollo de la IA debe reflejarse en principios y regulaciones que protejan a las personas y a los entornos naturales.

Este documento fue firmado por la Academia Pontificia por la Vida, Microsoft, IBM, FAO y el Gobierno italiano. En fechas posteriores adhirieron al texto el Parlamento Europeo, así como representantes de las religiones abrahámicas, compartiendo el ideario de establecer una ética al servicio de cada persona en su totalidad y de todas las personas sin discriminaciones ni exclusiones. Los principios estructurales son: transparencia, inclusión, responsabilidad, imparcialidad, seguridad y privacidad. [5]

e.2. Ética en la era de las tecnologías disruptivas. Una hoja de ruta operativa. Este texto de marzo de 2023 es el fruto de la colaboración entre el Dicasterio de Cultura y Educación junto con el Instituto para la tecnología, la ética y cultura (ITEC), el Markkula Center y la Universidad de Santa Clara (California).

Proporciona marcos y conceptos éticos para guiar el uso responsable de la IA, así como una serie de principios y encuadres para llevar adelante proyectos de una IA ética y sin daños. Entre esos principios destacan: a) respeto a la dignidad y los derechos humanos; b) promover el bienestar humano; c) preservar a la humanidad; d) promover la justicia, libre acceso, diversidad, equidad y la inclusión; e) responsabilidad por el uso de la IA; f) promover la transparencia y la explicabilidad de los sistemas de IA.[6]

---

[5] Pérez, M. " Hacia una nueva algor-ética. A propósito del mensaje de Su Santidad Francisco para la celebración de la 57ª Jornada Mundial de la Paz. El Derecho. Suplemento Derecho, Innovación y Desarrollo Sustentable, nro. 17, 2024. Cita digital ED-V-CCCXLIX-709.

[6] Dicasterio de Cultura y Educación, Instituto para la tecnología, la ética y cultura (ITEC), el Markkula Center y la Universidad de Santa Clara (California*). Ethics in the Age of Disruptive Technologies. An Operational Roadmap. Flahaux,* J.; Gren, B.; Skeet, A. editores, Santa Clara, California, junio 2024.

f) Disposición 2/ 2023 de la Subsecretaría de Tecnologías de la Información. Recomendaciones para una Inteligencia Artificial fiable.

Propone la gestión de los riesgos desde el diseño del producto a los fines de no introducir sesgos desde su concepción. Aboga por un acta de compromiso ético en que los modelos de entrenamiento deban ser transparentes y explicables. [7]

Se expone aquí una breve síntesis de la pluralidad de instrumentos existentes como muestra para establecer patrones comunes a todas ellas: a) Centralidad humana; b) necesidad de gestionar riesgos; c) evitar daños; d) transparencia desde el diseño del sistema, lo que incluye la algorítmica; e) respeto de las instituciones democráticas y de los derechos y libertades fundamentales; f) trazabilidad, información y explicabilidad de los sistemas como garantía para los consumidores y usuarios.

En el mientras tanto, nuestro sistema jurídico es un derecho vivo aplicable a estas nuevas situaciones.

3. EN BÚSQUEDA DE UNA RESPONSABILIDAD POR DAÑOS CAUSADOS POR SISTEMAS BASADOS EN IA

En las XXVII Jornadas Nacionales de Derecho Civil del 2017, en las conclusiones de la Comisión 3 Derecho de Daños, se establecieron algunas pautas a tomar en cuenta para el análisis de la responsabilidad por los daños ocasionados por sistemas basados en IA.

El punto de partida se halla en el art. 1757 del CCC en el que se establece que una actividad es riesgosa por su naturaleza, por los medios empleados o por las circunstancias de su realización pareciera una significativa probabilidad de riesgo o peligro para terceros ponderable en el marco de la causalidad adecuada.

---

[7] Para una ampliación del tema: Pérez, M. " Cápsula Comentario: En búsqueda de una regulación de la IA. Recomendaciones para una Inteligencia Artificial fiable. Análisis preliminar de la Disposición 2/ 2023 de la Subsecretaría de Tecnologías de la Información". El Derecho, Suplemento Derecho, Innovación y Desarrollo Sustentable, Nº 13, Junio 2023, Cita digital ED -IV-CDXCI-47, 23/06/2023.

Dentro del elenco de actividades riesgos, las conclusiones refieren a la utilización de algoritmos, actividades cibernéticas, plataformas digitales y sistemas operados por IA.

El anclaje se encuentra en la protección del daño injusto, que impone en forma prioritaria medidas tendientes a evitar la producción o mitigación dañosa en el desarrollo de actividades riesgosas o peligrosas de acuerdo a lo establecido en los arts. 1710 y sigs. CCC, art. 43 de la CN, así como en los arts. 9,10,1770 y concordantes del CCC.

Este marco normativo tiene su esencia en la necesaria interpretación dúctil, abierta, genérica y flexible de acuerdo al espíritu dinámico del CCC y de su sistema de derecho de daños. [8]

En esta línea de una responsabilidad objetiva para las actividades vinculadas a algoritmos e IA, son las Conclusiones a las que se arribaron en las XXVIII Jornadas Nacionales de Derecho Civil por las que la función preventiva abarca tanto los principios de prevención como el de precaución. En lo que respecta al principio de precaución se insiste en su aplicación extensiva e incorporación expresa a la legislación civil.

En lo que refiere a los riesgos de desarrollo, la función preventiva del derecho de daños es una herramienta útil a los fines de evitar el agravamiento o continuación del daño. [9]

Estas conclusiones de las jornadas, contribuyen a la reflexión acerca de la eficacia ante la eventual causación de daños en miras a la atribución de responsabilidades entre directores, desarrolladores y participantes en los proyectos, así como los superiores jerárquicos o los financiadores. Si pensamos en el desarrollo de la IA como una actividad riesgosa o peligrosa, el criterio de atribución objetivo desplaza al criterio subjetivo y compartirían una responsabilidad concurrente salvo que se acuerde o regule una responsabilidad solidaria.

---

[8] XXVII Jornadas Nacionales de Derecho Civil. Conclusiones Comisión 3. Disponible en https://www.fcjs.unl.edu.ar/jndc-2019/, consultado el 05/07/2024.

[9] XXVIII Jornadas Nacionales de Derecho Civil. Conclusiones Comisión 3. Derecho de Daños.https://mendozalegal.com/omeka/files/original/138acaaf234b7670b133d2405fd254d7.pdf, consultado el 03/07/2024.

4. ¿POR QUÉ ES NECESARIO APLICAR EL PRINCIPIO DE PRECAUCIÓN EN LOS SISTEMAS BASADOS EN IA?

En el devenir cotidiano se advierte la existencia de una existencia de una incertidumbre científica y jurídica sobre el modo en que evolucionarán los modelos fundacionales, tanto en lo que se refiere a la tipología de los modelos como a su posibilidad de autodeterminación.

Esa incertidumbre científica y jurídica se traduce en diferentes niveles de riesgo sobre a lo largo de todo el ciclo de utilidad del sistema. Estas áreas tan sensibles como seguridad, privacidad, salud o protección de las personas humanas y el medio ambiente, entre muchas otras requieren de marcos éticos y normativos de manera que se concilie el necesario y útil progreso con la protección de la persona humana y el planeta, así como un uso que permita la convivencia pacífica entre los pueblos.

Todas estas cuestiones parecen bastante utópicas a la luz de los acontecimientos por los que estamos atravesando en un abanico amplio entre las noticias falsas o manipuladas, así como los drones autónomos que tienen un error de cálculo y bombardean aldeas con inocentes, pero ¡ah!, es un error de cálculo y las víctimas son previsibles.

Es así como se hace necesario que, en los procesos de toma de decisiones, la gobernanza en materia de IA se torna en el eje del control de la incertidumbre y los riesgos de la actividad que pueden derivar en daños de carácter masivo no siempre mensurables.

En esa línea de gobernanza, el principio de precaución es un medio para propiciar una innovación tecnológica más segura, más transparente y menguar o evitar posibles impactos dañosos. Por otro lado, como principio protectorio de la persona humana,[10] permite una mayor y mejor protección de los sectores vulnerables, buscando el desarrollo de una de una IA inclusiva y deliberativa, no como una mera declamación política sino como instrumento para la gestión de riesgos tales como los sesgos de discriminación negativa, el evitar falsos positivos o negativos en los procesos de toma de decisiones automatizadas, para articular políticas de seguridad, salud y educación en las que los sistemas biométricos o la

[10] Cossari, M. *El principio precautorio como principio general para la protección de la persona humana. Editorial El Derecho, Buenos Aires, 2017.*

biometría aplicada a la morfología y/o emociones humanas sirvan a la sociedad.

Contribuye, además, a balancear los intereses de las grandes corporaciones o empresarios que, en su carrera por dominar un mercado de datos, en muchos casos se valen del suministro de datos, informaciones o procesos poco transparentes que conculcan derechos y garantías constitucionales.

La existencia de la incertidumbre científica y esta probabilidad dañosa, permite a los Estados establecer un régimen anticipatorio de daños y, por tanto, la determinación de la ulterior responsabilidad de los desarrolladores del algoritmo (y los sistemas de IA) ante esta probabilidad causal entre la génesis y el daño.

Este principio se potencia con la esencial transparencia de los procesos de tomas de decisiones en procura de evitar el fenómeno de cajas negras, de la opacidad algorítmica o el uso de datos tratados de una manera indebida.

Fortalecer el deber-derecho de información involucra tanto al sector público como el privado en el desarrollo de estas tecnologías, lo que de manera indirecta contribuye a la gestión de certezas y darles relevancia a cuestiones relacionadas con el impacto ambiental, la protección de la propiedad intelectual, modificar los procesos de entrenamiento de los modelos ante la posibilidad de errores fácticos, inconsistencias, sesgos o engaños al usuario.

5. INTELIGENCIA ARTIFICIAL ¿ UN POSIBLE RIESGO DE DESARROLLO?

La IA puede ser analizada como un sistema de procesos concatenados de carácter diverso y con alcances e implicancias que se mueven en el ámbito de la anticipación (gestión de riesgos) y la reparación (arts. 1757, 1758 del CCC). También, desde la perspectiva del estudio de su diseño, de los algoritmos, de los algoritmos automatizados, así como en el análisis de los procesos de tomas de decisiones donde se presentan fenómenos como las cajas negras, sesgos u errores que buscan ser “atribuidos” al sistema.

Desde la experiencia, daños de carácter masivo e irreparable como los escándalos de la talidomida o la droga DES, el consumo de tabaco o la utilización de metales pesados o radioactivos en la industria o la

alimentación, entre muchos otros, fueron el punto de partida para el análisis de la existencia de los llamados riesgos de desarrollo o del progreso.

En posiciones antagónicas o eclécticas, todas las teorías se centran en los productos elaborados, en su diseño y puesta en circulación o su trazabilidad, tienen un denominador común que es la causación de daños que se prolongan en el tiempo, donde no siempre se conoce su procedencia porque el estado de los conocimientos al momento de su entrada en el mercado no permitía percibir tal posibilidad dañosa o se la obvió o se la ocultó.

Los sistemas de IA o los algoritmos sean desde su programación o en los procesos de toma de decisiones automatizadas comparten estas características. Las grandes preocupaciones que planean en las distintas propuestas están dadas en cómo se pueden conculcar derechos y garantías, cómo se pueden causar daños de manera imperceptible o silenciosa, como muchos daños se van manifestando ahora, pero se desconocen a futuro. Preocupaciones que generan desafíos y tienen en la mira el largo plazo y la protección de los sectores más vulnerables.

Los riesgos de desarrollo son la contracara del espejo del principio de precaución. O más claro aún, cuando se habla de una responsabilidad basada en riesgos de desarrollo es hablar del fracaso del principio precautorio que de manera necesaria exige actuación en contextos de incertidumbre. [11]

Uno de los retos de estas tecnologías 4.0 es colocar al legislador en la necesidad de vertebrar un esquema de responsabilidad basado en la determinación del estado de la ciencia y de los conocimientos al momento del desarrollo algorítmico y de los modelos en ellos basados, la inclusión de los riesgos de desarrollo de forma expresa en la normativa de protección de los consumidores, así como en las normas de protección de datos personales.

[11] Pérez Álvarez, M. *El principio de precaución y los riesgos de desarrollo. La incertidumbre científica y la toma de decisiones jurídicas*. Editorial El Derecho, Buenos Aires, 2024, págs. 287 a 349.

EL ROL DE LA FUNCIÓN PREVENTIVA ANTE LA PREGUNTA POR LA RESPONSABILIDAD CIVIL DE LA INTELIGENCIA ARTIFICIAL

Por María Constanza Quiñones[1]

I. CONCLUSIONES

1. La función preventiva de la responsabilidad civil cumple un rol esencial en la evolución y el lanzamiento de las nuevas tecnologías, en la medida de que mantiene su eje en la protección de la persona humana, como centro de imputación de las normas del ordenamiento jurídico, ante el constante avance de esta tecnología considerada especialmente riesgosa.

2. La diferencia fundamental entre el principio de prevención y el principio de precaución radica en la falta de conocimiento científico en el acaecimiento del daño, y el nexo de causalidad entre el daño y la falla de la tecnología.

3. Si bien la inteligencia artificial se caracteriza por su ser imprevisible, esta característica no coincide con aquella del principio de precaución, en virtud de que la complejidad por hallar la causa del daño es resuelta por nuestro Código Civil y Comercial por medio de la teoría del riesgo creado.

4. La característica de su ser autónomo de la inteligencia artificial no coincide con aquel del desconocimiento de los posibles efectos o actos que pueden acaecer propios del principio de precaución, en virtud de que esa autonomía responde a una programación específica, donde el creador de la inteligencia artificial la programa para actuar de tal o cual modo.

5. Una vez lanzada al mercado, la inteligencia artificial no se escapa de la programación de su creador, quien puede configurarla de manera de que no de determinados resultados, o bien, no pueda responder a determinadas solicitudes por parte del usuario.

---

[1] Abogada graduada con honores de la Universidad Austral (UA). Maestranda en Derecho Empresario (UA). Coordinadora académica de la Maestría en Derecho Empresario Global (UA). Ayudante Diplomada en las cátedras de Derecho Privado I, Derecho de las Obligaciones, Derecho de Daños y Derechos Reales (UA).

La presente ponencia la avala el Dr. Ignacio E. Alterini.

6. La prohibición de la inteligencia artificial no es una medida adecuada y razonable, cuando el creador, desarrollador y comercializador ha realizado todas las pruebas posibles para asegurar un lanzamiento seguro al mercado.

7. La función preventiva cumple un rol esencial a la hora de determinar los costos y los incentivos para la realización de esta actividad de desarrollo de la nueva tecnología.

II. FUNDAMENTOS

1. INTRODUCCIÓN.

La modernidad nos demuestra todos los días que el ser humano ha revolucionado la tecnología, y que la tecnología ha revolucionado al ser humano. En el contexto actual de la cuarta Revolución Industrial, la Inteligencia Artificial (en adelante, IA) se presenta como una de sus protagonistas. Como tal, la misma comienza a ser aplicada en diversas áreas de nuestra cotidianeidad, como el transporte, la educación, la medicina, y en procesos de elaboración y fabricación. Lo cierto es que su omnipresencia en nuestra Sociedad, es cada vez mayor.

Si bien su desarrollo ha traído grandes beneficios, también debemos ser cuidadosos en su uso y su impacto en la Sociedad, en virtud de que del uso de la IA, se deriva la posibilidad de la producción de daños.

Se trata de una tecnología sujeta a un cambio y desarrollo constante, por lo que tenemos que analizar cuál es el rol del Derecho, y el rol protagónico que cumple a la hora de buscar la implementación pacífica de la tecnología. Su permisión es sumamente importante, en virtud de los beneficios que la acompañan, empero, en su desarrollo, implementación, comercialización, y uso, se reconoce su potencialidad para causar daños a terceros. En los mares por la búsqueda de una respuesta a las consecuencias jurídicas de los daños derivados de la IA, nos preguntamos por las funciones del sistema de Derecho de Daños del Código Civil y Comercial, y cómo podemos aplicar su normativa en este moderno escenario tecnológico.

Previo a la pregunta por quién responde ante un daño derivado de la IA, nos preguntamos por su prevención, intentando de lograr una aplicación adecuada para evitar lo mejor posible, el escenario resarcitorio. Es de mayor importancia que analicemos la función preventiva del Código Civil y

Comercial, y cómo opera la misma antes de la causación del daño en virtud de que va a tener un mayor impacto sobre los incentivos y precios del ejercicio de esta actividad.

En su aplicación, la función preventiva debe tener cuidado de no volverse nociva para su desarrollo, haciendo imposible su ejercicio. El sistema preventivo será eficiente cuando logre un equilibrio entre la protección del usuario y de los terceros, y a su vez permita el libre desarrollo de la tecnología, dando lugar al ejercicio de la libertad de creación.

2. LA CONTEXTUALIZACIÓN DEL SISTEMA DE DERECHO DE DAÑOS: SUS DOS FUNCIONES.

Dentro del Código Civil y Comercial, contamos con un sistema específico de responsabilidad civil. Poco a poco en el último tiempo, el Derecho de Daños ha adquirido cada vez mayor autonomía e independencia, hasta dictarse como una materia única. Propio de este sistema, es que el mismo cuenta con dos funciones: la función preventiva y la función resarcitoria.

Tradicionalmente, el foco siempre fue puesto en el ámbito de la reparación, dejando a la función preventiva en una zona de penumbra. Poco a poco, la función preventiva fue cobrando reconocimiento, y protagonismo. Así, se "fortalece la idea que la anticipación de los daños debe ser tratada no ya como una valoración moral o un principio del derecho, sino como una función en un rango de igualdad con la función resarcitoria y en este sentido se la consagra de manera expresa".[2] Este progreso resulta sumamente positivo, porque para que un ordenamiento jurídico sea eficiente, y suficiente, no se debe limitar a actuar ante el acaecimiento del daño o contingencia, sino que debe llevar a cabo la labor necesaria para evitarlo, y prevenirlo.

El propio legislador reconoció expresamente la importancia del rol de la función preventiva dentro del capítulo de la responsabilidad civil en los fundamentos del Anteproyecto de Código Civil y Comercial de la

[2] Lamanna, Guiñazu, Emiliano y Pérez, Matilde, "El daño jurídico frente a las nuevas tecnologías. Los presupuestos del daño resarcible: remedio antiguo frente a los nuevos daños", El Derecho, Diario, Tomo 289, 2020, p. 6.

Nación, por ser ella una expresión de eficacia para la tutela de los derechos personalísimos y la protección de los bienes colectivos. [3]

Encontrándonos en el marco del estudio de las nuevas tecnologías, donde el desarrollo y la innovación son constantes, nos encontramos en un plano de incertidumbre sobre las nuevas tecnologías que serán lanzadas. Aquí la función preventiva adquiere un rol protagónico, porque nos puede ayudar a enmarcar el contexto de la creación, y a propiamente prevenir el acaecimiento de perjuicios, por medio de la promoción de los cuidados e incentivos apropiados.

Debemos mencionar que nos encontramos ante una actividad especialmente riesgosa, encuadrada dentro del artículo 1757 del Código Civil y Comercial, en virtud de sus características propias, su inteligencia, su autonomía y su imprevisibilidad, que aparejan su potencialidad para provocar daños graves, en tanto atentan contra derechos fundamentales.[4]

Si bien debemos tener cuidado en no frenar el avance de la IA, también debemos pensar en la persona humana, y su calidad como centro de imputación de las normas del ordenamiento jurídico, en tanto en temas de esta índole, "…nos preocupa, una cosmovisión que, centrada en el hombre, le restituya su supremacía y ponga los logros científicos y técnicos al servicio de la sociedad. Es devolverle al ser humano la dignidad de ser el núcleo, el centro y no un mero numero estadístico o un instrumento económico."[5]

Debemos tener en cuenta que la función preventiva no nos permite eliminar el riesgo, pero si nos permite mitigarlo.

Ponemos el foco en esta función, porque a pesar de esa potencialidad para generar contingencias, apareja grandes beneficios que nos importan, por lo que la actividad debe ser permitida en nuestra Sociedad. Así, podemos hablar de las funciones que cumple, como "a) controlar, por ejemplo analizando rápidamente grandes cantidades de datos para detectar anomalías y patrones en las transacciones; b) descubrir, por ejemplo extrayendo

---

[3] Cfr. Krieger, Walter F y Jalil, Julian E., "Responsabilidad civil contractual y extracontractual. Funciones preventiva, resarcitoria, compensatoria y punitiva", Astrea, Buenos Aires, 2021, Edición 1, pp. 11-12.

[4] Cfr. Garrido, Cordobera, Lidia M.R., "Riesgos de desarrollo en el derecho de daños. Tecnología. Masificación. Consumo", Astrea, Buenos Aires, 2016, Edición 1, p. 1.

[5] Garrido, Cordobera, Lidia M.R., "Riesgos de desarrollo en el derecho de daños. Tecnología. Masificación. Consumo", Astrea, Buenos Aires, 2016, Edición 1, p. 3.

información de conjuntos de datos como el vínculo entre genes y enfermedades, y mediante simulaciones; c) predecir, por ejemplo utilizando modelos de previsión para analizar tendencias y hacer predicciones o recomendaciones, como el rendimiento futuro de las cosechas…".[6]

3. ¿PRINCIPIO DE PREVENCIÓN O PRINCIPIO DE PRECAUCIÓN?

Ante los nuevos y constantes avances de la tecnología, se ha comenzado a hablar de la posibilidad de la aplicación del principio de precaución. Se trata de un principio que nació en el siglo XX, y es propio del ámbito del derecho ambiental. Como tal, se sustenta en la función preventiva, buscando neutralizar los riesgos de los daños. Este principio como dimensión dentro de la responsabilidad civil, busca aumentar el deber de diligencia para así asegurar con mayor precisión, la prevención del daño.[7] Se busca que ambos principios se constituyan como puentes de enlace que puedan interactuar ante el sector jurídico que responde al derecho de la Ciencia y de la Técnica.[8]

El primer punto que queremos resaltar, es que prevención y precaución, son dos institutos diferentes, si bien hay autores que las mencionan de manera conjunta, entendiendo que "la racionalidad preventiva solo puede pensarse completa en su ensamblaje con la racionalidad precautoria"[9]. Así, un sector de la doctrina entiende que la función preventiva del Código Civil y Comercial abarca los dos principios, a pesar de no mencionar el principio de precaución en su literalidad. Empero, ambos responden a presupuestos distintos, en tanto la precaución opera cuando "… la relación causal entre una determinada tecnología y el daño temido no ha sido científicamente comprobado de modo pleno". [10] Y la prevención

---

[6] Castro Daniel, y Mclaughlin, Michael, "*Ten ways the precautionary principle undermines progress in AI*", *Information Technology and Innovation Foundation*, Estados Unidos, 2019, p. 4.

[7] Cfr. Cafferatta, Néstor A., "El principio precautorio", TR LALEY AR/DOC/11262/2003, p. 2.

[8] Cfr. García Sedano, Mareclino, "Sobre la autonomía, la creatividad y las consideraciones éticas de la inteligencia artificial en el arte contemporáneo", H-ART Revista de historia, teoría y critica de arte, Colombia, 2022, p. 33.

[9] Bestani, Adriana, "Principio de precaución", Astrea, Buenos Aires, 2012, Edición 1, p. 244.

[10] Andorno, Roberto, "El principio de precaución: un nuevo estándar jurídico para la era tecnológica", TR LALEY AR/DOC/19186/2011, p.8.

responde ante "… un mal que la ciencia puede objetivar y mensurar, o sea que se mueve dentro de las certidumbres de la ciencia"[11].

Vemos así que el punto diferenciador entre una y otra es la certeza o falta de certeza científica en el nexo de causalidad y el acaecimiento del daño. Se entiende que la IA es un supuesto de riesgo dudoso, que es el presupuesto de aplicación del principio precautorio. Y el principio de prevención solo aplica ante supuestos de riesgo actual.

No creo que sea posible aplicar el principio de precaución. En primer lugar, sabemos de antemano, que las notas distintivas de la IA, son su inteligencia, su autonomía, y su imprevisibilidad, las cuales le confieren a la actividad tanto de manera cualitativa como cuantitativa, su carácter de ser especialmente riesgosa. Serán estas notas las que nos ayudarán a argumentar porqué debemos aplicar la función preventiva ante esta temática.

Sí es cierto que en el ámbito de la IA, se habla de la dificultad de determinar el nexo causal, en virtud del desconocimiento del origen de la falla que ha sufrido su programación. De allí que una las características propias de la IA, sea su imprevisibilidad, e incluso se haya observado que su comportamiento parezca la de una caja negra, en tanto desconocemos la operatoria en virtud de la cual el daño fue causado. Si detenemos nuestro análisis aquí, parecería que el principio precautorio aplica con facilidad, empero, no es así.

Aquí el Código Civil y Comercial, resuelve la complejidad sobre la determinación del nexo de causalidad, mediante la aplicación de la teoría del riesgo creado, que propiamente busca resolver las dificultades de determinación de los hechos materialmente causantes del daño. Así, se aplica un criterio de imputación objetiva, siendo su basamento ese riesgo creado que "… postula que toda persona que introduce un riesgo que potencia la probabilidad de causar perjuicios a los bienes materiales o inmateriales del resto de sujetos de la sociedad tiene el deber legal de controlarlos y garantizar que los menoscabos no se concreten o materialicen, ya que si ello sucede deberá de resarcirlos, con absoluta prescindencia de si su actuar fue o no diligente"[12].

---

[11] Cafferatta, Néstor A., "El principio precautorio", TR LALEY AR/DOC/11262/2003, pp. 3-4.

[12] Marcellino, Leonardo, "Actividades riesgosas o peligrosas: posibles respuestas a algunos de los interrogantes que plantea su regulación en el Código Civil y Comercial", TR LALEY AR/DOC/4061/2019, pp. 1-2.

¿Y qué sucede con el análisis de la autonomía? Otro punto que debemos tener en cuenta, es esta segunda nota distintiva. La misma implica que, dependiendo del grado de su autonomía, la IA puede operar sin la intervención del ser humano, de allí que los efectos que pueda llegar a producir, no puedan ser conocidos, por la posibilidad de que se le pueda al usuario 'escapar de sus manos'. Parecería que una vez creada, la IA es liberada en nuestra cotidianeidad, quedando a la merced de su propia programación, que podría hacer algo distinto y ajeno a lo que su creador quiso. Así, este análisis nos deriva en su otra nota distintiva, la de su inteligencia, que simboliza el objetivo de su desarrollador, que es que pueda asemejarse y desplegarse igual que la inteligencia humana.

Si bien es atractiva la posibilidad de crear una tecnología que pueda comportarse y pensar como lo hace una persona humana, no es así el caso de la IA, que siempre va actuar en función de los objetivos que su desarrollador haya insertado en su programación. De esta manera, esa inteligencia, esa autonomía y esa imprevisibilidad, es bien conocida de antemano, y no cabría lugar a que la IA se rebele ante su creador, en virtud de que no posee esa capacidad propia de un ser que posee razón, y libre albedrío. La IA carece de esto, en virtud de que solo va a funcionar en consonancia con su programa de base.

Aquella incertidumbre científica no es propia de la IA, en virtud de que la IA es programada para actuar de determinado modo. Está en su configuración, realizar determinada actividad o no. Si la misma es programada para aprender por medio de la experiencia, en esa programación se puede configurar a la tecnología para que no de determinados resultados, o bien, no pueda responder a lo que su autor no quisiera.

Por lo tanto, ni la imprevisibilidad de la operación de la IA, ni su inteligencia, ni su autonomía alimentan el requisito de la incertidumbre científica propio del principio precautorio. Por lo que no hablamos de un riesgo incierto, sino más bien de un riesgo cierto.

Creo que podemos encontrar la respuesta en la siguiente cita: "La diferencia esencial entre ambos principios radica en la certeza o falta de certeza científica ante la producción del daño… En el principio de prevención ignoramos si, en un caso concreto, el daño va a producirse o no, pero no dudamos de la peligrosidad de una determinada cosa o actividad. Por otro lado, en el principio de precaución todavía existe incertidumbre

científica sobre la relación causal entre una determinada tecnología y el daño que se sospecha fundadamente que puede ocurrir"[13].

Si bien es atractivo el principio precautorio, porque "… incrementa fuertemente el deber de diligencia, instaura una nueva dimensión tutelar en el instituto de la responsabilidad civil: el aseguramiento de riesgos que puede ocasionar efectos calamitosos"[14], el mismo no corresponde con la actividad riesgosa que implica la IA, en cualquiera de los estadios de su Ciclo de vida.

Lo cierto es que el principio precautorio ha sido visto, por un lado, como "…una herramienta que ayuda a científicos, innovadores, responsables políticos, políticos y organizaciones sociales a reflexionar sobre qué tecnologías deben desarrollarse, qué umbral de daño puede permitirse y qué nivel de incertidumbre es aceptable para la sociedad"[15], y por otro lado, ha sido criticado por ser "…vago, incoherente, acientífico, arbitrario"[16].

Incluso, la aplicación del principio precautorio no debería ser una opción, en tanto no es la solución que nos permite llegar a un desarrollo armonioso de las nuevas tecnologías, en tanto el mismo a sido acusado "…de ser irracional y anticientífico, y numerosos autores han afirmado que ahoga la innovación al imponer exigencias poco razonables sobre la seguridad de las nuevas tecnologías".[17]

La adecuada contemplación de lo que antecede, y el reconocimiento del rol del programador, nos permitirá aplicar mejor la función preventiva, los incentivos, y proteger de manera más acabada a la persona humana. Con la aplicación del principio precautorio, desconocemos eso que antecede, desconocemos el funcionamiento propio de la IA, ese rol del creador al

---

[13] Cossari, Maximiliano, "Los daños y perjuicios y el principio de precaución en la jurisprudencia reciente", TR LALEY AR/DOC/874/2008, p. 2. Mientras que el principio de prevención encierra una conducta racional frente a un peligro cierto y mesurable por la ciencia, en el ámbito de la precaucion nos encontramos en un terreno de incertidumbres.

[14] Cafferatta, Néstor A, "El principio precautorio", TR LALEY AR/DOC/11262/2003, p. 2.

[15] De Smedt, Kristel y Vos, Ellen, "*The application of the Precautionary Principle in the EU*" en Mieg, Herald A. (editor),"*The Responsibility of Science*", Springer, Volumen 57, Alemania, 2022, p. 164.

[16] Ibid, p. 164.

[17] Hansson, Sven Ove, "*How extreme is the precuationary principle" en "Nanoethics: studies of new and emerging technologies*", Springer, Volumen 14, 2020, p. 2.

momento de programarla, y entonces, ¿qué protección le estamos brindando a la persona? Pareciera que el principio de precaución implica desconocer el rol que tiene el creador a la hora de programar la IA, que la puede programar para que actúe de tal o cual modo.

Por último, como mencionamos previamente, otra diferencia importante entre ambas, es que la prevención encuentra sustento normativo en el Código Civil y Comercial, mientras que la precaución no. Este último lo podemos encontrar en la Ley General de Ambiente, pero no posee una vocación expansiva hacia otros ámbitos del ordenamiento jurídico.

4. LA FUNCIÓN PREVENTIVA Y EL PRINCIPIO DE INNOVACIÓN

En el año 2023 el Estado de California de los Estados Unidos, decidió prohibir el uso de los robotaxis de la marca Cruise, empresa cuyo objetivo es crear autos con la más avanzada tecnología, que pueden conducir de manera autónoma, sin ningún conductor al mando. Aquella prohibición fue fruto del mal funcionamiento de un robotaxi, donde el "vehículo atropelló a una mujer que había sido previamente arrollada por un conductor humano y se vio lanzada directamente contra el vehículo no tripulado"[18].

¿Fue esta la respuesta indicada por parte de la autoridad automotor? Antes del lanzamiento del vehículo al mercado, la marca cumple con una serie de evaluaciones previas, equipando al vehículo con más de 40 sensores, visiones 360, y es probado por miles de kilómetros.[19] Incluso, la marca dijo que el auto logró reaccionar mejor que lo que lo haría una persona humana.

¿Qué incentivo a la inversión produce esa prohibición, si la marca de manera previa cumplió con los recaudos apropiados para lanzarla?

Así, la función preventiva cumplirá un rol determinante en el sistema de incentivos de la actividad. Según los cumplimientos previos que los desarrolladores, comercializadores, etc., tengan que cumplir, es que se determinaran los costos y los incentivos para su realización.

Es importante el análisis sobre los efectos de la aplicación de la función preventiva, en virtud de que puede ello determinar el grado de desarrollo e inversión en la IA. Así pues, se debe tener en cuenta cuál es el

[18] "San Francisco retira los robotaxis de Cruise tras otro atropello a un peatón" https://www.lavanguardia.com/motor/actualidad/20231025/9326650/san-francisco-retira-robotaxis-cruise-atropello-peaton-pmv.html, Consultada el 13/08/2023

[19] https://getcruise.com, consultada el 13/08/2023

bien jurídico protegido, y la importancia de que la eficacia de la exigibilidad del sistema de protección sea correspondiente al mismo, pero el costo de prevención, no puede ser mayor que el del bien. [20]

Si bien como tal es una actividad riesgosa por su potencialidad para causar daños a la persona, al patrimonio y a los bienes de incidencia colectiva, es una actividad que por los beneficios que apareja, es permitida, y debe ser así. Por ello el rol que cumple la función preventiva, no puede ser absoluto. El uso y la integración de la IA es de suma importancia, en tanto "hay una amplia y diversa gama de usos para la IA. Entre los primeros en adoptarla se encuentran los fabricantes de piezas que utilizan la IA para inventar nuevas aleaciones metálicas para la impresión en 3D; las empresas farmacéuticas que utilizan la IA para descubrir medicamentos que salvan vidas; las empresas mineras que utilizan la IA para predecir la ubicación de yacimientos minerales; las empresas de tarjetas de crédito que utilizan la IA para reducir el fraude; y los agricultores que utilizan la IA para aumentar la automatización. A medida que avance la tecnología, la IA seguirá aportando importantes beneficios a las personas y las sociedades."[21]

De esta manera, hablamos entonces de, por un lado, el rol de la función preventiva, y por otro, el rol de la libertad de creación, del principio de innovación. Resaltamos que "si los responsables políticos quieren que sus naciones obtengan todos los beneficios de la IA, deberían adoptar el principio de innovación para fomentarla…".[22]

Es así que, tenemos que mencionar que la actividad que implica la elaboración de artefactos integrados de IA, y su uso, posee externalidades positivas y negativas. Esas externalidades, refieren a los efectos positivos y negativos que la actividad posee frente a terceros.

Así, esas externalidades son las que venimos trabajando a lo largo del presente escrito. Siendo la externalidad negativa, la potencialidad de

---

[20] Cfr. Krieger, Walt F. y Jallil, Julian, E, "Responsabilidad civil contractual y extracontractual. Funciones preventiva, resarcitoria, compensatoria y punitiva", Astrea, Buenos Aires, 2021, Edición 1, p. 12.

[21] Hansson, Sven Ove, "*Ten ways the precautionary principle undermines progress in AI*", *Information Technology and Innovation Foundation*, Estados Unidos, 2019, p. 5.

[22] Castro Daniel, y Mclaughlin, Michael, "*Ten ways the precautionary principle undermines progress in AI*", *Information Technology and Innovation Foundation*, Estados Unidos, 2019, p. 3.

provocar un daño, y la positiva, todos los beneficios que el uso de la IA apareja.

Según cómo se lleve a cabo la aplicación de las normas del Código Civil y Comercial a estos supuestos, es que se establecerá un sistema de incentivos determinado para el desarrollo de la actividad. Lo importante entonces, es que ese sistema alimente de manera positiva ese sistema de incentivos. Ello en virtud de las externalidades positivas de la actividad.

Precisamos de un escenario donde se puedan internalizar las externalidades y facilitar la cooperación.[23] Se trata de una situación favorecedora no solo para quien sufre el daño, sino también para quien se dedica a la elaboración, desarrollo y uso de estos artefactos, de esta tecnología.

Según Daniel Castro y Michael Mclaughlin, algunas consecuencias de una mala aplicación de las políticas de prevención, son el "…desarrollo de la IA más lento y costoso, menos innovación, IA de menor calidad, menos adopción de la IA, menos crecimiento económico"[24]

Se trata de promover la eficiencia, no tratando de eliminar el riesgo, porque eso no es posible, sino mitigándolo. De manera que se adopte el cuidado que sea tanto suficiente como eficiente. Buscando así, un sistema óptimo de prevención.

Se tratará tanto de poner el foco en el desarrollador, como en el usuario. Hay que tener cuidado de que no se vuelva una actividad poco atractiva, si hay un nivel de prevención muy alto. Esas obligaciones de prevención no pueden significar un ataque total al desarrollo de la tecnología. Se trata de establecer un sistema de compensaciones donde se incentive a las personas a adoptar determinados niveles de cuidado y actividad. Se trata de tener en cuenta el costo social derivado del uso de la IA. [25]

---

[23] Cfr. Stordeur, Eduardo, "Análisis económico del Derecho: Una introducción", Buenos Aires, Abeledo-Perrot, 2011, p. 205-255.

[24] Castro Daniel, y Mclaughlin, Michael, "*Ten ways the precautionary principle undermines progress in AI*", *Information Technology and Innovation Foundation*, 2019, Estados Unidos, pp. 13-15.

[25] Cfr. Stordeur, Eduardo, "Análisis económico del Derecho: Una introducción", Buenos Aires, Abeledo-Perrot, 2011, p. 205-255.

Se trata de encontrar la mayor eficiencia, mediante la aplicación de nuestra normativa, de manera que promueva el desarrollo de esta actividad. No lo tendrá, cuando se ponga sobre el creador un peso incoherente sobre su tarea de prevención, en tanto hará que los costos sean muy altos, y no respete la teoría de Hikks, que dice que los beneficios que genera socialmente una actividad sean mayores que los costos.

¿POR QUÉ LA INTELIGENCIA ARTIFICIAL ES UNA ACTIVIDAD ESPECIALMENTE RIESGOSA?

Por María Constanza Quiñones[1]

I. CONCLUSIONES

Para la consideración de la Inteligencia Artificial como una actividad riesgosa, es necesario llevar a cabo una ponderación rigurosa, en virtud de la cual, pueda ser la misma considerada una actividad especialmente riesgosa.

La Inteligencia Artificial debe ser considerada una actividad especialmente riesgosa en virtud de sus 3 características propias, su autonomía, su inteligencia y su imprevisibilidad. Estas confieren a la nueva tecnología la idoneidad necesaria para quedar alcanzada por el criterio estricto de interpretación propio del instituto objeto de análisis.

En virtud del carácter de su inteligencia, nos encontramos ante la creación del riesgo en la medida de que se busca crear una tecnología cuya programación pueda asemejarse a la inteligencia humana, y aparentar pensar por sí misma.

En virtud del carácter de su autonomía, es que la Inteligencia Artificial encuadra dentro de la teoría del riesgo creado, en la medida de que se trata de una actividad lícita, que logra funcionar por sí misma, en función de su programación para actuar de tal y cual modo. A mayor nivel de autonomía, mayor es la probabilidad de acaecimiento de daños hacia terceros.

En virtud del carácter de su imprevisibilidad, es que resulta de mayor dificultad encontrar el nexo de causalidad entre la falla de la Inteligencia Artificial y el daño. Correspondiendo así la aplicación de la teoría del riesgo creado, propio de la aplicación del instituto de las actividades riesgosas.

---

[1] Abogada graduada con honores de la Universidad Austral (UA). Maestranda en Derecho Empresario (UA). Coordinadora académica de la Maestría en Derecho Empresario Global (UA). Ayudante Diplomada en las cátedras de Derecho Privado I, Derecho de las Obligaciones, Derecho de Daños y Derechos Reales (UA).

La presente ponencia la avala el Dr. Franco Andrés Melchiori.

II. FUNDAMENTOS

1. INTRODUCCIÓN

¿Es posible humanizar la Inteligencia Artificial (en adelante, IA)? Ello mismo pretende la marca Hanson Robotics, por medio de su Robot Sophia, el cual, según la empresa, ha logrado mostrar un profundo compromiso con las personas mediante la manifestación de una conexión emocional cálida e inolvidable.[2]

A lo largo del tiempo, la evolución de la tecnología nos resulta fascinante. El intelecto humano constantemente se desafía a sí mismo, e incluso a su propia imaginación, logrando creaciones deslumbrantes. Así, aparecemos hoy situados en el transcurso de la cuarta Revolución Industrial, protagonizada por las nuevas tecnologías, entre ellas la Inteligencia Artificial.

Desde los comienzos de los tiempos, toda creación del hombre respondía a una necesidad propia de él mismo. Y toda creación estaba destinada a estar a su servicio. Aquí aparece la importancia del rol de la tecnología, que como tal, desde su primera versión rudimentaria, se trató de objetos inanimados cuyas piezas ayudaron al desarrollo de la Sociedad.

Algo propio de este nuevo escenario, es que ya no solo nos encontramos ante la creación de aparatos tecnológicos cuyo fin se encuentra en estar al servicio del hombre, sino que por medio de la IA el ser humano se ha desafiado a crear una nueva tecnología que pueda pensar y actuar por sí misma, y de esta manera saltar del escenario de servicio al escenario de la interacción.

Nos encontramos con una nueva tecnología cuyo avance se centra en la gradual adquisición de rasgos antropomórficos, siendo su objetivo final asemejarse a la persona humana. A medida que la tecnología va logrando este objetivo, surgen diversos interrogantes en el Derecho sobre cuál es la naturaleza jurídica de la IA.

La utilización de la IA, y los resultados propios del *Machine Learning*, y del *Deep Learning*, han demostrado su probabilidad de causar daños en ese escenario que la rodea, con el cual interactúa. Ejemplos de ello

---

[2] https://www.hansonrobotics.com/hanson-ai/, consultado el 09/07/2024.

son "… a) los bugs o errores informativos; b) los sesgos en los algoritmos; y c) la manipulación algorítmica".[3] Y es por ello que es necesario que estudiemos esta nueva tecnología a través de las normas propias del Derecho de Daños del Código Civil y Comercial de la Nación, para así analizar cuál es el instituto de mejor aplicación ante los daños derivados de su uso.

En las Jornadas de Derecho Civil de Santa Fe del 2019, se concluyó que se trata de una actividad riesgosa. En el presente escrito, profundizaremos sobre porqué se trata de tal, y porqué debemos aplicar un criterio estricto a la hora de analizarlo. Por lo tanto, analizaremos porqué las tres notas distintivas de la IA, su inteligencia, autonomía e imprevisibilidad, hacen propio la aplicación del artículo 1757 del Código Civil y Comercial.

El análisis es de mayor importancia, en virtud de que nos encontramos ante una tecnología sujeta a cambio constante, por lo que debemos analizar los criterios tradicionales que nos permitirán responder a la par de la evolución de esta tecnología, para así proteger al damnificado, a la persona humana como centro de imputación del ordenamiento jurídico, y para responder también de manera correspondiente a los conceptos de justicia, seguridad jurídica y bien común.

2. LA APLICACIÓN DEL ARTÍCULO 1757 DEL CÓDIGO CIVIL Y COMERCIAL

El artículo 1757 del Código Civil y Comercial establece que toda persona responde por el daño causado por el riesgo o vicio de las cosas, o de las actividades que sean riesgosas o peligrosas por su naturaleza, por los medios empleados o por las circunstancias de su realización. La responsabilidad es objetiva. No son eximentes la autorización administrativa para el uso de la cosa o la realización de la actividad, ni el cumplimiento de las técnicas de prevención.

En primer lugar, vamos a hablar de actividad riesgosa, y no de cosa riesgosa, en virtud de que la IA no es una bien material, sino en realidad un bien inmaterial, en virtud de que se alimenta y se construye a partir de algoritmos, que, como tales, no tienen consistencia material.

---

[3] Colombo, María Celeste, "¿La utilización de algoritmos es una actividad riesgosa?", TR LALEY AR/DOC/3516/2019, p. 4.

La misma responde al concepto de actividad, en virtud de que se trata de la sumatoria de "…acciones, conductas, operaciones, o trabajos desarrollados por una persona o empresa..."[4], propios del Ciclo de Vida de la IA, que abarca desde su desarrollo hasta su comercialización y uso. De esta manera, involucra "… una complejidad de varias conductas humanas positivas y negativas que combinadas con otros elementos mecánicos o inmateriales en su conjunto conforman organizadamente la actividad"[5]. Vemos cómo podemos englobarla bajo esta definición, en la medida que involucra elementos inmateriales, siendo tal la IA.

Ahora bien, ¿por qué puede ser considerada riesgosa? Para poder encuadrar esta actividad dentro del instituto objeto de análisis, la misma deberá tener una determinada potencialidad para causar daños a terceros. Ello implica que debemos estar ante una actividad que sea especialmente riesgosa, como así lo establecía el Proyecto de Código Civil y Comercial de 1998. Este último calificaba a la actividad riesgosa como una actividad especialmente riesgosa, aquella que llevada a cabo tiene aptitud de causar daños frecuentes o graves.

El actual Código Civil y Comercial omitió este aditamento en la literalidad de la norma, empero, "… de todos modos debe conservar su vigencia a los fines de una correcta interpretación de la actual regulación en la materia"[6]. La aplicación de este criterio implica la aplicación de un criterio estricto para analizar si la actividad es o no riesgosa.

El análisis debe ser realizado ex ante, es decir, previo al acaecimiento del daño, lo cual resulta acertado, en la medida de que el carácter riesgoso de una actividad nunca podría ser juzgado luego del acaecimiento del daño. Debemos realizar de manera previa un juicio abstracto, preguntándonos por la capacidad de la actividad para tener esa potencialidad de riesgo.[7]

---

[4] Enghelmayer, Fernando, "Responsabilidad derivada de ciertas actividades riesgosas o peligrosas en el Código Civil y Comercial de la Nación", TR LALEY AR/DOC/2101/2016, p. 5.

[5] Marcellino, Leonardo, "Actividades riesgosas o peligrosas: posibles respuestas a algunos de los interrogantes que plantea su regulación en el Código Civil y Comercial", TR LALEY AR/DOC/4061/2019, p. 2.

[6] Marcellino, Leonardo, "Actividades riesgosas o peligrosas: posibles respuestas a algunos de los interrogantes que plantea su regulación en el Código Civil y Comercial", TR LALEY AR/DOC/4061/2019, p. 5.

[7] Cfr. Ibid.

Ahora bien, ¿por qué es especialmente riesgosa? Seguidamente, analizaremos porqué la IA queda dentro del estándar estricto de calificación de este instituto. Tenemos que analizar porqué tiene la idoneidad necesaria para que califiquemos sus resultados dañosos como frecuentes, o graves.

3. SU INTELIGENCIA

En primer lugar, nos encontramos con la primera nota distintiva, su **inteligencia**. Para comprender porqué esta primera nota implica un riesgo, tendremos que hablar de dos conceptos puntuales: la inteligencia humana y la inteligencia artificial. Cuando hablamos de la inteligencia humana, podemos citar a Howard Gardner, cuyas investigaciones nos dicen que existen inteligencias múltiples propias del ser humano, como son las inteligencias en lógico-matemática, lingüística-verbal, musical, espacial, interpersonal, intrapersonal e incluso, la inteligencia naturalista, la existencial, la creativa, la emocional y la colaborativa[8]. Así, podemos ver cómo las operaciones de la inteligencia humana resultan de la más diversas áreas, y de la más diversa índole. No se trata solo de una operación matemática, sino que va más allá, alcanzando la creatividad y las emociones de la persona.

En el caso de la IA, centralmente cuando hablamos de inteligencia artificial, la misma trata de "… la capacidad de una máquina o sistema informático de simular y realizar tareas que normalmente requerirían inteligencia humana, como el razonamiento lógico, el aprendizaje y la resolución de problemas".[9] Por medio de ella su creador busca lograr una tecnología que pueda desplegarse ante un problema como lo haría desde su intelecto, una persona humana. Se trata de una programación específica, a partir de la cual la IA por medio de la experiencia logra responder a los planteos que la rodean.

Ello se encuentra estrictamente vinculado con dos ramas de la IA que son el *Machine Learning (ML)* y el *Deep Learning (DL)*, refiriéndose el primero a la posibilidad de la IA de predecir su comportamiento a partir de la información con la cual es programada. El propósito del desarrollo del *ML*

---

[8] Cfr. Gardner, Howard, citado por Falcón, Enrique M, "El derecho artificial", TR LALEY AR/DOC/283/2024, p. 1.

[9] Morandín-Ahuerma, F, "*What is Artificial Intelligence*?" *Int. J. Res. Publ. Rev*., *3*(12), 1947-1951, Enero de 2023, DOI: 10.55248/gengpi.2022.31261, p. 1947.

es lograr una IA que pueda superarse a sí misma por medio de la experiencia, y que a partir de ella y del aprendizaje de esta, pueda incluso responder frente a situaciones para las cuales no fue programada.[10] Para lograrlo, deberá realizar un trabajo interno, que como tal se asemeja al que realiza el intelecto humano. De esta manera, el *ML* "es un método de análisis de datos que automatiza la creación de modelos analíticos. Permite a los ordenadores aprender y mejorar automáticamente a partir de la experiencia sin ser programados explícitamente"[11].

Por otro lado, el *DL,* sub-rama del *ML*, refiere a las diversas arquitecturas de aprendizaje profundo[12], vinculadas con el rol de las Redes Neuronales Artificiales, y la posibilidad de la tecnología de independizarse por completo de la intervención de los humanos[13], por medio del procesamiento de datos por parte de las distintas capas de algoritmos.[14]

---

[10] Cfr. Bonina, Nicolas, "Inteligencia artificial y derecho. ¿Las máquinas van a reemplazar a los abogados?", TR LALEY AR/DOC/3809/2020, p. 6.

[11] Mahyman, Amini y Sharifani, Koosha, "*Machine Learning and Deep Learning: a review of methods and applications*", *World Information technology and Engineering Journal*, Volume 10, Issue 07, 2023, p. 2.

[12] Sabry, Fouad, "*Artificial Neural Networks: Fundamentals and Applications for Decoding the Mysteries of Neural Computation*", One Billion Knowleadgeable, E-book, 2023, p. 114. Las arquitecturas de aprendizaje profundo, como las redes neuronales profundas, las redes de creencias profundas, el aprendizaje profundo por refuerzo, las redes neuronales recurrentes y las redes neuronales convolucionales, se han aplicado a campos como la visión por ordenador, el reconocimiento del habla, el procesamiento del lenguaje natural, la traducción automática, la bioinformática, el diseño de fármacos, el análisis de imágenes médicas, la climatología, la inspección de materiales y los programas de juegos de mesa, donde han producido resultados comparables a los producidos por humanos y, en algunos casos, superiores.

[13] Corvalán, Juan G; Días Dávila, Laura C; y Simari. I, Gerardo, "Inteligencia artificial: bases conceptuales para comprender la revolución de las revoluciones" en el Tratado de Inteligencia Artificial y Derecho Corvalan, Juan G (Director), Thomson Reuters La Ley, Tomo I, Buenos Aires, 2021, p. 57.

[14] Santarelli, Fulvio G, "La madeja de la inteligencia artificial. En busca de la punta del hilo", TR LALEY AR/DOC/2711/2022, p. 5.

Se diferencian la una de la otra, en la medida de que en el ML se recurre al uso de métodos estadísticos, mientras que en el DL se utilizan las redes neuronales para aprender de grandes conjuntos de datos.[15]

Vemos así, cómo la IA es alcanzada por la definición de la actividad, en la medida de que su desarrollo implica un conjunto de conductas, acciones, y elaboraciones para lograr el resultado del sistema tecnológico.

Empero, si bien la IA nos ofrece soluciones a través del lenguaje de la programación, y logra hacernos creer que piensa, dista ello de que la máquina pueda entender el despliegue que realiza como lo haría una persona humana. Como podemos ver en las definiciones previamente analizadas, la IA no es más que una imitación de la inteligencia humana. Es importante que no caigamos en la ilusión de que la máquina piensa, por más elaborada que sea su respuesta.

Lo cierto es que la IA intenta de simular la inteligencia humana, lo que "…no es otra cosa que imitarla, esto es, entrar en el juego de la imitación".[16] Empero, resaltamos que se trata de un intento limitado, en tanto "…la finalidad de imitar el comportamiento humano desde lo cognitivo, y no así, desde lo emocional"[17]. Es así, que si bien la IA puede llevar a cabo operaciones lógicas, nunca podremos llegar a igualar la inteligencia humana con la inteligencia artificial, en la medida de que nunca podrá llevar a cabo un acto de razón, y tampoco, un acto de emoción.

De esta manera, vemos entonces cómo esta primera nota distintiva provoca la idoneidad de la IA para ser considerada riesgosa. Se alimenta el elemento positivo que existe en el instituto de las actividades riesgosas, encontrándonos ante la creación de riesgo, en la medida que se busca crear una tecnología cuya programación pueda asemejarse al de la inteligencia humana, y pueda pensar por sí misma.

---

[15] Cfr. Mahyman, Amini y Sharifani, Koosha. "*Machine Learning and Deep Learning: a review of methods and applications*", *World Information technology and Engineering Journal,* Volumen 10, Issue 07, 2023, p. 1.

[16] Cervera Castellano, Rafael, "El camino hacia el autómata emocional: computación afectiva", STOA, Volumen 9, Número 17, 2018, p. 5.

[17] González Arencibia, Mario y Martinez Cardero, Dagmaris, "Dilemas éticos en el escenario de la inteligencia artificial", Economía y Sociedad, Volumen 25, Número 57, 2020, p. 6.

4. SU AUTONOMÍA

En segundo lugar, precisamos analizar la segunda nota distintiva de la IA, su **autonomía**. Es aquí donde encontraremos un argumento esencial, en la medida de que en virtud de su autonomía, es que la IA como actividad lícita se escapa del control del sujeto que la usa o crea. Al hablar de autonomía, como en el caso de la inteligencia, debemos hacer primero una diferenciación entre la autonomía humana y la autonomía artificial.

En definitiva, cuando hablamos de la autonomía humana, la misma trata de la capacidad de la persona humana de auto determinarse a sí misma, y de poder crear para sí su propio criterio y pensamiento. Hablamos a su vez del rol de la conciencia propia del ser humano. Es su posibilidad de moverse libremente, y actuar en razón de su propio criterio.

¿Podemos trasladar estos conceptos a la autonomía artificial? Una de las características principales de la IA moderna, es su habilidad de operar sin la intervención de un ser humano. Como así sucede con los vehículos autónomos, donde el vehículo es capaz de tomar sus propias decisiones, sin necesidad de operar en virtud de solicitud del conductor, o incluso puede no haber conductor.[18] Así sucede con los robotaxis.

Lo primero que debemos resaltar, es que existen diversos grados de autonomía en la IA. Es de mayor relevancia, en la medida de que a la hora de juzgar, se debe analizar en cada caso en concreto en qué se fundamenta la aplicación de la norma, y así graduar la responsabilidad otorgada al dueño o guardián. No solo ello, sino que será un factor determinante para su calificación como actividad riesgosa, en la medida de que mientras aumenta su autonomía, también aumenta esa potencialidad de la actividad de causar daños a terceros. Respondiendo de esa manera a la teoría de riesgo creado propio del artículo 1757.

Consiguientemente, la autonomía de la IA crece gradualmente ante la mayor sensibilidad de la máquina y la creciente posibilidad de actuar de

---

[18] Cfr. Chesterman, Simon, "*Artificial Intelligence and the problem of autonomy*", Notre Dame Journal on Emerging Technologies (JET), 1 (2), 2020, p. 212. *A key feature of modern artificial intelligence is the ability to operate without human intervention. … it is helpful to distinguish between automated and autonomous activities. Many vehicles have automated functions, such as cruise control which regulates speed. These functions are supervised by the driver, who remains in active control of the vehicle. Autonomous in this context means that the vehicle itself is capable of making decisions without input from the driver-indeed, there may be no driver at all.*

ella de manera independiente ante una mayor variedad de condiciones y factores ambientales, logrando así actuar, razonar y elegir [19]

De esta manera, Fabio Morandín-Ahuerma identifica cuatro grados de autonomía, resultando los mismos los siguientes: reactiva, deliberativa, cognitiva y autónoma[20]. Así pues, nos encontramos con los dos extremos de posibles autonomías, donde aquella IA con una autonomía reactiva, es "…capaz de realizar tareas especificas de manera autónoma, pero no tiene capacidad de recordar eventos pasados ni de anticipar situaciones futuras" y aquella que es autónoma, "es capaz de interactuar de manera autónoma con su entorno, tomar decisiones y aprender de nuevas situaciones, y puede cambiar sus objetivos y estrategias en función de las circunstancias"[21]. Un claro ejemplo de estos últimos son los autos Tesla.

Por otro lado, en la literatura sobre este tema, nos podemos encontrar con otros autores que plantean también su punto de vista sobre los tipos de autonomía existentes. Entre ellos, Abu Rayhan, identifica 5 niveles de autonomía, donde en el nivel 0 nos encontramos con robots que son controlados por completo por los seres humanos, sin capacidades de autonomía, en el nivel 3 los robots pueden operar de manera autónoma en condiciones que fueron definidas de manera previa, pero aun requieren de la intervención de un ser humano para actuar en situaciones inciertas o bien no familiares, y en el nivel 5, tenemos los robots que son completamente

[19] Cfr. Formosa, Paul, "*Robot autonomy vs. human autonomy: social robots, artificial intelligence, and the nature of autonomy"*, Minds and Machines, Springer, 2021. p. 599.

[20] Morandín-Ahuerma, Fabio. (2022), "*What is Artificial Intelligence*?" *Int. J. Res. Publ. Rev*., *3*(12), 1947-1951, Enero de 2023, DOI: 10.55248/gengpi.2022.31261, p. 1947-1950. Deliberativa: tiene la capacidad de planificar y tomar decisiones basándose en información del entorno y en objetivos predeterminados. Puede analizar situaciones y elegir acciones que le permitan cumplir con objetivos específicos, y puede adaptarse a entornos cambiantes utilizando información del pasado y del futuro. Cognitiva: tiene la capacidad de imitar las funciones cognitivas humanas, como el razonamiento, el aprendizaje y la percepción, y puede adaptarse a nuevas situaciones y entornos. Se caracteriza por imitar las funciones cognitivas humanas, como el razonamiento, aprendizaje y la percepción, y por su capacidad de adaptarse a nuevas situaciones y entornos.

[21] Ibid, p. 1950.

autónomos, y pueden tomar decisiones de manera independiente sin la necesidad de que haya intervención humana.[22]

Diversos autores reconocen que esta característica propia de la IA tiene impactos negativos y positivos sobre la autonomía humana. Si bien la búsqueda constante de la antropomorfización de la máquina revela los grandes avances de la tecnología y del intelecto humano, la misma posee importantes implicancias sobre la autonomía humana que tenemos que tener en cuenta. Diversas investigaciones han demostrado que los sistemas de IA pueden socavar o limitar la autonomía humana.[23] La cuestión central está en que si delegamos en la tecnología la toma de decisiones sobre determinados asuntos, o bien la delegación de tareas de nuestro día a día, el ser humano perderá autonomía propia. Lo cierto es que "la creciente deferencia hacia los sistemas algorítmicos en diversos procesos de toma de decisiones plantea la cuestión de si las elecciones de los usuarios pueden considerarse auténticas, y si esta tendencia empobrecerá nuestra capacidad de autodeterminación".[24]

La autonomía humana es propia de la naturaleza del hombre, empero, la misma para su apropiado despliegue depende fuertemente de su aspecto relacional, "el respeto de los demás constituye en parte la autonomía, y lo mismo ocurre con las relaciones con uno mismo: también constituyen otro

---

[22] Cfr. Rayhan, Abu, "*Artificial intelligence in robotics: from automation to autonomous systems*", China Bangla Engineers & Consultants Ltd, 2023, pp. 6-7. "*Autonomy in robotics can be categorized into different levels based on the extent of human involvement and decision-making authority: Level 0: No autonomy – Robots are entirely controlled by humans without any autonomous capabilities; Level 1: Function-specific autonomy – Robots have limited autonomy in specific functions or tasks, but overall control lies with humans; Level 2: Supervised autonomy – Robots can operate autonomously but require human supervision and intervention when faced with challenging situations; Level 3: Conditional autonomy – Robots operate autonomously in predefined conditions but still require human intervention in uncertain or unfamiliar situations; Level 4: High autonomy – Robots can operate autonomously in most situations but may still require human oversight or intervention in exceptional cases; Level 5: Full autonomy – Robots are capable of operating and making decisions independently in any situation without human intervention*"

[23] Laitinien, Arto y Sahlgreen, Otto, "*AI systems and respect for human autonomy*". Frontiers in Artificial Intelligence, volume 4, 2021, p. 2.

[24] Ibid, p. 2. "Increasing deference to algorithmic systems in various decision-making processes raises the question of whether users choices can be regarded as authentic, and whether this tendency will impoverish our capacity for self-determination".

aspecto de la autonomía".[25] Esto se encuentra atado con el hecho de que "...la importancia del respeto o reconocimiento interpersonal está estrechamente ligada al hecho de que los seres humanos nacen como personas meramente autónomas en potencia y necesitan reconocimiento y respeto para desarrollar su capacidad de autodeterminación". [26]

La cuestión es que la autonomía de la IA no es moral, y por lo tanto no puede llevar a cabo el paso de respetar la autonomía del ser humano, ella carece de deberes. Pueden simular que tienen moral, pero no llegan a ser agentes morales. Es por ello que la conciencia de las máquinas solo podría ser posible de tener a consideración, si reducimos toda la experiencia del ser humano al computacionalismo, que comprende a la mente humana simplemente como un centro de tratamiento de información. [27]

Vemos así la importancia de plantear la diferenciación entre la autonomía humana y la autonomía artificial. Hay que tener cuidado de no darle mayor lugar a la autonomía artificial por encima de la autonomía humana. No es bueno que todas las decisiones terminen en manos de ellos. En definitiva, la autonomía de la IA, no es más que esta programada para determinadas áreas, pero no se puede desplegar en cualquier ámbito de la vida. Carece de la posibilidad de desarrollarse como lo hace la autonomía humana, que depende en parte de su relación con otros seres humanos.

5. SU IMPREVISIBILIDAD

Por último, procederemos a analizar la tercera nota distintiva de la IA, su **imprevisibilidad**. Aquí continuamos en línea con los conceptos de ML y DL, en virtud de los cuales el actuar de la IA "…no sigue necesariamente una secuencia de razonamiento que un ser humano pueda prever o deducir de forma lógica".[28] Lo cierto es que los sistemas de IA que

---

[25] Laitinien, Arto y Sahlgreen, Otto, "*AI systems and respect for human autonomy*'', Frontiers in Artificial Intelligence, Volume 4, 2021, p. 4.

[26] Ibid, p. 4. *When others respond by recognizing the person as autonomous and respecting them, a relational aspect of autonomy is formed*.

[27] Walsh, Keneth R; Mahesh, Sathiadev, y Trumbach, Cherie C, "Autonomy in AI Systems: Rationalizing the fears", The Journal of Technology Studies, Volumen 47, Número 1, 2021, p. 40.

[28] Araya Paz, Carlos, "Desafíos legales de la inteligencia artificial en Chile", Revista chilena de derecho y tecnología, Volumen 9, Número 2, 2020, p. 261.

logran aprender por medio del aprendizaje y tomar decisiones 'propias', hacen que su actuar se vuelva imprevisible. Así, puede tomar decisiones que no fueron previstas por su creador, y por ello hablamos de la imprevisibilidad como una de sus notas características.

Esta imprevisibilidad es propia de los objetivos de sus creadores. De hecho, "se están realizando investigaciones para que un robot pueda deducir y anticipar reacciones humanas y su capacidad y flexibilidad para adaptarse y/o tomar decisiones fuera de los planos predeterminados a través de las técnicas de la probabilidad, estadísticas y los patrones"[29]

Nos encontramos en un escenario donde nunca sabremos con precisión qué es lo que va a suceder, como así pasó con los dos ordenadores de Facebook que crearon su propio idioma, donde los mismos lograron optimizar "…el lenguaje en que fueron programados para acelerar la tarea encomendada. Es decir, los ordenadores tomaron una ruta no programada, incomprensible e imprevisible para nuestra especie"[30]

Se vuelve así, una caja negra, donde perdemos la previsibilidad de su actuar, y entonces no resulta explicable su actuar, en virtud del denominado aprendizaje no supervisado, propio de la aplicación de los supuestos de IA basados en mecanismos de *Deep Learning*.[31] Lo que plantea un problema para el análisis de la causalidad, a la hora de preguntarnos por la causa adecuada del daño. Ante la pérdida de control de ella, se dificulta la posibilidad de identificar de dónde proviene la falla. ¿Cómo podemos brindar mayor protección a la víctima en este caso?

Aquella imprevisibilidad, resulta en la imposibilidad de controlar la IA. Si no sabemos cómo se va a comportar, carecemos de la posibilidad de controlarla. Puede tratarse tanto de la imposibilidad de control por parte de

[29] Santos Gonzales, María Jose, "Regulación legal de la robótica y la inteligencia artificial: retos de futuro", Revista jurídica de la Universidad de León, número 4, 2017, pp. 26.

[30] López Baroni, Manuel Jesús, "Las narrativas de la inteligencia artificial", Revista de Bioética y Derecho, Universitat de Barcelona, 2019, pp. 13-14.

[31] Cfr. Melo, Verónica E. "Responsabilidad por daños e inteligencia artificial: ¿vino nuevo en odres viejos?" TR LALEY AR/DOC/1185/2021, p. 3.

las personas a cargo de su supervisión, como de cualquier persona que esté haciendo uso de la misma.[32]

6. CONCLUSIÓN

Podemos ver cómo por medio de una ponderación rigurosa, la IA puede ser calificada bajo el instituto de las actividades riesgosas, activando la aplicación de este capítulo normativo del Código Civil y Comercial. Sus notas distintivas, su inteligencia, autonomía e imprevisibilidad, hacen que el desarrollo y el uso de la IA se vuelva una actividad con aquella potencialidad para causar daños a terceros, que pueden llegar a ser graves, afectando derechos fundamentales, volviéndose así riesgosa desde un punto de vista cualitativo.

Vemos cómo es riesgosa por su naturaleza, en virtud de que "intrínseca y naturalmente, cualesquiera sean las circunstancias en las que se efectué, la actividad conlleva un peligro inmanente"[33]. Se vuelve riesgosa también de manera cuantitativa, donde por medio de un juicio abstracto, vemos que hay un gran número de potenciales damnificados.

---

[32] Cfr. Araya Paz, Carlos, "Desafíos legales de la inteligencia artificial en Chile", Revista chilena de derecho y tecnología, Volumen 9, Numero 2, 2020, p. 261-262.

[33] Enghelmayer, Fernando, "Responsabilidad derivada de ciertas actividades riesgosas o peligrosas en el Código Civil y Comercial de la Nación", TR LALEY AR/DOC/2101/2016, p. 5.

LA IMPUTACIÓN CAUSAL EN LOS DAÑOS DERIVADOS DE LA INTELIGENCIA ARTIFICIAL

Por María Florencia Ramos Martínez[1]

I. CONCLUSIONES

1. Los daños derivados de la IA, provocados por el uso regular, (correcto o incorrecto) pueden ser causalmente atribuibles mediante el criterio de adecuación. Es posible detectar un patrón de regularidad y previsibilidad objetiva.

2. Los daños derivados de la IA, provocados por el desorden o error en el procesamiento de datos, que hacen al funcionamiento irregular del sistema de IA, puede ser debatidos en cuanto al método causal, ello a la luz de la previsibilidad y la pretendida autonomía del algoritmo.

3. No obstante, cabe considerar que el error en el procesamiento de datos, o en la toma de decisiones por parte de los algoritmos que se desvían del objetivo para el cual han sido entrenados, no es una contingencia imprevisible, sino que es parte del dinamismo propio de la autonomía del sistema de IA. Por lo tanto la potencialidad de generar perjuicios es un dato objetivo, pronosticable para el creador, proveedor, diseñador, operador, responsable del despliegue, o cualquier otro sujeto, persona física o jurídica, que pone en el mercado un sistema o modelo de IA, se sirve o lo emplea.

4. Los daños derivados de un erróneo procesamiento de datos o errónea respuesta de salida de los algoritmos por su supuesta autonomía, son imprevisibles en el resultado dañoso concreto, pero son previsibles como parte de un dinamismo dentro de cualquier sistema de IA. Es posible admitir que hay antecedentes fácticos sobre daños producidos por

---

[1] Abogada, Facultad de Derecho y Ciencias Sociales, U.N.C.; Doctora en Derecho y Ciencias Sociales de la Facultad de Derecho U.N.C.; Posdoctora en Derecho Ciencias Sociales de la Facultad de Derecho UNC.; Premio Dr. Roberto Repetto, Academia Nacional de Derecho y Ciencias Sociales de Buenos Aires, año 2021; Profesora Asistente de la asignatura Derecho Privado VII (Derecho de Daños) de la Facultad de Derecho de la U.N.C.; Docente de posgrado en la Facultad de Derecho U.N.C.; Vicedirectora del Centro de Estudios de Derecho de Daños, Facultad de Derecho U.N.C. Ponencia con aval del Prof. Dr. Daniel Pizarro

algoritmos que no responden como se espera conforme a su entrenamiento.

5. La clasificación de los sistemas de IA, en regulaciones normativas, (Reglamento de Inteligencia Artificial, aprobado por el Parlamento Europeo), entre sistemas de alto riesgo y de riesgo sistémico, revela el conocimiento de la virtualidad causal para provocar daños.

6. Los perjuicios económicos, psicológicos y físicos como resultado de un procesamiento de datos erróneos, o de toma de decisiones contrarias al objetivo de entrenamiento, son factibles por ende, previsibles.

7. No habría inconveniente para adjudicar causalidad a su responsable, aun bajo el patrón de la adecuación. La perspectiva de lo previsible exige una ponderación de circunstancias esperables objetivamente que sucedan, lo cual no es incompatible aun cuando el error sea poco frecuente.

8. Puede acudirse a patrones causales de la llamada teoría de la imputación objetiva. El patrón causal del incremento del riesgo permitido, supone establecer normativamente un estándar de potencialidad dañosa aceptable. Ello requiere un consenso previo sobre una base de regularidad, por lo tanto, coincide con la tesis de la adecuación.

9. El riesgo permitido y no permitido deriva del consenso social y legislativo sobre cuáles son los límites al uso de la tecnología. Exige ponderación y un serio replanteo desde una mirada integral que exponga riesgos y beneficios. Se trata de un sinceramiento social respecto del costo que estamos dispuestos a pagar por el uso de la tecnología.

II. FUNDAMENTOS

1. INTRODUCCIÓN

Como se sabe, en la actualidad son numerosos los campos donde la AI, interviene activamente: diagnósticos médicos, recomendaciones de contenido audiovisual o de compras futuras, reconocimiento de texto, predicciones climáticas, identificación de personas u objetos en fotografías o vídeos.

La IA es definida como "la capacidad de las máquinas para usar algoritmos, aprender de los datos y utilizar lo aprendido en la toma de

decisiones tal y como lo haría un ser humano".[2] *El Reglamento de Inteligencia Artificial, aprobado por el Parlamento Europeo*[3]*, en adelante R.E., establece en el Anexo de definiciones,"* A los efectos del presente Reglamento, se entenderá por: 1) «sistema de IA»: un sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales;"

La implementación de algoritmos4 que permiten identificar, reconocer e incluso predecir fenómenos o situaciones complejas, conlleva a su vez un riesgo de daño que no puede ser ignorado y que en numerosas oportunidades logra concretarse.

Se mencionan que los "algoritmos más avanzados, al ser interpretaciones matemáticas de los datos obtenidos, no explican la realidad subyacente que los produce. Los artefactos o robots, que funcionan por medio de los algoritmos, presentan cierto grado de autonomía en su funcionamiento, de impredecibilidad, y también cuentan con la capacidad de causar daño físico, lo que abre una nueva etapa en la interacción entre los seres humanos y la tecnología."[5]

---

[2]AZNAR DOMINGO, Antonio, DOMINGUES VILLARROEL, María P., "La responsabilidad civil derivada del uso de la inteligencia artificial", disponible en: https://elderecho.com/responsabilidad-civil-derivada-uso-inteligencia-artificial

[3] Resolución legislativa del Parlamento Europeo, 13 de marzo de 2024.

[4] Se definen como "un conjunto finito y organizado de instrucciones, que debe satisfacer cierto conjunto de condiciones con la intención de proveer soluciones a un problema; debe ser capaz de ser escrito en un determinado lenguaje; es un procedimiento que es llevado a cabo paso a paso; la acción de cada paso está estrictamente determinada por el algoritmo, la entrada de datos y los resultados obtenidos en pasos previos; cualesquiera que sean los datos de entrada, la ejecución del algoritmo debe terminar después de un número finito de pasos; el comportamiento del algoritmo es físicamente instanciado durante la implementación en la computadora". (Confr. MASSIOTI, Matías, "La insuficiencia de la causalidad como presupuesto de la responsabilidad civil en los daños producidos por la robótica y los sistemas autónomos", disponible en https://www.redalyc.org/journal/4175/417571103009/html/)

[5]MASSIOTI, Matías, "La insuficiencia de la causalidad como presupuesto de la responsabilidad civil en los daños producidos por la robótica y los sistemas autónomos", disponible en: https://www.redalyc.org/journal/4175/417571103009/html/

Uno de los puntos que ofrece mayor complejidad, es el referido al proceso de aprendizaje del algoritmo denominado "entrenamiento, donde la máquina se alimenta con datos sobre eventos pasados para que pueda anticipar eventos futuros…Los algoritmos de aprendizaje automático aprenden y evolucionan según lo que las personas hacen en línea. Sería imposible para los humanos supervisar cada decisión que toma un algoritmo."[6]

Uno de los inconvenientes en este campo radica en la imputación de autoría, ya que como regla no es posible endilgar participación material directa a una persona física o jurídica, ello en base a la pretendida autonomía de los procesos evolutivos de los algoritmos.

2. LA AUTONOMÍA ALGORÍTMICA Y LOS DIFERENTES ESCENARIOS DE DAÑOS CAUSADOS POR LA IA

Los escenarios de daños producidos como consecuencia de la intervención de la IA, son variados.[7]

El R.E. que regula la IA, establece en el art. 5 "Al mismo tiempo, dependiendo de las circunstancias relativas a su aplicación, utilización y nivel de desarrollo tecnológico concretos, la IA puede generar riesgos y menoscabar los intereses públicos y los derechos fundamentales que protege el Derecho de la Unión. Dicho menoscabo puede ser tangible o intangible y abarca los perjuicios físicos, psíquicos, sociales o económicos."

La mentada regulación, en el art. 110, declara que: "Los modelos de IA de uso general pueden plantear riesgos sistémicos, por ejemplo, cualquier efecto negativo real o razonablemente previsible en relación con accidentes graves, perturbaciones de sectores críticos y consecuencias graves para la

[6]MASSIOTI, Matías, "La insuficiencia de la causalidad como presupuesto de la responsabilidad civil en los daños producidos por la robótica y los sistemas autónomos", disponible en: https://www.redalyc.org/journal/4175/417571103009/html/

[7]Como posibles daños cabe mencionarse, aquellos derivados de vehículos autónomos que se basan en la conducción automática sin operador humano. A su vez, dentro de los daños puramente virtuales, se mencionan los derivados de estadísticas y fórmulas predictivas de personas insolventes, que definen categorías de sujetos que no pueden acceder a préstamos bancarios y que por lo tanto se les agrava su estándar de pobreza y exclusión; afectación a privacidad de datos personales la plataforma CHAT-GPT que afecta derechos de autor, entre otros supuestos.

salud y la seguridad públicas, cualquier efecto negativo real o razonablemente previsible sobre los procesos democráticos y la seguridad pública y económica o la difusión de contenidos ilícitos, falsos o discriminatorios. Debe entenderse que los riesgos sistémicos aumentan con las capacidades y el alcance de los modelos, pueden surgir durante todo el ciclo de vida del modelo y se ven influidos por las condiciones de uso indebido, la fiabilidad del modelo, la equidad y la seguridad del modelo, el grado de autonomía del modelo, su acceso a herramientas, modalidades novedosas o combinadas, las estrategias de divulgación y distribución, la posibilidad de eliminar las salvaguardias y otros factores."

Frente a estos escenarios cabe cuestionarse en base a qué paradigma corresponde implementar la atribución de autoría material para la imputación de responsabilidad.

La autonomía aparece como la característica más marcada en el marco de los daños producidos por la intervención de la IA. El R.E. en el art. 12 reconoce que los "sistemas de IA están diseñados para funcionar con distintos niveles de autonomía, lo que significa que pueden actuar con cierto grado de independencia con respecto a la actuación humana y tienen ciertas capacidades para funcionar sin intervención humana."

En el caso de daños derivados de la intervención de robots, es posible considerar que la responsabilidad de los fabricantes, aunque también cabe cuestionar la incidencia causal de las conductas de los usuarios, propietarios, poseedores y operadores. A su vez, está también latente la responsabilidad de los programadores y desarrolladores de softwares.

Como puede apreciarse el problema de la atribución de autoría, presupone solucionar el dilema causal y particularmente, del método mediante el cual formular el juicio conector entre el antecedente y el consecuente.[8]

[8] En este sentido se señala que las "dudas doctrinales se centran en la dificultad de determinar a quién se le puede imputar la responsabilidad por los daños causados por el comportamiento impredecible del robot; esto es, por las acciones que este despliegue de forma autónoma, independiente de su creador o entrenador, más allá de las instrucciones, en forma de algoritmos, incorporadas a su software."8 (Confr. ZURITA MARTÍN, Isabel, La responsabilidad civil por los daños causados por los robots inteligentes como productos defectuosos, Reus, Madrid, 2020., p. 31)

3. LA AUTORÍA DEL DAÑO. SUJETOS RESPONABLES

En virtud del carácter autónomo de los sistemas de IA, cabe cuestionarse la posibilidad de determinar la autoría del daño respecto de personas físicas o jurídicas.

La Resolución del Parlamento Europeo sobre responsabilidad civil en la IA[9], dispone que "todas las actividades, dispositivos o procesos físicos o virtuales gobernados por sistemas de IA pueden ser técnicamente la causa directa o indirecta de un daño o un perjuicio, pero casi siempre son el resultado de que alguien ha construido o desplegado los sistemas o interferido en ellos" (art. 7). De este modo no es posible desconocer la injerencia de determinados sujetos en el proceso causal del daño producido.

Si bien no hay consenso en la doctrina nacional y de derecho comparado sobre la denominación de los responsables por los daños causados por los sistemas de IA, que el diseñador del modelo, el proveedor o bien el operador, son sujetos que pueden tener incidencia causal con su conducta respecto de los daños, ya por la arquitectura del modelo (diseñador), bien por la puesta en funcionamiento, o por deficiente control (proveedor). Las obligaciones son variadas, supervisión, información, transparencia, actualización de documentación, etc.

La Resolución del Parlamento Europeo con recomendaciones sobre la regulación de la responsabilidad civil en materia de IA[10], establece que el operador inicial es "la persona física o jurídica que define, de forma continuada, las características de la tecnología, proporciona datos y un servicio de apoyo final de base esencial y, por tanto, ejerce también un grado de control sobre un riesgo asociado a la operación y el funcionamiento del sistema de IA; considera que por «ejercicio del control» se entiende cualquier acción del operador que influya en el funcionamiento del sistema de IA y, por consiguiente, en la medida en que expone a terceros a sus potenciales riesgos; considera que esas acciones podrían afectar al funcionamiento de un sistema de IA desde el inicio al fin, al determinar la

[9] Resolución del Parlamento Europeo con recomendaciones destinadas a la Comisión sobre un régimen de Responsabilidad civil en materia de inteligencia artificial (2020/2014(INL)). Texto aprobado, Bruselas 20/10/2020.

[10] Resolución del Parlamento Europeo con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial (2020/2014(INL). Texto aprobado, Bruselas 20/10/2020.

entrada, la salida o los resultados, o podrían cambiar las funciones o procesos específicos dentro del sistema de IA". El operador final es "la persona física o jurídica que ejerce un grado de control sobre un riesgo asociado a la operación y el funcionamiento del sistema de IA y se beneficia de su funcionamiento"[11]

Asimismo, reconoce que "podrían darse situaciones en las que haya más de un operador, por ejemplo, un operador final y un operador inicial; considera que, en ese caso, todos los operadores deben ser responsables civiles solidarios, aunque teniendo al mismo tiempo derecho a reclamar en la vía de regreso unos de otros de forma proporcional"[12]

Por otra parte, el R.E. de IA, se refiere al proveedor como aquella "persona física o jurídica o autoridad, órgano u organismo de otra índole públicos que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca comercial, previo pago o gratuitamente".

El mentado reglamento, establece en el art. 13 que el "concepto de «responsable del despliegue» a que hace referencia el presente Reglamento debe interpretarse como cualquier persona física o jurídica, incluida cualquier autoridad, órgano u organismo de otra índole públicos, que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional. Dependiendo del tipo de sistema de IA, el uso del sistema puede afectar a personas distintas del responsable del despliegue".

En el art. 91, el R.E. determina que "…los responsables del despliegue deben adoptar las medidas técnicas y organizativas adecuadas para garantizar que utilizan los sistemas de IA de alto riesgo conforme a las instrucciones de uso... Asimismo, los responsables del despliegue deben garantizar que las personas encargadas de poner en práctica las instrucciones de uso y la supervisión humana establecidas en el presente Reglamento

[11] Resolución del Parlamento Europeo con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial (2020/2014(INL), n° 12

[12] Resolución del Parlamento Europeo con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial (2020/2014(INL), n° 13

tengan las competencias necesarias, en particular un nivel adecuado de alfabetización, formación y autoridad en materia de IA para desempeñar adecuadamente dichas tareas."

Por su parte, el art. 93 de dicha normativa, destaca el rol del responsable del despliegue en la protección de los derechos fundamentales. Finalmente, el art. 101 del mismo cuerpo legal, señala: "Los proveedores de modelos de IA de uso general tienen una función y una responsabilidad particulares a lo largo de la cadena de valor de la IA,", obligaciones vinculadas a la transparencia, elaborar documentación y mantenerla actualizada, facilitar información de uso general del sistema de IA, entre otras." Los arts. 53 y 55 del R.E. contemplan deberes de los proveedores.

La determinación de obligaciones, revelan un juicio causal implícito sobre la necesidad de las acciones esperables a los fines de impedir o minimizar los daños.

4. DESAFÍOS DE LA CAUSALIDAD ADECUADA FRENTE A DAÑOS DERIVADOS DE LA IA

Como se sabe, el régimen causal establecido por el art. 1726 y sgts. del C.C. y C.N., reconoce la tesis de la adecuación como método para determinar la conexión causal entre conducta antecedente y daño consecuente.[13]

Ello supone comprobar la regularidad[14] y la previsibilidad objetiva. En este contexto, se objeta que, precisamente por la dinámica asociada a la regularidad, la tesis de la adecuación deviene insuficiente para procesos excepcionales[15].

---

[13] Art. 1726 "Son reparables las consecuencias dañosas que tienen nexo adecuado de causalidad con el hecho productor del daño."

[14] Como se sabe, la aludida tesitura exige una ponderación de hechos que guarden similitud en su desarrollo a los fines de permitir un encuadre fáctico en una determinada clase de **conductas**, de las cuales, a su vez, pueda inferirse la asociación con respecto a un determinado efecto. (Confr. ACCIARRI, Hugo A., La relación de causalidad y las funciones del derecho de daños, Reparación, prevención, minimización de costos sociales, Buenos Aires, Abeledo-Perrot, 2009, p. 94)

[15] FIERRO, Guillermo J., Causalidad e imputación, Buenos Aires, Astrea, 2002, p. 240

Frente a este panorama corresponde cuestionarse: ¿El régimen causal contemplado en el art. 1726 y sgts., resulta aplicable a supuestos de daños derivados de la IA?

En relación a ello podemos detectar dos áreas de análisis. Un primer supuesto, donde los perjuicios se derivan de un uso regular del sistema de IA. Los daños se producen en el cumplimiento del objetivo primario, tal como sucede en aquellos casos de perfilamiento económico para predecir acceso a préstamos u otras operatorias bancarias. Allí la discriminación y la vulneración de derechos fundamentales, deviene como consecuencia directa de la implementación del sistema de IA. La respuesta del algoritmo es coherente con la finalidad para la cual ha sido creado. Puede ingresar en este campo, daños que sin ser objetivo primario del sistema, se consideran una respuesta posible en el desarrollo del procesamiento de datos, tal lo que sucede en la violación de derechos de propiedad intelectual. No son modelos creados para vulnerar derechos intelectuales, no obstante ello, por el dinamismo de sus algoritmos, son funcionales a tal fin. [16] De alguna manera, luce como probable que el daño suceda, aunque no sea directamente querido por el modelo.[17]

Un segundo ámbito de análisis, es el de daños producidos por un funcionamiento erróneo, atribuible a la autonomía de los algoritmos. Los perjuicios causados escaparían a toda posibilidad de ser predecibles. La causa del daño sería el comportamiento del algoritmo que, en su proceso evolutivo o de entrenamiento, ha se ha desviado del objetivo para el cual fue entrenado.

---

[16] Aplicaciones como CHAT-GPT ha estado en el foco de la regulación del Parlamento Europeo para exigir transparencia y resguardo de los derechos de propiedad intelectual. El art. 105 del R.E., dispone que "Todo uso de del contenidos protegidos por derechos de autor requiere la autorización del titular de los derechos de que se trate", reforzando luego en el art. 106 que "los proveedores de modelos de IA de uso general deben adoptar directrices para el cumplimiento del Derecho de la Unión en materia de derechos de autor y derechos afines, en particular para detectar y cumplir las reservas de derechos expresadas por los titulares de derechos"

[17] El R.E., reconoce estos sistemas "los grandes modelos generativos, capaces de generar texto, imágenes y otros contenidos, presentan unas oportunidades de innovación únicas, pero también representan un desafío para los artistas, autores y demás creadores y para la manera en que se crea, distribuye, utiliza y consume su contenido creativo. El desarrollo y el entrenamiento de estos modelos requiere acceder a grandes cantidades de texto, imágenes, vídeos y otros datos.", lo que pone en riesgo la propiedad intelectual. (Art. 105)

En el primer caso, son aplicables las reglas de la responsabilidad civil referidas a la atribución causal. No hay impedimento alguno para establecer la determinación de autoría conforme las reglas de la tesis de la adecuación, afirmado en la previsibilidad objetiva de los daños por parte del diseñador, proveedor, o cualquier otro responsable. No habría inconveniente respecto del patrón de lo previsible ya que se trata de un riesgo inherente a la plataforma, red social, aplicación, etc.

La causalidad adecuada, parecería lucir insuficiente frente a los supuestos de daños derivados de la IA, cuando ello se genere a partir del propio proceso evolutivo autónomo del algoritmo. Es posible advertir una suerte de independencia respecto de su diseñador, o bien de su impredecible comportamiento que lo torna imprevisible. Así se menciona como ejemplo, lo sucedido respecto de ciertos supuestos de discriminación por rasgos étnicos.[18] El algoritmo no sigue un patrón lógico sino que su desarrollo obedece a interpretaciones del propio algoritmo al procesar datos de los que se nutre.

En estos casos, si bien el daño específico puede escapar al pronóstico causal, la autonomía del algoritmo y los riesgos que ello conlleva, es conocida o cognoscible por el productor, proveedor o responsable del despliegue. Es posible, aunque dificultoso, la aplicación del método de la adecuación. Cabe admitir criterios causales complementarios.

5. CRITERIOS CAUSALES COMPLEMENTARIOS. LA PROBABILIDAD RAZONABLE. LA IMPUTACIÓN OBJETIVA

La aplicación del modelo estadístico, bajo el paradigma del more probable than not[19], representa un avance en la valoración de la causalidad,

---

[18] Muestra de ello es el caso de discriminación de la aplicación Google Photos (2015), donde personas de rasgos africanos fueron asimilados a gorilas.

[19] Esta regla proveniente del Common Law, se ha proyectado en otros ordenamientos del derecho comparado. En relación a ello se apunta que en "el Common Law goza de gran predicamento la máxima more probable than not, en cuya virtud, basta contar con una probabilidad superior al 50% para concluir que la causa imputable al demandado es plausible de producir el resultado dañoso. La jurisprudencia italiana e inglesa sigue también, con frecuencia, esta orientación probabilística, aunque con distintos criterios en los casos donde no se supera el umbral de certeza necesario para el progreso total de la acción (por ejemplo, 50%, 75%, 90%, etc.); esto es, para un sector, en todos aquellos supuestos en que el umbral de certeza es inferior al estipulado (por ejemplo, 49%, 74%, 89%, etc.), corresponde rechazar el reclamo indemnizatorio; mientras que para otros,

especialmente en supuestos donde se hace evidente la ausencia de certeza causal[20]. Comparte su identidad con la causalidad adecuada, pero le imprime mayor rigor al exigir un estándar o porcentaje de probabilidad afirmado en el aporte científico de ciertas áreas (medicina, ingeniería, etc).

Una variante del patrón de la probabilidad, está dado en función de la razonabilidad. Lo razonable asociado a lo probable, se funda en un juicio de observación y conocimiento sobre lo que es posible que suceda.

El art. 29 del R.E., al referirse a la prohibición de sistemas de IA que tengan por objeto manipular el comportamiento humano, determina que se considera tal, aquel que "provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona o a otra persona o grupo de personas, en particular perjuicios que pueden acumularse a lo largo del tiempo y que, por tanto, deben prohibirse."

Dentro de la denominada teoría de la imputación objetiva, la atribución causal resuelta en base a la noción de "riesgo permitido" propuesta por Roxin, alude a ciertas contingencias adversas que deben ser soportadas asociadas a la normalidad de la vida cotidiana[21]. Siendo ello así, "un resultado será imputable objetivamente cuando se ha realizado en él el

---

corresponde acoger parcialmente la pretensión y resarcir el daño, en proporción a la incidencia causal que la conducta, situación o estado del encartado tuvo en la producción del evento, tomando como límite porcentual un piso del 5% o 10%" (Confr. PREVOT, Juan M., "El problema de la relación de causalidad en el Derecho de la Responsabilidad Civil", Revista Chilena de Derecho Privado, N° 15, dic. 2010, Santiago, 2010, p. 168)

[20] MOSSET ITURRASPE, Jorge, "La relación de causalidad en la responsabilidad extracontractual", Revista Latinoamericana de Derecho, Año I, N° 1, enero-junio 2004, p. 357-380, disponible en: http://historico.juridicas.unam.mx/publica/rev/indice.htm?r=revlad&n=1

[21] La noción de riesgo permitido se constituye a partir de una prohibición, exactamente a partir de la idea de riesgos prohibidos o desaprobados. Los primeros, implican cierta zona de libertad para el agente dañador en la cual la sociedad debe aceptar o tolerar, ya que "no es deber de todos eliminar cualquier riesgo". (Confr. MELCHIORI, Franco A., Las teorías de la causalidad en el daño: Equivalencia de las condiciones, causalidad adecuada e imputación objetiva en la doctrina del Tribunal Supremo, Bosch Editor, Barcelona, 2020

p. 82) "La idea de riesgo permitido, alude a todas las acciones peligrosas que, no obstante serlo, pueden ser emprendidas teniendo en cuenta su utilidad social". (Confr. TERRAGNI, Marco A., "Imputación objetiva", Revista de Derecho de Daños, 2002-3, Rubinzal-Culzoni, Santa Fe, 2002, p. 281 y 282)

riesgo jurídicamente no permitido creado por el autor"[22]. Por lo tanto, un "resultado causado por el agente sólo le es imputable cuando su comportamiento ha creado para el objeto del mismo un riesgo no cubierto por el riesgo permitido, y ese peligro se ha realizado precisamente en el concreto resultado"[23].

La determinación del riesgo permitido, supone un estándar normativo previo de riesgo aceptable y no aceptable. "En los casos de riesgo permitido, la imputación al tipo objetivo requiere la transgresión de un límite de permisibilidad y con ello la creación de un peligro no permitido".[24]

El R.E. establece una clasificación de sistemas de IA, que conllevan mayor riesgo. Así, el art. 54 del establece: "El riesgo de estos resultados sesgados y efectos discriminatorios son especialmente pertinentes por lo que respecta a la edad, la etnia, la raza, el sexo o la discapacidad. Por lo tanto, los sistemas de identificación biométrica remota deben clasificarse como de alto riesgo debido a los riesgos que entrañan."[25]

La determinación de sistemas de IA de alto riesgo conlleva una presunción de probabilidad dañosa, atendiendo a un juicio de ponderación sobre experiencia previa del cual se deduce su alto índice de dañosidad potencial.

---

[22]FIERRO, Guillermo J., Causalidad e imputación, Buenos Aires, Astrea, 2002, p. 382

[23]GARCÍA-RIPOLL MONTIJANO, Martín, Imputación objetiva, causa próxima y alcance de los daños indemnizables, Ed. Comares, Granada, 2008, p. 23

[24] ROXIN, Claus, La imputación objetiva en el derecho penal, (ABANTO VÁZQUEZ, Manuel A., Trac.), 2° Edición, 2° Reimpresión, Ed. Grijley, 2014p. 101

[25] Entre la gran variedad de supuestos, el R.E. menciona expresamente como sistema de alto riesgo aquellos empleados "para evaluar la calificación crediticia o solvencia de las personas físicas, ya que deciden si dichas personas pueden acceder a recursos financieros o servicios esenciales como la vivienda, la electricidad y los servicios de telecomunicaciones. Los sistemas de IA usados con estos fines pueden discriminar a determinadas personas o grupos y perpetuar patrones históricos de discriminación, como por motivos de origen racial o étnico, género, discapacidad, edad u orientación sexual, o generar nuevas formas de discriminación." (art. 58) Igualmente, se señala que "Deben clasificarse como de alto riesgo determinados sistemas de IA destinados a la administración de justicia y los procesos democráticos, dado que pueden tener efectos potencialmente importantes para la democracia, el Estado de Derecho, las libertades individuales y el derecho a la tutela judicial efectiva y a un juez imparcial." (Art. 61)

No caben dudas que los sistemas de IA, particularmente los que se estructuran con mayor nivel de autonomía, resultan altamente riesgosos para usuarios y terceros. A los fines de la imputación causal, cabe dirimir el nivel de riesgo permitido y el prohibido, lo cual configura un desafío pendiente.

LA RESPONSABILIDAD CIVIL FRENTE A LA AUTONOMÍA DE LA INTELIGENCIA ARTIFICIAL: PROPUESTA DE UN FACTOR DE ATRIBUCIÓN OBJETIVO

Por Rodolfo Fabián Rodríguez Rivas[1]

I. CONCLUSIONES

1. Ante la creciente autonomía de los Sistemas Inteligencia Artificial (en adelante IA), surge la necesidad de establecer un factor de atribución objetivo específico para imputar responsabilidad por los daños causados por estos sistemas. Los enfoques tradicionales de responsabilidad, como la culpa o el riesgo creado, resultan inadecuados para abordar los desafíos que plantea la IA debido a su complejidad y autonomía.

2. La propuesta de establecer una categorización de la IA según su nivel de riesgo, como lo sugiere el Parlamento Europeo, puede ser un paso en la dirección correcta. Esto permitiría atribuir responsabilidad de manera objetiva a los operadores de IA de alto riesgo, reconociendo el potencial significativo de causar daños. Por otro lado, se requeriría una diligencia debida por parte de los operadores para eximirlos de responsabilidad en casos de sistemas de IA de bajo riesgo.

3. Es crucial distinguir entre el programador de la IA y el algoritmo mismo, considerado un bien inmaterial. La autonomía de las decisiones del algoritmo y la opacidad inherente de la IA dificultan la asignación de responsabilidad según los modelos tradicionales. Por lo tanto, se propone el concepto de "riesgo autónomo", que reconoce la capacidad de la IA para tomar decisiones independientes y sugiere una forma de responsabilidad objetiva.

---

1 Es profesor adjunto de la catedra de “Obligaciones” y de “Derecho de Daños” de la Universidad Nacional de La Pampa; es especialista en Derecho Civil por la Universidad Nacional de La Plata (febrero de 2003) y en Derecho de la Magistratura Judicial por la Universidad de San Martín (noviembre de 2012). Con posgrados en la Universidad de Buenos Aires: uno en Inteligencia Artificial y Derecho (2020) y otro en Inteligencia Artificial, Consumo, Daños y Seguros (2021). Maestrando en Derecho Civil en la Universidad Nacional de la Provincia de La Pampa. Juez de Cámara Civil, Comercial, Laboral y de Minería en General Pico, La Pampa. frodriguezrivas@gmail.com

4. Este enfoque presume la autonomía de la IA, a menos que se demuestre lo contrario por parte de las partes involucradas. Además, busca adaptarse a la naturaleza única de la IA y proporcionar un marco legal claro para abordar los desafíos emergentes en materia de responsabilidad civil.

5. En resumen, la introducción de la IA plantea la necesidad de repensar los principios tradicionales de responsabilidad civil y desarrollar nuevos enfoques que tengan en cuenta la complejidad y la autonomía de estas tecnologías. La propuesta de un factor de atribución basado en el "riesgo autónomo" puede proporcionar un marco adecuado para abordar estos desafíos y garantizar una asignación justa y eficaz de responsabilidad en casos de daños causados por la IA.

II. FUNDAMENTOS

1. INTRODUCCIÓN

En primer término, he de definir los sistemas de Inteligencia Artificial a fin de poder analizar luego su responsabilidad civil. Entre muchas definiciones, más de 20 sobre la I.A., he elegido la que considero más completa, que es la brindada por el Parlamento Europeo, que dice: *"Se entenderá por sistema de inteligencia artificial a todo sistema basado en programas informáticos o incorporado en dispositivos físicos que muestra un comportamiento que simula la inteligencia, entre otras cosas, mediante la recopilación y el tratamiento de datos, el análisis y la interpretación de su entorno y la actuación, con cierto grado de autonomía, para lograr objetivos específicos"*[2]

Así es que la IA se encuentra presente en la vida cotidiana de las personas, gracias a servicios como YouTube, Spotify o Netflix, también el Chat GPT en sus distintas variantes y empresas. Agentes de bolsa, médicos, *brokers* de seguros, agentes inmobiliarios e incluso, abogados, confían en las herramientas predictivas que funcionan mediante IA para ejecutar tareas altamente especializadas, y hasta creativas. La I.A se

2 (Parlamento Europeo, "Régimen de responsabilidad civil en materia de inteligencia artificial", octubre 2020, disponible en https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_ES.html (consultado el 18/04/2021)

relaciona con las técnicas de *machine learning* (aprendizaje automatizado) y *deep learning*, que utiliza las Redes Neuronales Artificiales[3]. En las décadas por venir, la IA seguirá transformando más campos del actuar humano y traerá enormes avances con relación a la conveniencia, la comodidad y la seguridad; pero, al mismo tiempo, aparejará nuevos desafíos. La proliferación de la IA también provocará consecuencias disvaliosas, como, por ejemplo, entre otras cuestiones, violaciones a la privacidad, discriminación y accidentes causados por IA. El derecho de daños se enfrentará al problema de determinar si el daño causado por una IA puede ser atribuido a título de culpa a alguien o si se trata de un defecto del producto que lo torna inapto para su destino o qué regulación jurídica le corresponderá.

2. DAÑOS CAUSADOS POR I.A.

Hemos visto que los agentes inteligentes resultantes de la aplicación de tecnologías de IA pueden "aprender" y "tomar decisiones" por sí mismos con base en instrucciones algorítmicas con las que se los ha programado. Los sistemas de I.A. en ocasiones no cumplen con su objetivo a pesar de haber sido realizados con el fin de proporcionar soluciones a los problemas humanos.[4] La IA depende de datos humanos, que pueden incluir engaños, lo que plantea el riesgo de que los algoritmos causen daño o engañen.

---

3 En apretada síntesis tratare de describir más importantes sistemas de funcionamiento de la I. A. En primer lugar, debe destacarse al machine learning (aprendizaje automatizado) como el conjunto de técnicas de aprendizaje automático a partir de algoritmos. Estos últimos deben entenderse como una serie metódica de pasos que caben ser empleados para realizar cálculos, resolver problemas y tomar decisiones. En otras palabras, resulta ser la técnica por la cual las máquinas logran su aprendizaje.

El deep learning consiste en un sistema que imita al cerebro humano basado en redes neuronales. Contrariamente a las neuronas humanas, las neuronas artificiales solo procesan valores numéricos y realizan cálculos matemáticos relativamente simples con ellos. Recordemos aquí que toda información que ingresamos en una computadora (sean imágenes, sonido o textos) está digitalizada, esto es, expresada en una inmensa cantidad de números/dígitos (más precisamente unos y ceros).

4 Los daños que pueden causar son habitualmente limitados, aunque ya se han detectado accidentes fatales con automóviles autónomos, errores en la detección de tumores en las exploraciones de ecografías, tomografías o reconocimiento de imágenes y otros poco documentados que son producto de la implementación de programas donde los datos accesibles, disponibles o digitalizados pueden ser escasos y pudieran arrojar falsos negativos o positivos que pueden desembocar en conclusiones erróneas o accidentes de

Los sesgos[5] en los datos de la IA pueden causar daños al introducir prejuicios en el aprendizaje automático en varias fases: la calidad de los datos, la selección de atributos, la contextualización y los circuitos de retroalimentación. Esto puede resultar en decisiones discriminatorias.

Además, los algoritmos crean "burbujas" personalizadas al filtrar contenido según nuestros hábitos en línea, reforzando nuestros sesgos y manipulando nuestro comportamiento de consumo.

Los errores informáticos, o "bugs", ocurren cuando los programas no funcionan como se espera, y en sistemas de aprendizaje automático, los algoritmos opacos actúan como cajas negras, haciendo difícil entender sus decisiones y provocando comportamientos aparentemente ilógicos.

3. LA RESPONSABILIDAD CIVIL EN LA ERA DE LA INTELIGENCIA ARTIFICIAL

a) La Emergencia de un Nuevo Paradigma en la Responsabilidad Civil: De la Culpa a la Objetividad.

La revolución industrial y la sociedad de masas en los siglos XIX y XX provocaron cambios en la responsabilidad civil debido a los daños causados por máquinas y automóviles. Esto evidenció una división entre poderosos y débiles y llevó a contratos predispuestos y a una intervención estatal para buscar equidad. Surgieron doctrinas de responsabilidad objetiva, reevaluando el resarcimiento del daño como un asunto social. Los juristas consideraron varias alternativas, y en Argentina, la reforma del código civil en 1968 consolidó un sistema de responsabilidad equilibrado.

b) La Aparición de Tecnologías Innovadoras y la Inteligencia Artificial (I.A.)

importancia. Es peor aún si estas situaciones problemáticas se producen en la etapa en las que el programa está "aprendiendo" de sus propias conclusiones porque eso conlleva la posibilidad de reconocer información equivocada como base para próximas conclusiones del sistema.

5 Un sesgo cognitivo, en términos excesivamente generales, implica una desviación de la decisión que se entiende como racional, lógica, coherente o consistente con otras decisiones.

El avance tecnológico y la integración de la inteligencia artificial han transformado profundamente la responsabilidad civil. La evolución de la IA, junto con el big data, ha generado un impacto significativo en diversos aspectos de la vida cotidiana, desde negocios hasta interacciones en línea. Estas innovaciones disruptivas desafían los fundamentos clásicos del derecho de daños, cuestionando los modelos de responsabilidad subjetiva y objetiva. En este nuevo contexto, es fundamental adaptarse y desarrollar nuevas competencias para enfrentar los desafíos emergentes y aprovechar las oportunidades que surgen. Esta ponencia abordará tres desarrollos tecnológicos clave y sus implicancias en la responsabilidad por daños.

i. El Internet de las Cosas (IoT, por sus siglas en inglés):

Se refiere a la red de objetos físicos que están equipados con tecnología, como sensores, software y otras tecnologías, con el propósito de conectarse e intercambiar datos con otros dispositivos y sistemas a través de internet. Estos objetos pueden variar desde dispositivos comunes como electrodomésticos y automóviles hasta sistemas industriales y equipos médicos.

ii. Robot

No hay acuerdo entre los ingenieros en qué es un robot; se lo suele definir como un dispositivo autónomo o semiautónomo que realiza sus tareas bajo control humano directo, control parcial y supervisión humana o de forma completamente autónoma. Ahora bien, el robot sin estar dotado de I.A. es una "cosa", por el contrario, un robot con I.A. tiene cierto grado de autonomía, lo marca una diferencia a la hora de analizar su responsabilidad civil. Según la doctrina de García-Prieto Cuesta, un robot es una máquina con cierta complejidad en sus componentes, diseño y comportamiento, que utiliza información sobre su entorno para interactuar con él[6].

Ante ello, surge de la intención de los creadores de materializar la inteligencia artificial en una forma física capaz de interactuar en su entorno. En otras palabras, mientras que la I.A. puede existir sin la necesidad de un

6 GARCÍA-PRIETO CUESTA, JUAN, "¿Qué es un robot?", en BARRIO ANDRÉS, Moisés, Derecho de los Robots. Madrid, Wolters Kluwer, 2018

cuerpo físico, los robots inteligentes dependen de un sistema de inteligencia para funcionar.

Personalidad del Robot: La idea de otorgar personería jurídica electrónica a robots con IA está en etapas iniciales, presentando un desafío para el ordenamiento jurídico. A diferencia de las personas jurídicas tradicionales, que dependen de la acción humana, la IA podría tomar decisiones basadas en su propio aprendizaje, lo que complica la atribución de responsabilidad.[7]

iii. Vehículos autónomos:

Los vehículos autónomos operan sin intervención humana usando sensores, cámaras, radares y algoritmos de IA para navegar y tomar decisiones. Incluyen sistemas de percepción, decisión, control y conectividad para seguridad y eficiencia. Ofrecen beneficios como mayor seguridad y comodidad, pero enfrentan desafíos legales, éticos y de infraestructura antes de su adopción generalizada. Pueden operar en diferentes niveles de autonomía, desde asistencia al conductor hasta autonomía completa.

iv. Chat-GPT

Es un modelo de lenguaje generativo que utiliza la arquitectura de Transformer para comprender y generar texto en lenguaje humano.

En el caso específico del ChatGPT-3, es capaz de generar respuestas en lenguaje natural a partir de las entradas de texto que recibe. Si bien no es exactamente una Red Generativa Adversarial (GAN), su diseño se enfoca en generar texto en función del contexto y las pautas aprendidas durante el entrenamiento. En este sentido, se puede considerar como una especie de red generativa en el contexto de la generación de texto y el procesamiento del lenguaje natural.[8]
ChatGPT-3 es capaz de realizar una amplia variedad de tareas relacionadas

7 En consecuencia, a diferencia de la responsabilidad de las personas jurídicas que siempre será por definición indirecta, resultándole imputable la acción de un tercero por el cual conforme el ordenamiento jurídico debe responder, la responsabilidad de del sujeto de derecho electrónico podría ser directa, tanto en la órbita contractual como extracontractual

8 ROSATI, Florencia - LAMARCA VIDAL, Mariana (2023) • Los retos legales de la inteligencia artificial en ChatGPT. Descifrando el futuro LA LEY 10/05/2023, 1

con el procesamiento del lenguaje natural, como responder preguntas, generar texto coherente, traducir idiomas, redactar contenido y más. Ha sido entrenado en grandes cantidades de datos de texto para aprender patrones lingüísticos y contextuales, lo que le permite generar respuestas coherentes y relevantes en función de las entradas de texto que recibe. (Corvalan Juan G. 2023).

La IA, a diferencia del resto, puede tener cierto nivel de autonomía para tomar decisiones basadas en datos con poca o nula intervención humana. Detrás de las respuestas de ChatGPT no hay personas respondiendo tipo call center. Incluso, la propia empresa aclara que el sistema puede arrojar respuestas que ni siquiera pueden ser explicadas por sus programadores, aunque también el bot nos aclara: "todo lo que "sé" y "digo" "se basa en los datos con los que fui entrenada y las directrices que mis desarrolladores establecieron para mí"[9].

En este contexto, el derecho de daños se encuentra en un terreno complejo y en constante evolución, donde es necesario definir los límites y adaptarse a las nuevas realidades emergentes.

4. DIFERENTES POSTURAS EN MATERIA DE RESPONSABILIDAD CIVIL FRENTE A LA I.A.

En el contexto del avance tecnológico descripto anteriormente, es esencial examinar cómo el derecho argentino está adaptando sus doctrinas para abordar la reparación de los daños causados por la I.A. Diversos argumentos doctrinarios se entrelazan en este ámbito, formando una red de enfoques y posturas que buscan proporcionar soluciones adecuadas. A continuación, se presenta una síntesis breve de estas perspectivas y las dudas que generan:

a) Por el hecho Ajeno

Esta responsabilidad existe en los casos en que la ley asigna a alguien que, sin haber obrado el acto que causa daño, debe indemnizarlo en atención a su particular vinculación con el victimario. En el derecho argentino, el "daño por el hecho ajeno" se refiere a la responsabilidad que una persona o

9 Inteligencia artificial generativa como ChatGPT: ¿Un nuevo Renacimiento? Una explosión de inteligencia humana colectiva a hombros de IA • Corvalán, Juan Gustavo • LA LEY 05/06/2023 , 1 • LA LEY 2023-C , 278

entidad tiene por los daños causados por otra persona que se encuentra bajo su cuidado, supervisión o dependencia. Estamos hablando de una responsabilidad indirecta y objetiva conforme nuestro ordenamiento jurídico (arts. 1753 hasta el 1756, Cód. Civ. y Com.).

Las incógnitas sin responder que se hace la doctrina respecto de este régimen de responsabilidad son: ¿Deberíamos establecer la responsabilidad de una I. A. o de un robot dotado de I.A. en función de las normas de los daños causados por los hijos o en función de los daños causados por los dependientes? ¿Cuál de estos supuestos es más idóneo para responsabilizar al ente artificial? En cualquier caso, ¿la responsabilidad debería recaer en el dueño del robot o en su creador?[10]

b) El riesgo de la cosa y responsabilidad por los Animales.

El Código Civil y Comercial de Argentina (en adelante C.C. y C.) establece una responsabilidad objetiva para el daño causado por cosas, con el dueño y el guardián como responsables concurrentes. Sin embargo, la inteligencia artificial, al ser intangible y no material, no encaja en la definición de "cosa" según el artículo 16. Por lo tanto, los daños causados por IA no puede regular bajo los artículos correspondientes a cosas riesgosas. La autonomía de la IA y su opacidad complican la identificación de responsables y el control. La responsabilidad por daños de animales sigue la misma lógica.

c) Actividad Riesgosa:

El Dr. Jorge Galdós señala que "la actividad riesgosa o peligrosa constituye la conjunción de acciones, conductas, operaciones o trabajos desarrollados por una persona, empresa u organización económica que (aunque no de modo excluyente) puede estar vinculada causalmente con cosas o con conjuntos de cosas (máquinas, herramientas, aparatos, establecimientos, explotaciones etc.) en las que el riesgo (la inminencia de daño) o el peligro (la situación que puede generar daño), para sus propios dependientes o terceros, deriva de tareas, servicios, productos, sustancias o prestaciones que reportan utilidad para la sociedad y generan para sus

10 CORVALAN JUAN G. Tratado de Inteligencia Artificial y Derecho; Tomo III, pag. 326-332; Ed. La Ley año 2021.

dueños o beneficiarios un provecho, generalmente económico. Esa actividad lucrativa asociada con el riesgo o peligro conduce a imputar objetivamente el deber resarcitorio"[11]

Las técnicas de machine learning y deep learning no siempre son inofensivas; de hecho, tienen un considerable potencial para causar daños a terceros, especialmente cuando se emplean algoritmos defectuosos. Dado que estas actividades pueden provocar daños dependiendo de las circunstancias y los elementos utilizados, se pueden consideran actividades riesgosas según el artículo 1757 del C. C. y C.[12]

Esta conclusión fue alcanzada por unanimidad en las XXVII Jornadas Nacionales de Derecho Civil realizadas en el 2019 en la ciudad de Santa Fe. En las conclusiones de la Comisión de Daños sobre "Actividades riesgosas o peligrosas", se subrayó que "la utilización de algoritmos, las actividades cibernéticas, las plataformas digitales y los sistemas operados por inteligencia artificial" pueden incluirse entre las actividades riesgosas.[13]

La crítica que puede efectuarse es que, la teoría del riesgo de la actividad se basa en acciones de la persona humana que implican el uso de bienes materiales y/o el manejo directo de riesgos tangibles. Los algoritmos, especialmente en el machine learning y deep learning, pueden presentar una complejidad que desafía su aplicación directa. La naturaleza opaca de algunos modelos de IA, donde incluso los desarrolladores pueden tener dificultades para explicar el funcionamiento interno de los algoritmos, complica la atribución de responsabilidad en base a la actividad riesgosa.

La teoría del riesgo de la actividad, al ser aplicada al desarrollo algorítmico, enfrenta limitaciones significativas debido a la naturaleza intelectual y técnica del desarrollo de algoritmos, la complejidad y opacidad de la IA, y la rápida evolución del campo tecnológico.

5. PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO

11 GALDÓS, Jorge M., "El art. 1757 del Cód. Civ. y Com. (el anterior art. 1113 Código Civil)", RCyS 2015-IV, 176

12 COLOMBO, María Celeste- "La utilización de algoritmos es una actividad riesgosa?" - LA LEY 2019-F , 678.

13 Conclusiones elaboradas en la Comisión Nº 3 que se encuentran en https://www.fcjs.unl.edu.ar/sitios/ jndc.Pages.showSubcategoria&id=1009

En el derecho comparado observamos que el parlamento europeo durante estos años fue dictando reglamentos y diferentes normativas en relación con la Inteligencia Artificial, también en materia de responsabilidad civil. Independientemente que no posean una aplicación directa en nuestro sistema legal considero importante su mención en apretada síntesis.

Califica a la I.A. según el riesgo que puedan causar:

a) Riesgo Inaceptable:

Prohibición total de la IA que se consideren una amenaza clara para la seguridad, los medios de subsistencia y los derechos de las personas. Ejemplos incluyen sistemas de "puntuación social" por gobiernos y ciertas aplicaciones de vigilancia masiva.

b) Alto riesgo

La responsabilidad de "alto riesgo" se refiere al riesgo considerable de que una I.A. autónoma cause daños o perjuicios a personas de manera impredecible y que exceda las expectativas razonables. La magnitud del potencial depende de la relación entre la gravedad del posible daño o perjuicio, el grado de autonomía de la toma de decisiones, la probabilidad de que el riesgo se materialice y el modo y el contexto en que se utiliza la I.A. Se prevé que, para estos casos, la responsabilidad será objetiva: el operador de una I.A de alto riesgo será objetivamente responsable de cualquier daño o perjuicio causado por una actividad física o virtual, un dispositivo o un proceso gobernado por dicho sistema de IA. Se trata, mediante este factor de atribución, de facilitar la prueba del daño a la víctima cuando este ha sido causado por I.A. de alto riesgo

c) Bajo riesgo

El operador de una I.A. puede evitar la responsabilidad demostrando que tomó medidas razonables para prevenir daños o que realizó acciones diligentes en la selección, puesta en marcha y mantenimiento del sistema. En el debate europeo sobre responsabilidad en tecnologías emergentes, como vehículos autónomos, se cuestiona si la responsabilidad debería recaer en el productor o el operador, dado que el control sobre la tecnología varía y el concepto de "operador" se vuelve crucial.Aunque tanto el control como el beneficio son consideraciones importantes, este último es más difícil de

cuantificar, lo que puede generar incertidumbre en la asignación de responsabilidad.[14]

6. FACTOR DE ATRIBUCIÓN FRENTE A LA IRRUPCIÓN DE LA TECNOLOGÍA

Una vez abordado el avance tecnológico, su tratamiento en la responsabilidad civil en el derecho argentino en sus argumentaciones doctrinarias y una simple síntesis del derecho comparado europeo, es pertinente el examen de uno de los elementos que generan mayor confusión a luz del desarrollo y autonomía de los sistemas I.A., que es el *"Factor de Atribución"*

Una definición muy clara es la brindada por Ramón Daniel Pizarro (2015)[15] que expresa que "El factor de atribución es el elemento axiológico o valorativo en virtud del cual el ordenamiento jurídico dispone la imputación de las consecuencias dañosas del incumplimiento obligacional o de un hecho ilícito stricto sensu a una determinada persona". En este orden de ideas la Dra. Matilde Zabala de González[16] también expresa que "Demostrada la producción de un daño y que este ha sido causado adecuadamente por un sujeto o por persona o cosas a su cargo, todavía es menester enunciar un juicio de valor, que permite determinar si aquel debe o no responder. Si ese juicio es positivo se configura un factor de atribución de la responsabilidad" (Zavala de González, 1999).

Se observa que, en el desarrollo de la I.A., intervienen diferentes sujetos. Por este motivo, al producirse un daño a la persona, al momento de responder, surge el concepto de culpa (factor subjetivo de responsabilidad). Pero, los sistemas de I.A. van creciendo en grados de autonomía de acuerdo con el progreso tecnológico. Ello hace que el concepto de culpa, tal como lo conocemos se diluya, ya que una I.A. no podría, en principio, ser declarada

14 Grupo de Expertos en Responsabilidad y Nuevas Tecnologías es un grupo de expertos independiente creado por la Comisión Europea. Responsabilidad por Inteligencia Artificial y Otras Tecnologías Digitales Emergentes

15 PIZARRO, Ramón Daniel (2015); Tratado de la Responsabilidad Objetiva, La Ley –Buenos Aires.

16 ZAVALA DE GONZALEZ, (1999) Resarcimiento de Daños, Presupuesto y Funciones del Derecho de danos Tomo 4, Nro.53, pág. 355 y ss; Ed. Hammurabi

"culpable" en tanto carece de discernimiento. No obstante, si la víctima quisiera reclamar ante los proveedores, operadores, desarrolladores o usuarios de los sistemas de I.A., las normas basadas en la culpa no son adecuadas para las reclamaciones por los daños causados, ya que los damnificados necesitarán acreditar una acción u omisión ilícita por parte de alguno de los sujetos involucrados. Sin embargo, las características específicas de la I.A., incluidas la complejidad, la autonomía, y la opacidad (el llamado "efecto caja negra") pueden impedir que las víctimas identifiquen a la persona responsable y prueben su "culpabilidad" para obtener una demanda de responsabilidad civil exitosa.

Frente al daño, se debe presumir la autonomía de la I.A. En consecuencia, si se alega por parte del sujeto sindicado como responsable que la I.A. carece de autonomía, corresponde a éste sujeto, ya sea el dueño del sistema, el programador, o el operador como guardián del mismo, la carga probatoria de demostrar esta falta de autonomía. Solo en el caso y una vez que se acredite dicha falta, podría evaluarse la responsabilidad del sujeto responsable mediante un factor de atribución subjetivo.

Ante esta situación poco favorable para las víctimas, es que se recurre a los factores objetivos de responsabilidad, pero estos tampoco encajan de una manera autosuficiente, ya que para poder aplicarlos se requiere acudir a institutos jurídicos (tales como: responsabilidad por daños causados por animales; responsabilidad por el hecho ajeno, riesgo creado, actividad riesgosa, etc.) que fueron diseñados para otros supuestos, los cuales pueden quedar obsoletos a medida que avanza la tecnología y el grado de autonomía de la I.A.

A raíz de lo antedicho surge la siguiente pregunta que da lugar a esta ponencia: ¿ante la autonomía creciente de la I.A. puede existir un factor de atribución objetivo específico, para imputar responsabilidad frente a los daños causados por los sistemas de I.A.?

7. PROPUESTA

Habiendo observado en una ajustada síntesis que en el derecho argentino los factores de atribución subjetivos no son de aplicación a los daños causados por la I.A. autónoma; que los factores objetivos, como el riesgo creado o la actividad riesgosa, no contienen respuestas adecuadas ya que no son específicos para la autonomía que desarrolla la I.A. Cabe sugerir

un nuevo factor de atribución que pueda contener el déficit que se observa en los actuales factores de atribución.

Es esencial discernir entre la labor del programador de un sistema de IA y el propio algoritmo, considerado un bien inmaterial en los términos contemplados por el C. C. y C. (art 16). En el caso específico de la I.A. el algoritmo opera de manera independiente respecto al programador, y las deficiencias que ocasionalmente surgen no necesariamente derivan de un riesgo inherente a la actividad de programación, sino que a menudo están relacionadas con las decisiones autónomas adoptadas por el propio algoritmo. Por lo tanto, es pertinente afirmar que hablar de "actividad" en relación con modelos matemáticos y computacionales, como el *Deep Learning* o el Aprendizaje Automático, puede carecer de precisión conceptual.

La noción de actividad riesgosa, según establecida en el C.C. y C., típicamente implica una acción ejecutada por ser humano. Sin embargo, resulta evidente que esta normativa no previó la eventualidad de que una I.A. basada en modelos matemáticos, como el *Deep Learning*, cuyas decisiones son autónomas respecto a la intervención humana, pudiera llevar a cabo riesgos.

No obstante, categorizar los sistemas de IA como "actividades riesgosas" podría conducir a una desproporción, implicando que cualquier individuo (ya sea humano o entidad jurídica, como una empresa) que haga uso de la IA estaría participando en una actividad riesgosa. Esta perspectiva resulta inadecuada en términos de asignación de responsabilidad y se distancia, inclusive hoy, de la intención subyacente en la normativa vigente.

Es pertinente establecer una distinción entre una I.A., un Robot y un automóvil. Estas entidades, aunque dotadas de componentes materiales, adquieren un grado de desarrollo autónomo debido a la integración de una I. A. De esta manera, despliegan un comportamiento que trasciende su naturaleza meramente material (escapan del concepto de cosa art.16 C.C.y C.), lo que conlleva una reconsideración en cuanto al factor de atribución de riesgos en el contexto tradicional.

Cuando se focaliza la atención en las circunstancias en las que el origen del daño deriva de la autonomía facilitada por la incorporación de algoritmos en un sistema de I. A., se torna evidente que es la propia capacidad autónoma del sistema la que genera el perjuicio. En esta instancia, la I.A. se eleva por encima de la mera categoría de "cosa", adquiriendo la

condición de un bien inmaterial. Consecuentemente, el enfoque previamente planteado, en el cual el riesgo es atribuible a una "cosa" o a una "actividad", se torna insuficiente para comprender la naturaleza intrínseca del riesgo asociado a la I. A.

Por lo tanto, resulta más apropiado abrazar la perspectiva previamente delineada, donde el concepto de "riesgo autónomo" emerge como el marco adecuado para abordar los desafíos legales y de atribución en este contexto. Este enfoque reconoce la singularidad de la IA y la autonomía de sus decisiones, distinguiéndola de las nociones tradicionales de riesgo inherentes a actividades humanas o al dominio de las "cosas". En última instancia, el término "riesgo autónomo" emerge como un concepto capaz de arrojar luz sobre la intersección entre la I. A. y el ámbito de la responsabilidad legal.

El término "riesgo autónomo" o "riesgo autosuficiente" se desvincula del concepto tradicionalmente asociado a la noción amplia de actividad riesgosa, al precisar el ámbito de atribución de responsabilidad. Este enfoque presupone que los sistemas de inteligencia artificial pueden tomar decisiones y acciones de manera independiente, desvinculadas de los elementos específicos que constituyen el riesgo originado por una actividad determinada. En esta perspectiva, se postula que el grado intrínseco de autonomía inherente a la inteligencia artificial conlleva una forma de responsabilidad objetiva.

La autonomía inherente a los sistemas de IA debe ser presumida, a menos que se demuestre lo contrario por parte de las partes imputadas de responsabilidad, ya sean los creadores del sistema de IA, los programadores involucrados, los guardianes legales de dichos sistemas o incluso los usuarios que sirven de ellos.

Para abordar la complejidad y autonomía de la I.A., es crucial diferenciar entre el programador y el algoritmo que es un bien inmaterial. La I.A. puede tomar decisiones autónomas, y su opacidad complica la aplicación de modelos tradicionales de responsabilidad. Por ello, se propone el concepto de "riesgo autónomo", que reconoce esta independencia y sugiere un modelo de responsabilidad objetiva, presumiendo la autonomía de la IA a menos que se demuestre lo contrario. Este enfoque busca un marco legal claro y adaptado a la naturaleza única de la IA, facilitando la gestión de los desafíos en responsabilidad civil y permitiendo una asignación justa y efectiva de la responsabilidad por daños causados por la IA.

8. COROLARIO

Es importante destacar que los límites de este trabajo y la relevancia de la cuestión abordada exigen un análisis más exhaustivo de esta nueva figura jurídica. En particular, se requiere un desarrollo más detallado en aspectos como las eximentes de responsabilidad y el grado de responsabilidad que se debe definir en función de la autonomía de la I.A.

Este enfoque preliminar representa un punto de partida para una nueva perspectiva sobre un tema en constante evolución y que presenta un potencial significativo para causar daños. Es fundamental continuar con la investigación y el análisis para adaptar la normativa a las realidades emergentes y a los desafíos que plantea la I.A.

9. BILBLIOGRAFIA

COLOMBO, María Celeste ¿La utilización de algoritmos es una actividad riesgosa? • LA LEY 08/11/2019, 1 • LA LEY 2019-F, 678.

CORVALAN Juan G. Tratado de Inteligencia Artificial y Derecho; Tomo III, Ed. La Ley año 202l.

CORVALAN Juan Gustavo, "Inteligencia artificial generativa como ChatGPT: ¿Un nuevo Renacimiento? Una explosión de Inteligencia humana colectiva a hombros de IA"; publicado en La Ley 05-06-2023- La Ley 2023-C,278.

CARABALLO Julio César y GAMEN Sebastián A. "La responsabilidad civil de los algoritmos. ¿Dónde estamos parados?"; elDial DC2B95; Publicado el: 05/08/2020 copyright © 1997 - 2023 Editorial Albrematica S.A.

DANESI, Cecilia C. ¿Quién responde por los daños ocasionados por los robots? • RCyS 2018-XI, 24.

DANESI, Cecilia, C Inteligencia artificial y responsabilidad civil: un enfoque en materia de vehículos autónomos • Sup. Esp. LegalTech 2018 (noviembre), 39.

DOMINGUES Villarroel María Patrizia; AZNAR DOMINGO, Antonio; La responsabilidad civil derivada del uso de inteligencia artificial (https://elderecho.com/responsabilidad-civil-derivada-uso-inteligencia-artificial)

FOSSACECA (h.), Carlos A. - MOREYRA, Pilar: Aproximaciones a la responsabilidad civil por la utilización de inteligencia artificial y derecho de los robots. Una mirada jurídica • RCyS 2020-VIII, 20

MARTINEZ, Carla I. responsabilidad civil derivada del uso de algoritmos: la cuestión de la jurisdicción internacional cuando el demandado no cuenta con radicación en argentina: 27-02-2021; Doctrina **Cita:** MJ-DOC-15787-AR||MJD15787

MELO, Verónica E. Responsabilidad por daños e inteligencia artificial: ¿vino nuevo en odres viejos? • Melo, Verónica E. • RCyS 2021-III, 3.

ORTEGA, Andrés, "La imparable marcha de los robots", Ed. Alianza, Madrid, 2016, ps. 18 y anteriores.

PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre los principios éticos para el desarrollo, el despliegue y el uso de la inteligencia artificial, la robótica y las tecnologías conexas • SIN ESPECIFICAR • SupAbCorp 2020 (noviembre),

ROSATI, Florencia - LAMARCA VIDAL, Mariana (2023) • Los retos legales de la inteligencia artificial en ChatGPT. Descifrando el futuro LA LEY 10/05/2023, 1

ROSSITER, Jonathan, "La robótica, los materiales inteligentes y su impacto futuro para la humanidad", en El próximo paso. La vida exponencial, Ed. BBVA — Open Mind, Madrid, 2016, p. 31.

ZAPIOLA GUERRICO, Martín: Inteligencia artificial y seguros: aplicaciones en la actividad aseguradora. Ventajas y desafíos •, LA LEY 15/06/2021, 1 • RDCO 309, 73.

IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN LA RESPONSABILIDAD CIVIL: DESAFÍOS REGULATORIOS

Por Tomás Rueda Laje[1]

I. CONCLUSIONES

1. Propuesta de *lege ferenda*: Es necesario implementar un marco regulatorio específico que contemple las particularidades de la IA, para proteger bienes jurídicos esenciales y prevenir la generación de daños. Este régimen debe complementar las disposiciones del Código Civil y Comercial (CCyC), incorporando estándares de seguridad rigurosos desde el diseño y desarrollo de sistemas de IA utilizados en áreas críticas, como la salud, el transporte, la justicia, la gestión ambiental, y el ámbito militar, asegurando que los desarrolladores, proveedores y usuarios cumplan con obligaciones claras que promuevan un uso ético y transparente de la tecnología. Las normas deben establecer controles rigurosos y procedimientos de evaluación de impacto para garantizar que la IA opere de manera segura en estos sectores. Asimismo, es necesario que los sistemas de IA en estos ámbitos sean supervisados de manera continua para prevenir riesgos y asegurar el cumplimiento de las normativas

2. Propuesta de *lege ferenda*. Se debe prohibir el uso de IA en áreas donde su implementación pueda causar daños significativos o violar derechos fundamentales de las personas. Ejemplos de usos prohibidos incluyen la manipulación de la opinión pública mediante la difusión masiva de información falsa, la vigilancia masiva mediante tecnologías de identificación biométrica sin consentimiento, y la evaluación continua y sesgada de emociones en contextos laborales o educativos. La regulación debe garantizar que la IA no sea utilizada para vulnerar la privacidad, la dignidad humana o los derechos fundamentales de las personas.

---

[1] Abogado. Magíster en Derecho Empresarial y en Derecho de los Negocios Internacionales. Profesor Adjunto y profesor de posgrado en la Universidad Blas Pascal. Cuenta a los fines de la presente ponencia, con el aval del Dr. Tomás G. Rueda, profesor titular de la Cátedra de Derecho de Daños de la Universidad Blas Pascal.

3. Propuesta de *lege ferenda*. Algunos sistemas de IA pueden clasificarse como actividades riesgosas según el artículo 1757 del CCyC, lo que implica una responsabilidad objetiva. Por otro lado, hay sistemas de IA que no generan riesgo, como la provisión de herramientas de desarrollo o la actividad de los motores de búsqueda, donde se aplica un régimen de responsabilidad subjetiva. La determinación del tipo de responsabilidad debe realizarse en función de las circunstancias de cada caso concreto.

4. Propuesta de *lege ferenda*: En los casos de responsabilidad objetiva, la legitimación pasiva recaerá sobre quienes tengan la dirección, fiscalización o control del sistema de IA, o en quienes obtengan un aprovechamiento económico del despliegue de la actividad. En contraste, en situaciones de responsabilidad subjetiva, la responsabilidad recaerá sobre quienes actúen de manera culposa o dolosa.

5. El estatuto del consumidor es plenamente aplicable a los daños derivados del riesgo o vicio de productos que incorporan sistemas de IA, así como a los daños ocasionados por el riesgo o vicio en la prestación de servicios que incluyan IA. En este contexto, los errores de sistema, sesgos algorítmicos y defectos de información se consideran vicios del producto o servicio, siendo aplicable el artículo 40 del CCyC, que establece la responsabilidad objetiva de todos los sujetos que participaron de la cadena de comercialización.

6. El riesgo de desarrollo no es una causal autónoma de eximición de responsabilidad tanto en casos de responsabilidad objetiva como subjetiva.

II. FUNDAMENTOS

1. INTRODUCCIÓN: DESAFÍOS REGULATORIOS

La inteligencia artificial (IA) es una tecnología con un potencial transformador sin precedentes para la humanidad. En los últimos años, hemos sido testigos de un crecimiento exponencial, especialmente en el campo de la IA generativa, que ha impactado prácticamente todas las esferas de la sociedad contemporánea. Sin embargo, junto con sus enormes beneficios, la implementación de la IA conlleva riesgos significativos que deben ser debidamente gestionados para garantizar un uso adecuado de este recurso tecnológico, y prevenir la causación de daños a las personas.

A nivel global, la mayoría de los países están explorando cómo adaptar sus marcos normativos para garantizar un uso ético, seguro y transparente de esta tecnología.

La Unión Europea ha asumido un rol de liderazgo en esta tarea con la reciente aprobación del Reglamento sobre IA ("RIA").

En Estados Unidos, el enfoque regulatorio ha sido más fragmentado y basado en directrices específicas para sectores particulares. La administración de Biden ha promovido iniciativas como el "*Blueprint for an AI Bill of Rights*" que establece principios de protección y transparencia, y la Comisión Federal de Comercio (FTC) ha emitido directrices que abordan prácticas engañosas y la protección de la privacidad en el uso de IA. Sin embargo, aún no se ha aprobado una legislación federal integral que cubra todos los aspectos de la IA.

En Argentina, el marco regulatorio está en proceso de evolución. El país ha comenzado a considerar la necesidad de una legislación específica para la IA a través de diversos proyectos de ley en el Congreso que buscan establecer normas claras sobre la responsabilidad, la transparencia y la ética en el uso de esta tecnología. Estos proyectos buscan crear un entorno regulatorio que pueda equilibrar la innovación con la protección de los derechos de los ciudadanos, aunque aún no se ha implementado un marco normativo definitivo.

En este contexto, el primer paso es evaluar si el sistema normativo vigente es suficiente para regular eficazmente los efectos de la IA, o si debe adecuarse con una normativa específica sobre la materia.

La propuesta de *lege ferenda* consiste en establecer un régimen regulatorio específico para proteger bienes jurídicos esenciales, que permitan prevenir la causación de daños a las personas. Dada la complejidad de la IA y sus características distintivas—como la opacidad, autonomía y capacidad de aprendizaje— junto con su potencial transformador, justifican plenamente esa necesidad.

En este proceso regulatorio, es importante señalar que la tecnología en sí misma no es ni buena ni mala, sino que su impacto dependerá del uso que las personas hagan de la misma. Por ejemplo, en el ámbito de la salud, la IA puede analizar imágenes médicas con alta precisión para la detección temprana del cáncer, con mayor antelación y precisión a la que es propia a los métodos tradicionales. Sin embargo, utilizada con fines ilícitos, la IA puede generar daños significativos a las personas, afectando seriamente

derechos fundamentales como la privacidad y la no discriminación. De ahí que el principal desafío regulatorio sea implementar un marco normativo que proteja adecuadamente estos derechos, sin ser tan restrictivo como para obstruir el avance tecnológico.

2. DEFINICIONES PRELIMINARES Y RIESGOS ASOCIADOS A LA IA

a) Definiciones y nociones técnicas preliminares

Para regular la responsabilidad civil derivada de la utilización de sistemas de IA, es esencial definir primeramente qué es la IA y conocer algunas de sus modalidades posibles. Según el RIA:

"La IA es un sistema basado en máquinas diseñado para funcionar con diversos niveles de autonomía, que puede mostrar capacidad de adaptación tras su despliegue, infiriendo a partir de la entrada recibida cómo generar salidas como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales[2]."

Existen dos grandes categorías para clasificar este recurso tecnológico: por un lado, IA simbólica o tradicional ("IAS") y por otro, aprendizaje automático o *machine learning* ("AA").

La IAS utiliza la representación simbólica del conocimiento humano y el razonamiento lógico-deductivo[3]. Por ejemplo, un sistema experto, que deduce diagnósticos médicos a partir de síntomas específicos.

El AA analiza grandes cantidades de datos para identificar patrones y hacer clasificaciones o predicciones sin seguir reglas explícitas ni requerir intervención humana durante el proceso[4].

Una variante comúnmente utilizada de AA es el aprendizaje mediante redes neuronales artificiales, inspirado en el funcionamiento del cerebro humano. La modalidad más representativa de este enfoque es el aprendizaje profundo o *deep learning* ("AP"). Este sistema utiliza

---

[2] https://artificialintelligenceact.eu/es/article/3/

[3] Garnelo, Marta, Shanahan, Murray, "*Reconciling deep learning with symbolic artificial intelligence: representing objects and relations*", Current Opinion in Behavioral Sciences, Volumen 29, 2019, pp. 17-23. Disponible el 02 de julio de 2024 en: https://www.sciencedirect.com/science/article/pii/S2352154618301943?via%3Dihub.

[4] https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained

numerosas capas de neuronas artificiales interconectadas, similar a las neuronas organizadas jerárquicamente en los cerebros humanos, para procesar información y generar un resultado. Actualmente, el AP es el enfoque de AA más exitoso, con mejor generalización a partir de datos pequeños y mejor escalabilidad para datos grandes y presupuestos de cómputo[5]. Es un mecanismo altamente efectivo en aplicaciones como el reconocimiento de imágenes, procesamiento de lenguaje natural y conducción autónoma.

Por último, existe una subcategoría del AP, que es la IA generativa ("IAG"), que tiene la capacidad para crear contenido nuevo a partir de instrucciones específicas recibidas por un usuario. En este contexto, los Grandes Modelos de Lenguaje ("LLM", por sus siglas en inglés), constituyen una forma de IAG, que pueden producir texto coherente, imágenes, canciones, videos y código de programación, convirtiéndose en herramientas poderosas para la creación y asistencia en diversas tareas.

b) Riesgos asociados a la IA

La IA impulsa una revolución tecnológica con un potencial transformador sin precedentes para la sociedad contemporánea. Entre sus características más destacadas, se encuentra la capacidad de automatizar tareas, mejorar la eficiencia y tomar decisiones autónomas con una precisión superior a la humana. No obstante, junto con estos beneficios, surgen desafíos significativos, especialmente en el ámbito del derecho de daños, donde es crucial proteger los derechos fundamentales de las personas y ofrecer previsibilidad a las empresas tecnológicas.

Entre los riesgos asociados a la IA se destacan los sesgos algorítmicos, la opacidad del sistema, las alucinaciones, las deepfakes y las preocupaciones sobre la privacidad de los datos.

Los sesgos algorítmicos ocurren cuando los sistemas de IA, al ser entrenados con datos históricos, replican o incluso agravan prejuicios existentes, lo que puede resultar en decisiones injustas o discriminatorias.

Además, el procesamiento masivo de datos personales por parte de la IA plantea serias inquietudes sobre la privacidad. Los modelos de IA, que

[5] Manning, Christopher, *Artificial Intelligence Definitions*, Stanford University Human-Centered Artificial Intelligence, 2020.

requieren grandes volúmenes de datos para operar de manera eficiente, incrementan el riesgo de violaciones de privacidad y del uso indebido de información sensible. Por ello, es esencial establecer marcos normativos que aborden estos riesgos, asegurando un uso de la IA que sea equitativo y respetuoso con los derechos fundamentales.

La opacidad es otro riesgo significativo asociado a la IA. Dado que muchos algoritmos de IA funcionan como "cajas negras", es difícil comprender cómo toman decisiones o llegan a conclusiones. Esta falta de transparencia puede generar desconfianza, especialmente cuando las decisiones afectan a los derechos de las personas.

Otro desafío que presenta la IA son las alucinaciones, que ocurren cuando los sistemas de IA generan información incorrecta o sin fundamento. Este riesgo es particularmente grave en aplicaciones críticas donde la precisión es esencial, como en la medicina o en la administración de justicia.

La robótica, que materializa sistemas de IA en entidades físicas como robots, también presenta desafíos legales significativos. Robots como "Sophia" de Hanson Robotics ilustran cómo la integración de IA en robots puede realizar tareas complejas y autónomas, como la interacción conversacional y el reconocimiento facial. Sophia es un robot humanoide capaz de mantener conversaciones naturales y expresar emociones, lo que la convierte en un referente en la discusión sobre el potencial y los límites de la IA. Sin embargo, también plantea cuestiones sobre la responsabilidad en caso de daños causados por estos dispositivos, como la infracción de la privacidad o daños físicos, y la necesidad de un marco regulatorio claro y específico[6].

Los drones son otro ejemplo relevante. Utilizados para vigilancia y seguridad, pueden infringir fácilmente la privacidad o causar daños físicos a personas o cosas. Determinar la responsabilidad por accidentes o ataques causados por drones inteligentes es un problema complejo que requiere una claridad normativa.

En el ámbito médico, los robots utilizados en cirugías o como asistentes pueden cometer errores que resulten en daños graves a los pacientes, generando necesidades específicas de regulación para

[6] https://www.hansonrobotics.com/sophia/

proporcionar los niveles adecuados de seguridad jurídica que la utilización de la tecnología requiere.

Otro desafío importante es la proliferación de las *deepfakes*, que son sistemas de IA utilizados para crear imágenes, sonidos y videos falsos, pero extremadamente realistas. El nivel de sofisticación de la tecnología hace que sea prácticamente imposible distinguir un caso real de otro ficticio. Bajo esta modalidad, es sumamente sencillo y factible vulnerar la identidad de las personas, afectando su privacidad y reputación. Además, este tipo de tecnología puede ser utilizado para difundir información falsa, o cometer delitos, lo que resalta la necesidad de contar con un marco regulatorio sólido para abordar adecuadamente esta problemática.

Es esencial contar encontrar el punto justo de equilibrio entre la innovación tecnológica y la protección de los derechos de las personas. Por tal motivo, el régimen normativo debería incluir definiciones precisas, criterios claros para atribuir responsabilidades y exenciones, reglas para superar la opacidad del sistema, y medidas específicas para prevenir la generación de daños.

Nuestro ordenamiento jurídico argentino contiene normas regulan correctamente los efectos derivados del uso de sistemas de IA. Sin embargo, es necesario adecuar dicha normativa para contemplar las especificidades propias de la IA, especialmente cuando están comprometidos los bienes jurídicos esenciales. Esto permitirá no solo garantizar una mejor protección de los derechos fundamentales de las personas, sino también fomentar un entorno seguro y predecible para el desarrollo tecnológico.

En conclusión, la regulación efectiva de los sistemas de IA es crucial para garantizar que esta revolucionaria tecnología contribuya positivamente al progreso humano sin comprometer la seguridad ni los derechos fundamentales de las personas.

3. PROPUESTA DE LEGE FERENDA

a) La necesidad de establecer un marco normativo especifico con fines preventivos del daño

La prevención es una función primordial del derecho de daños, como lo reconocen los Arts. 1708, 1710 y siguientes del CCyC. Según esta normativa, toda persona tiene el deber de evitar, en la medida de lo posible, causar daños injustificados a terceros.

La naturaleza compleja de la IA —caracterizada por su opacidad, autonomía y capacidad de aprendizaje— y su potencial transformador justifican la necesidad de establecer un régimen regulatorio específico. Aunque el CCyC proporciona una base sólida para la prevención del daño, es imprescindible desarrollar un marco normativo que aborde las particularidades de la IA. Este marco debe complementar y expandir las disposiciones existentes, asegurando que se contemple adecuadamente la singularidad de la tecnología y se prevengan daños potenciales a través de una normativa adaptada a su naturaleza y dinámica de funcionamiento.

En esta línea de pensamiento, establecer estándares de seguridad rigurosos desde las fases iniciales de diseño y desarrollo de sistemas de IA que involucren bienes jurídicos esenciales, es necesario para gestionar adecuadamente estos riesgos. Además, la imposición de obligaciones claras a los distintos sujetos involucrados, según el rol que desempeñen, promueve un uso ético, seguro y transparente de la tecnología.

b) Usos prohibidos de la IA

El punto de partida de la propuesta normativa es prohibir determinados usos de la IA, por su potencialidad de causar daños significativos o violar derechos fundamentales de las personas.

Un ejemplo claro del potencial destructivo de la IA es su capacidad para manipular a las personas mediante la difusión masiva y automatizada de información falsa o sesgada. A través de sistemas de IA, esta desinformación puede ser diseminada de manera altamente efectiva, influenciando insidiosamente las opiniones y decisiones de los individuos. Un caso que ilustra este peligro es el uso de *bots* impulsados por IA en redes sociales durante elecciones para crear y difundir noticias falsas dirigidas a distintos segmentos del electorado, basadas en perfiles detallados de los usuarios[7].

Otro ejemplo es el uso de tecnologías de identificación biométrica en espacios públicos, como el reconocimiento facial, para la vigilancia masiva de las personas. Este tipo de práctica plantea serias preocupaciones sobre la privacidad y la libertad individual, ya que permite la monitorización constante de personas sin su consentimiento, creando un entorno de control

[7] https://news.microsoft.com/es-xl/enfrentar-el-momento-combatir-los-deepfakes-de-ia-en-las-elecciones-a-traves-de-un-nuevo-acuerdo-tecnologico/

y coacción. Sin embargo, una excepción podría considerarse cuando existan bases objetivas que indiquen la comisión de delitos.

Además, los sistemas diseñados para analizar y controlar las emociones humanas mediante IA, como aquellos utilizados en contextos laborales o educativos, pueden invadir la esfera más íntima de la persona, sometiéndola a evaluaciones continuas y potencialmente sesgadas que afectan su bienestar psicológico y su derecho a la privacidad.

Finalmente, los sistemas de puntuación social, que asignan calificaciones a los individuos en función de su comportamiento, plantean graves riesgos para la dignidad humana y la igualdad de oportunidades. Estos sistemas pueden conducir a la discriminación y a la marginación social, violando principios básicos de justicia y equidad.

Estas prohibiciones garantizan que el uso de la IA no socave los derechos fundamentales ni cause daños irreparables a las personas.

c) Usos regulados de IA

La propuesta de lege ferenda plantea la necesidad de regular la implementación de la IA en áreas críticas para garantizar que su uso sea seguro, justo y ético.

En el ámbito de la **salud**, la IA aplicada en el diagnóstico y tratamiento médico debe estar sujeta a regulaciones que aseguren la fiabilidad y seguridad de los sistemas, protegiendo el derecho de los pacientes a recibir una atención adecuada.

En el sector del **transporte**, es crucial que los sistemas de IA utilizados en la conducción autónoma y la gestión del tráfico sean sometidos a controles estrictos, con el fin de garantizar la seguridad de los usuarios y la eficiencia en la gestión del transporte.

La gestión de **servicios públicos**, como la energía, el agua y las telecomunicaciones, también debe ser monitoreada para evitar interrupciones que puedan afectar a la población.

En el **ámbito judicial**, es esencial que la IA utilizada en la toma de decisiones sea supervisada para asegurar un juicio justo y una defensa efectiva.

En cuanto al **medio ambiente**, las aplicaciones de IA en la gestión ambiental deben ser reguladas para promover la sostenibilidad y evitar el deterioro ecológico.

Por último, en el **ámbito militar**, la IA requiere un control estricto para prevenir la escalada de conflictos y garantizar el cumplimiento de las leyes internacionales humanitarias.

En el desarrollo, implementación y uso de la IA para algunos de los usos regulados referidos precedentemente, varios actores desempeñan un papel crucial, y es esencial asignarles obligaciones preventivas para garantizar un manejo ético y seguro de la tecnología.

En primer lugar, es fundamental que **los desarrolladores de IA** realicen pruebas exhaustivas en entornos controlados para garantizar la fiabilidad y seguridad de los sistemas. Además, se debe llevar a cabo una evaluación de impacto para identificar y mitigar posibles riesgos asociados con la implementación de la IA. La supervisión humana continua es esencial para asegurar que los sistemas operen conforme a las normativas y principios éticos, y se debe cumplir con el deber de informar a los usuarios sobre las capacidades, limitaciones y riesgos de las herramientas de IA. Por último, es crucial mantener una alta calidad de los datos utilizados, asegurando que sean precisos, seguros y estén alineados con las normativas de protección de datos.

Los proveedores de datos están obligados a garantizar la calidad, precisión y seguridad de los datos proporcionados, cumpliendo con las normativas de protección de datos y privacidad, y asegurando que los datos utilizados provengan de fuentes con consentimiento informado.

Los integradores de sistema deben asegurar que los sistemas integrados con IA cumplan con todas las normativas aplicables, manteniendo la coherencia entre los diferentes componentes y realizando auditorías regulares para verificar el cumplimiento de los estándares de seguridad y ética.

Los proveedores de infraestructura tienen la responsabilidad de mantener la infraestructura que soporta los sistemas de IA segura, actualizada y resiliente frente a amenazas cibernéticas, implementando medidas de redundancia y planes de contingencia para minimizar el impacto de posibles fallos.

Los comercializadores y distribuidores, por su parte, deben asegurar que los productos de IA que comercializan o distribuyen cumplan con todas las normativas de seguridad y ética aplicables, proporcionando a los consumidores información clara y precisa sobre las limitaciones y riesgos potenciales de estos productos.

Finalmente, **los usuarios** tienen la obligación de utilizar la IA de manera ética y conforme a las normativas vigentes, especialmente en áreas sensibles como la salud, la justicia o la seguridad pública. Es crucial que el personal encargado de operar sistemas de IA esté debidamente capacitado y que exista supervisión humana constante para mitigar los riesgos asociados.

4. FACTORES DE ATRIBUCION DE RESPONSABILIDAD

a) Introducción

La determinación del factor de atribución de responsabilidad en daños derivados de sistemas de IA genera debates significativos en la jurisprudencia y la doctrina.

En primer lugar, es esencial diferenciar la responsabilidad derivada de hechos ilícitos o extracontractuales de la responsabilidad contractual.

b) Responsabilidad extracontractual

Algunos sistemas de IA pueden ser considerados actividades riesgosas conforme al artículo 1757 del CCyC, por los medios empleados o las circunstancias de su realización. En consecuencia, en estos casos la responsabilidad es de naturaleza objetiva. Este fue la conclusión adoptada por las Jornadas Nacionales de Derecho Civil de Santa Fe en 2019[8].

Sin embargo, es importante señalar que no todos los usos de la IA deben ser categorizados como actividades riesgosas. Un ejemplo claro son los *frameworks* como TensorFlow o PyTorch, que se limitan a proporcionar herramientas que permiten a los desarrolladores crear y entrenar modelos de IA. Considerar estas plataformas como actividades riesgosas implicaría que las empresas proveedoras tendrían que responder objetivamente por cualquier daño causado por sistemas de IA creados con esas herramientas.

[8] https://www.fcjs.unl.edu.ar/jndc-2019/

Esta responsabilidad sería desproporcionada e inviable, ya que las empresas no tienen control sobre cómo se utilizan estas herramientas por terceros.

Otro ejemplo relevante es el de los motores de búsqueda, que emplean algoritmos de IA para indexar sitios web. En el caso "María Belén Rodríguez" decidido por la Corte Suprema de Justicia de la Nación[9], se determinó que estos buscadores de contenido no son responsables de manera objetiva por los contenidos que indexan. Su actividad no se considera riesgosa bajo el artículo 1757 del CCyC, y sería imposible exigirles una supervisión activa sobre todos los sitios web que indexan, ya que esto excede el alcance de su función como buscadores de contenido.

c) Responsabilidad contractual

En cuanto a la responsabilidad contractual, el primer paso es analizar lo acordado entre las partes, considerando la autonomía de la voluntad. Si no se ha previsto nada en particular, será necesario determinar si la obligación es de resultados o de medios. Si se trata de una obligación de resultados, el factor de atribución será objetivo; en cambio, si es una obligación de medios, será subjetivo.

Además, es importante mencionar el deber tácito de seguridad, que impone una responsabilidad objetiva. Este deber obliga a las partes a garantizar la seguridad de sus sistemas, asegurando que el adquirente no sufra daños en su integridad física o en sus bienes. Este deber de seguridad se traduce en una obligación de resultado, donde la falla en la protección del usuario o consumidor activa la responsabilidad objetiva del proveedor.

d) Legitimación Pasiva

En los casos de responsabilidad objetiva, la legitimación pasiva recae de manera concurrente en el titular de la actividad, quien puede dirigir, fiscalizar o controlar el sistema de IA, o en quienes obtengan un aprovechamiento económico del despliegue de la actividad. Por ejemplo, una empresa que desarrolla y comercializa un sistema de IA que pueda ser considerado actividad riesgosa, será responsable por los daños causados por

[9] http://www.saij.gob.ar/corte-suprema-justicia-nacion-federal-ciudad-autonoma-buenos-aires-rodriguez-maria-belen-google-inc-otro-danos-perjuicios-fa14000161-2014-10-28/123456789-161-0004-1ots-eupmocsollaf.

dicho sistema, salvo que pueda acreditar la interrupción del nexo adecuado de causalidad.

En cuanto a la responsabilidad por incumplimiento obligacional, la responsabilidad recae en el co-contratante que incumple la obligación. Por ejemplo, si una empresa proveedora de software no garantiza la seguridad de su sistema conforme lo pactado en el contrato, deberá responder por los daños causados al usuario.

e) Exención de responsabilidad

En casos de responsabilidad objetiva, el responsable puede eximirse de responsabilidad si logra interrumpir el nexo adecuado de causalidad, lo cual puede darse por el hecho de un tercero extraño, el hecho de la propia víctima o un caso fortuito. Por otro lado, en la responsabilidad subjetiva, la eximición se da probando la ausencia de culpa.

La conducta del usuario es un factor crucial en la determinación de la responsabilidad. En sistemas de IA generativa, los desarrolladores deben poder demostrar mediante los prompts ingresados por los usuarios que cualquier daño resultó de un uso inapropiado del sistema. Esto podría permitir a la empresa eximirse de responsabilidad si la víctima es el propio usuario, o intentar eventualmente una acción de reintegro contra el usuario si el afectado es un tercero. Esta medida no solo protege a los desarrolladores, sino que también fomenta un uso más consciente y responsable de las tecnologías de IA.

Es crucial destacar que el riesgo de desarrollo no constituye un supuesto de eximición autónomo en el sistema argentino. Esto se alinea con la naturaleza de la responsabilidad objetiva por riesgo creado, donde el defecto del producto o servicio existe independientemente del conocimiento que se tenga de él.

5. DAÑOS DERIVADOS DE SISTEMAS DE IA EN RELACIONES DE CONSUMO

En el ámbito de las relaciones de consumo, el artículo 40 de la Ley de Defensa del Consumidor (LDC) contempla dos supuestos de responsabilidad:

Inadecuación material del producto o servicio: El defecto del producto o servicio frustra total o parcialmente el interés del consumidor en

la prestación. Por ejemplo, si un sistema de IA no cumple con las expectativas generadas o prometidas, el proveedor podría ser responsable.

Inadecuación cualitativa del producto o servicio: Aquí, el defecto se origina en una falla de seguridad que genera un daño a la integridad física o patrimonial del consumidor.

Los errores de sistema, los sesgos algorítmicos y los defectos de información o advertencia se consideran defectos de diseño. Los consumidores o usuarios deben recibir información adecuada, clara y circunstanciada sobre los riesgos asociados al uso de sistemas de IA, incluyendo cómo se recopilan, almacenan, usan y destinan los datos.

La propuesta de lege ferenda propone precisar la legitimación pasiva de acuerdo con la dinámica particular de la cadena de distribución y desarrollo de sistemas de IA. En este sentido, debería contemplarse una distribución clara de responsabilidades entre desarrolladores, proveedores y otros intermediarios, considerando las características específicas de cada sistema y su impacto potencial.

DAÑOS DERIVADOS DE LA INTELIGENCIA ARTIFICIAL

Por Tomás Guillermo Rueda[1]

I. CONCLUSIONES

1. En materia de prevención de daños derivados de la Inteligencia Artificial resultan aplicables las Recomendaciones para una Inteligencia Artificial Fiable (Subsecretaría de Tecnología de la Información-Jefatura de Gabinete de Ministros-).

2. Los datos obtenidos para los sistemas de IA deben ser consistentes con el derecho internacional y acorde a los valores y principios reconocidos internacionalmente al efecto; respetando el ordenamiento nacional.

3. En coherencia con lo expuesto, deben observarse mecanismos de supervisión, evaluación del impacto, auditoría y diligencia debida, que garanticen la rendición de cuentas de los sistemas de IA y su impacto en el tiempo.

4. Responsabilidad Genérica - Deberes de Prevención del daño:

a. Existiendo un sistema jerarquizado de aprendizaje automático, y prácticamente ilimitado, resulta esencial la aplicación del principio de Prevención como herramienta para prevenir y en su caso aminorar las consecuencias lesivas devenidas de la actividad de la IA

b. Toda persona, en cuanto de ella dependa, será responsable de evitar el daño como de prevenir su acaecimiento o mitigar sus consecuencias, sirviendo como parámetro las mentadas Recomendaciones referenciadas en el punto "I" (Art.1710 y ss, CCC).

5. Responsabilidad Específica

Responsabilidad objetiva (actividad riesgosa) y subjetiva (falta de diligencia)

---

[1] Profesor titular de la Cátedra de Derecho de Daños, Universidad Blas Pascal, doctor en derecho.

En el caso de la utilización de la IA resultan obligados, los usuarios, proveedores y terceros equiparados, con distintas escalas de responsabilidad.

Usuario: Responsabilidad subjetiva:

a) Incumplir deberes propios al utilizar o supervisar el sistema de IA de conformidad con los mecanismos de supervisión previstos al efecto y en tanto estén a su alcance y la diligencia debida;

b) Exponer el sistema de IA a datos de entrada, bajo su control, que no eran pertinentes ni adecuados a los fines previstos.

Fabricante: Responsabilidad objetiva

a) Responsabilidad objetiva ante la provocación de daños, por la introducción en la comunidad de una actividad susceptible de generar riesgos para terceros, independientemente de su beneficio.

Proveedores: Responsabilidad objetiva

a) Responsabilidad objetiva por equipararse su situación a la del fabricante en la introducción de la actividad potencialmente dañosa.

Terceros equiparados en la introducción de la actividad riesgosa: Responsabilidad objetiva, por similares fundamentos.

6. Las normas y principios protectorios del régimen consumeril resultan enteramente aplicables a la actividad de la IA en tanto se trate de la adquisición o uso de un servicio como destinatario final en los términos de los Arts. 1092/3, CCC

II. FUNDAMENTOS

1. IA – SÍNTESIS INTRODUCTORIA

La inteligencia artificial es una subdisciplina del campo de la Informática que busca la creación de máquinas que puedan imitar comportamientos inteligentes"2

Aprendizaje Automático (Machine Learning), es la rama del campo de la Inteligencia Artificial, que busca como dotar a las máquinas de capacidad de aprendizaje (entendido este como la generalización de un conocimiento a partir de un conjunto de experiencias)

Lo importante del Machine Learning es saber distinguir entre dos escenarios distintos. Por ejemplo: es muy distinto programar una máquina para que pueda moverse a programar esa misma máquina para que aprenda a moverse.

Si tomamos el ejemplo del reconocimiento facial, no es lo mismo programar una máquina para que distinga los elementos de una cara que hacerlo de tal manera que aprenda qué es una cara. A su vez, el aprendizaje se jerarquiza por niveles, acorde la cantidad de capas añadidas3

Existen diversas técnicas para cubrir distintas aplicaciones (árboles de decisión, modelos de regresión, modelos de clasificación, técnicas de caracterización, etc.), sin embargo, de entre todas ellas hay que destacar la de las redes neuronales.

2. CLASES DE APRENDIZAJES

Realizada esta síntesis introductoria, podemos desarrollar brevemente lo que hemos expresado precedentemente.

El Deep Learning es una versión del aprendizaje automático que trata de imitar la inteligencia humana. Los algoritmos trabajan en capas de

---

[2] ***https://www.edsrobotics.com/blog/deep-learning/***

3 Las redes neuronales son capaces de aprender de forma jerarquizada. Esto significa que la información se aprende por niveles: en las primeras capas se aprenden conceptos muy básicos como qué es un diente, un labio, una nariz, un ojo…y en las posteriores capas se usa lo aprendido previamente para aprender conceptos más abstractos, como una cara, un cuerpo humano…Esto hace que, a medida que añadimos más capas, la información que se aprende es cada vez más abstracta y, por ello, más complejo.

redes neuronales artificiales. La información es ingresada a la primera capa de red neuronal, posteriormente se conduce capa por capa por lo que el aprendizaje se jerarquiza. Los algoritmos de la capa inferior se sirven de lo procesado por las capas superiores perfeccionando los procesos de aprendizajes

El aprendizaje puede dividirse en diferentes grupos, destacando como lo más utilizado:

Aprendizaje supervisado

Aprendizaje no supervisado

Aprendizaje reforzado

a) ¿Qué es el aprendizaje supervisado?

De los tipos de aprendizaje que se utilizan en el Machine Learning, el aprendizaje supervisado es el más común. Se le denomina así porque es el desarrollador o programador (es decir, un ser humano) el que actúa como guía para enseñar al algoritmo las conclusiones a las que debe llegar. O sea, la salida del algoritmo ya es conocida previamente.

En conclusión, es un aprendizaje cerrado porque se supervisa que para determinado dato X, el algoritmo aprenda determinado dato Y.

Ejemplo de aprendizaje supervisado

Un ejemplo muy aclarador es la clasificación de nuestros e-mails en las distintas bandejas que tenemos en nuestro correo electrónico.

¿Cómo son capaces los sistemas de clasificar un e-mail como SPAM y cómo pueden mandar otro directamente a la bandeja de entrada? Es muy sencillo, aprenden millones y millones de datos a los que se les asocia determinadas palabras como SPAM. Así, un e-mail de un cliente o un amigo aparecerá en tu bandeja de entrada, y una promoción sospechosa con productos de baja calidad probablemente acabe en SPAM.

Así aprenden los softwares y los dispositivos. Cuando los usamos, nosotros mismos les estamos enseñando qué es SPAM y qué no lo es. Parece que la Inteligencia Artificial es algo que nos es ajeno en el día a día, pero está mucho más presente en nuestras vidas de lo que somos conscientes.

b) ¿Qué es el aprendizaje no supervisado?

Por otro lado, el aprendizaje no supervisado está más estrechamente alineado con la Inteligencia Artificial ya que da la idea de que una máquina puede aprender a identificar procesos y patrones complejos sin necesidad de que un ser humano le proporcione orientación y supervisión a lo largo del proceso de aprendizaje.

Algunos ejemplos de algoritmos de aprendizaje no supervisado incluyen el agrupamiento y las reglas de asociación. En el caso de este tipo de aprendizaje no existe un conjunto de datos de entrenamiento previo, se aborda el problema utilizando sólo datos de entrada y sólo con operaciones lógicas para guiarlo.

Ejemplo de aprendizaje no supervisado

Un ejemplo que puede resumir estos dos aprendizajes sería el siguiente: en un conjunto de datos encontramos hexágonos y pentágonos de color negro y de color blanco. Con el aprendizaje supervisado, la solución de este problema sería bastante sencillo. Consistiría en enseñar a la máquina varias cosas: primero, que la forma con seis lados es un hexágono, que la forma con cinco lados es un pentágono, y que determinado valor de luz en un píxel concluye que se trata de color negro y de color blanco. De esta manera el algoritmo aprende a distinguir sólo pentágonos blancos, pentágonos negros, hexágonos blancos, y hexágonos negros. Con el aprendizaje no supervisado, el algoritmo es capaz de reconocer determinado número de lados y determinados píxeles de color. Así, cuando se le presenten nuevas formas, sabrá reconocer si algunas se asemejan en lados o en color a estas formas y clasificarlos de manera correcta.

3. LOS RIESGOS DE LA IA

Entre los diversos riesgos conocidos, uno especialmente alarmante es la invasión y afectación de los derechos personalísimos. La extraordinaria capacidad de la IA generativa para narrar historias que confirman las ideas y los puntos de vista preconcebidos de las personas puede amplificar el efecto de las cámaras de eco y de los sesgos ideológicos.

Ya sea que se trate de una historia fabricada, una imagen adulterada o un video sintético, los productos de la IA generativa pueden ser tan convincentes que crean un falso sentido de realidad.

Esto puede propalar información errónea, incitar al pánico e incluso desestabilizar sistemas económicos y financieros con una eficiencia e intensidad inusitadas.

4. OTRAS LESIONES CONEXAS NO CONTEMPLADAS

Queda al margen del análisis supuestos de afectaciones a derechos esenciales como la protección de datos (ya contemplada en la ley nacional 25.326), violaciones a la Intimidad de las personas cuya protección encuentra sustento constitucional y legalmente establecido (Código Civil y Comercial) y contra la discriminación en cualquiera de sus manifestaciones (ley nacional 23.592).

5. LA IA COMO ACTIVIDAD RIESGOSA/VICIOSA

"Actividades riesgosas o peligrosas".

Doctrinariamente se destacó que "puede incluirse en el elenco de actividades riesgosas, entre otras: la utilización de algoritmos, las actividades cibernéticas, las plataformas digitales y sistemas operados por inteligencia artificial"[4] .

No únicamente el contenido (actividad del sistema), sino que su continente es también un elemento encuadrado en la previsión del Art. 1757, CCC.

En tal sentido, por software se entiende la "producción de un conjunto estructurado de instrucciones, procedimientos, programas, reglas y documentación contenida en distintos tipos de soporte físico (cinta, discos, circuitos eléctricos, etc.) con el objetivo de hacer posible el uso de equipos de procesamiento electrónico de datos"[5].

También se reconoció que la actividad desplegada por las técnicas de machine learning y deep learning no siempre es inocua, sino que posee una notable e intrínseca potencialidad dañosa para terceros cuando hace uso de algoritmos defectuosos.

---

[4] XXVII Jornadas Nacionales de Derecho Civil, Santa Fe, 2019

[5] r. Chudnovsky, Daniel; López Andres y Melitsko, Silvana. El sector de software y servicios informáticos (SSI) en la Argentina: Situación actual y perspectivas de desarrollo. DT 27/Julio de 2001. Págs. 30 a 34.Citado por Rivera, Silvana Cristina, en:" ¿El régimen legal aplicable al software resulta un obstáculo para el desarrollo y generalización de la innovación?. https://repositorio.udesa.edu.ar/; jun/jul 2024

Se pueden advertir al menos tres situaciones generadoras de daños en los algoritmos: a) los *bugs* o errores informáticos; b) los sesgos en los algoritmos; y c) la manipulación algorítmica (captadores de perfil).

Todos enmarcan en una actividad intrínsecamente riesgosa o viciosa, potencialmente perjudicial en la persona o sus bienes.

6. PREVENCIÓN DEL DAÑO

a) Evaluación de riesgos y medidas preventivas

Un sistema de IA nunca podrá reemplazar la responsabilidad final de los seres humanos y su obligación de rendir cuentas.

En caso de que pueda producirse cualquier daño para los seres humanos, debería garantizarse la aplicación de procedimientos de evaluación de riesgos y la adopción de medidas para impedir que ese daño se produzca o, producidos, se aminoren sus efectos perjudiciales.

No obstante se sugiere la implementación de un sistema de Gestión de Riesgos que certifique determinados criterios de calidad, validación y prueba de los sistemas de IA antes de su puesta en servicio.

b) Medidas de Prevención del daño.

Los daños no deseados (riesgos de seguridad) y las vulnerabilidades a los ataques (riesgos de protección) deberían ser evitados y deberían tenerse en cuenta, prevenirse y eliminarse a lo largo del ciclo de vida de los sistemas de IA

Los actores de la IA deberían promover la diversidad y la inclusión, garantizar la justicia social, salvaguardar la equidad y luchar contra todo tipo de discriminación, de conformidad con el derecho internacional.

La Subsecretaría de Tecnologías de la Información, dependiente de la Secretaría de Innovación Pública, publicó el día 2 de junio de 2023, la Disposición 2/2023, mediante la cual se aprobaron las **"Recomendaciones para una Inteligencia Artificial Fiable"**.

Es importante que los datos para los sistemas de IA se recopilen, utilicen, compartan, archiven y supriman de forma consistente con el derecho internacional y acorde a los valores y estos principios enunciados, respetando al mismo tiempo los marcos jurídicos nacionales, regionales e internacionales pertinentes.

Deberían elaborarse mecanismos adecuados de supervisión, evaluación del impacto, auditoría y diligencia debida, incluso en lo que se refiere a la protección de los denunciantes de irregularidades, para garantizar la rendición de cuentas respecto de los sistemas de IA y de su impacto a lo largo de su ciclo de vida

7. RESPONSABILIDAD CONTRACTUAL Y EXTRACONTRACTUAL. RESPONSABLES.

a) Responsabilidad contractual. Seguridad del producto. Falencias constitutivas.

Los fabricantes son responsables por la seguridad del producto y que el público en general tiene derecho a esperar.

Es decir, la seguridad está dada por las expectativas que el producto genera tanto en su finalidad como características objetivas y las propiedades del producto en atención a las necesidades del usuario y a su propia vulnerabilidad en materia de ciberseguridad

El defecto del producto se relaciona, así, con falencias constitutivas objetivas como con su falta de adecuación a la finalidad y función que le fuera asignada (no se adecua a la función cuando no satisface la necesidad del usuario-falla en el sistema de voz, por ejemplo-).

b) Responsabilidad extracontractual

Las previsiones aquí consideradas se relacionan con aquellos sucesos que afectan la salud y el patrimonio de los consumidores, en la órbita de la responsabilidad extracontractual.

La defectuosidad del producto no se relaciona con la falta de aptitud según previsiones contractuales previamente delimitadas sino con su potencialidad dañosa (cualquiera fuere su origen, defectos congénitos, falta de supervisión, omisión de actualización del sistema, etc.)

c) Extensión de la responsabilidad de los fabricantes:

Los fabricantes extienden su responsabilidad más allá de la puesta del producto en el mercado, cuando los programas informáticos y servicios conexos permanecen bajo la órbita de su contralor, por mejoras o actualizaciones conocidas a ese entonces y que deban practicarse o ser

autorizados por su parte o de algún modo intervenga en su suministro por terceros.

d) Estatuto Consumeril:

En caso de que la utilización del algoritmo se enmarque en una relación de consumo, en los términos de los arts. 1092 y 1093, del CCC y arts.1y 2, de la Ley de Defensa del Consumidor, la responsabilidad deviene objetiva en atención de lo dispuesto por el art. 40 de la mencionada legislación.

Las normas y principios protectorios del régimen consumeril resultan enteramente aplicables a la actividad de la IA, en tanto conlleve adquisición o utilización de un servicio, en forma gratuita u onerosa, como destinatario final, en beneficio propio o de su grupo familiar o social.

8. RESPONSABILIDADES EMERGENTES:

a) Responsables genéricos

Responsabilidad por los deberes de prevención del daño.

En términos generales, existen responsables genéricos que se determinan por su factibilidad de ocasionar un daño por su acción u omisión como de prevenir el daño o mitigar sus efectos, en cuanto de ellas dependan, que se definirán en cada caso particular acorde las Recomendaciones para una Inteligencia Artificial Fiable" (subsecretaría de Tecnología de la Información, ver nota "5") y las previsiones del Art. 1710, CCC.

Cuando hablamos de responsabilidad por el desarrollo de estas actividades, referimos a su potencialidad dañosa y la consecuente obligación de prevenir la posible producción de un daño, su continuación o agravamiento, en cabeza de quien pueda ocasionar el daño por su acción u omisión sino también de quien puede evitar el daño o mitigar sus efectos.

b) Responsables específicos

Responsabilidad por actividades riesgosas

En el caso de la utilización de la IA resultan sus obligados los fabricantes, proveedores y usuarios, con distintas escalas de responsabilidad.

Usuario: Responsabilidad subjetiva: a) incumplió su deber de utilizar o supervisar el sistema de IA de conformidad con los mecanismos de

supervisión previstos al efecto y en tanto estén a su alcance, y la diligencia debida; b) Expuso el sistema de IA a datos de entrada, bajo su control, que no eran pertinentes ni adecuados a los fines previstos.

Fabricante: a) Responsabilidad objetiva, por actividad riesgosa, ante la provocación de daños, por la introducción en la comunidad de una actividad susceptible de generar daños para terceros, independientemente de su beneficio.[6]

Proveedores: a) Responsabilidad objetiva por equipararse su situación a la del fabricante en la introducción de la actividad potencialmente dañosa.

Terceros equiparados en la introducción de la actividad riesgosa: Responsabilidad objetiva, por similares fundamentos. Se trata de aquellos sujetos que, además del fabricante y proveedor, intervienen en la cadena de introducción del producto al mercado.

9. ÉTICA DE LA INTELIGENCIA ARTIFICIAL[7]

Este punto deviene esencial porque su contenido enmarca los deberes de prevención a los que debe sujetarse el uso de la IA

Es importante que los datos para los sistemas de IA se recopilen, utilicen, compartan, archiven y supriman de forma consistente con el derecho internacional y acorde a los valores y estos principios enunciados, respetando al mismo tiempo los marcos jurídicos nacionales, regionales e internacionales pertinentes.

Conforme los lineamientos de la **Unesco**, deberían reconocerse principios básicos que hacen a la Ética de la inteligencia artificial:

---

[6] XXVII Jornadas Nacionales de Derecho Civil, Santa Fe, 2019

[7] Unesco. https://www.unesco.org › recommendation-ethics y SUBSECRETARIA DE TECNOLOGIAS DE LA INFORMACION**2023-06-02**JEFATURA DE GABINETE DE MINISTROSSUBSECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Disposición 2/2023DI-2023-2-APN-SSTI#JGM

Proporcionalidad e inocuidad. Debería reconocerse que las tecnologías de la IA no garantizan necesariamente, por sí mismas, la prosperidad de los seres humanos ni del medio ambiente y los ecosistemas. En caso de que pueda producirse cualquier daño para los seres humanos, debería garantizarse la aplicación de procedimientos de evaluación de riesgos y la adopción de medidas para impedir que ese daño se produzca.

Seguridad y protección. Los daños no deseados (riesgos de seguridad) y las vulnerabilidades a los ataques (riesgos de protección) deberían ser evitados y deberían tenerse en cuenta, prevenirse y eliminarse a lo largo del ciclo de vida de los sistemas de IA para garantizar la seguridad y la protección de los seres humanos, del medio ambiente y de los ecosistemas.

Equidad y no discriminación. Los actores de la IA deberían promover la diversidad y la inclusión, garantizar la justicia social, salvaguardar la equidad y luchar contra todo tipo de discriminación, de conformidad con el derecho internacional. Los actores de la IA deberían hacer todo lo razonablemente posible por reducir al mínimo y evitar reforzar o perpetuar aplicaciones y resultados discriminatorios o sesgados a lo largo del ciclo de vida de los sistemas de IA, a fin de garantizar la equidad de dichos sistemas.

Sostenibilidad. Debería llevarse a cabo con pleno conocimiento de las repercusiones de dichas tecnologías en la sostenibilidad la evaluación continua de los efectos humanos, sociales, culturales, económicos y ambientales de las tecnologías de la IA.

Derecho a la intimidad y protección de datos. Es importante que los datos para los sistemas de IA se recopilen, utilicen, compartan, archiven y supriman de forma consistente con el derecho internacional y acorde a los valores y estos principios enunciados, respetando al mismo tiempo los marcos jurídicos nacionales, regionales e internacionales pertinentes.

Supervisión y decisión humanas. Puede ocurrir que, en algunas ocasiones, los seres humanos decidan depender de los sistemas de IA por razones de eficacia, pero la decisión de ceder el control en contextos limitados seguirá recayendo en los seres humanos, ya que estos pueden recurrir a los sistemas de IA en la adopción de decisiones y en la ejecución de tareas, pero un sistema de IA nunca podrá reemplazar la responsabilidad final de los seres humanos y su obligación de rendir cuentas.

Transparencia y explicabilidad. La transparencia y la explicabilidad de los sistemas de IA suelen ser condiciones previas fundamentales para garantizar el respeto, la protección y la promoción de los derechos humanos, las libertades fundamentales y los principios éticos. Las personas deberían tener la oportunidad de solicitar explicaciones e información al responsable de la IA o a las instituciones del sector público correspondientes. Dichos responsables deberían informar a los usuarios cuando un producto o servicio se proporcione directamente o con la ayuda de sistemas de IA de manera adecuada y oportuna.

Responsabilidad y rendición de cuentas. Deberían elaborarse mecanismos adecuados de supervisión, evaluación del impacto, auditoría y diligencia debida, incluso en lo que se refiere a la protección de los denunciantes de irregularidades, para garantizar la rendición de cuentas respecto de los sistemas de IA y de su impacto a lo largo de su ciclo de vida.

10. LA INTELIGENCIA EMOCIONAL Y LA INTELIGENCIA ARTIFICIAL.

La reproducción parcial de este blog nos lleva a los límites que la persona debe establecer en relación a la IA y de allí su transcripción.

¿Puede la IA sustituir la inteligencia emocional humana?[8]

Si nuestro cerebro cambiara a un sistema lógico de pensamiento, como funcionan los sistemas interpretativos de los sistemas de la IA; perderíamos nuestra flexibilidad mental, sería muy aburrido si fuéramos solamente lógicos, calculadores y totalmente libres de todo error. Después de todo no vivimos en un mundo estático. El cambio es lo que nos impulsa hacia adelante. Nos adaptamos al cambio en forma constante.

Tan pronto como el cerebro comete un error no solamente trata de corregirlo, sino que también lo utiliza productivamente. Es precisamente debido a que un error ofrece el potencial de mejora a sistema con defectos, el que ha prevalecido, en nuestra evolución como humanos. Este es el precio que debe pagar por nuestra capacidad de permanecer flexibles. El arte no es evitar los errores. Cualquiera que trate de evitar los errores se volverá tan

[8] https://www.telefonica.com/es/sala.comunicacion/blog/inteligencia-artificial-inteligencia-emocional-humana/

aburrido como una computadora. Y, lo que es peor, reemplazable. Entonces tarde o temprano, los algoritmos serán capaces de evitar los errores y realizar una acción en forma eficiente y sin errores. Pero reconocer que un error puede tener una finalidad, es esa capacidad que solamente tenemos los humanos. Ahora comprendemos que el cerebro casi sistemáticamente incorpora los errores para examinarlos y así alterar su conducta. Y esta es una lección muy importante para aprender: "errar es humano" y, para el cerebro, es extremadamente útil.

…La característica única del pensamiento humano yace precisamente en que no es exacto ni perfecto. Nuestro pensamiento propenso al error es la única cosa que nos hace superior a las computadoras. Esencialmente nuestra "debilidad" en el pensamiento es realmente nuestra más grande arma secreta mental.

De este análisis anterior, y hablando de emociones, nuestra "debilidad humana", también nos podríamos preguntar, ¿Cómo es que la inteligencia Artificial interpreta las emociones de una imagen o en un mensaje?, ya que las mismas delatan a los humanos, en las micro gesticulaciones que se evidencian en nuestros rostros cuando transitamos por alguna de ellas.

¿Cómo se desarrolla un detector automático de emociones de este tipo?

En primer paso es hacer una lista de emociones a partir de la variedad interminable de nuestros estados de ánimo. Tras una investigación en Nueva Guinea, con el científico Paul Ekman, psicólogo estadounidense pionero en el estudio de las emociones y su expresión facial, se evidenció que la humanidad comparte seis sentimientos universales que inevitablemente pueden ser leídos en nuestros rostros, estos son: alegría y tristeza, asco e ira, sorpresa y miedo.

Esta teoría de Paul Ekman evalúa el estudio de las emociones en su micro mímica, donde se evidencia y afirma la existencia de la verdad de las personas expresadas en su rostro.

Aunque esta clasificación es muy controvertida para los científicos, suele servir de base para todos los informáticos en el reconocimiento de emociones, justamente por su sencillez.

Estas seis emociones universales son el punto de partida. El segundo paso es conseguir que clasificadores humanos asignen miles de caras a estas

seis categorías, de esta forma se crean los datos de entrenamiento para las máquinas. Finalmente comienza el aprendizaje automático, hasta que el sistema informático logra arrojar los mismos resultados que los clasificadores humanos. Una vez hallada la mejor configuración, los sistemas se convierten en una herramienta que todos los programadores utilizan como detectores universales de emociones.

Se considera que a través de estos avances se puede creer en la idea de construir detectores de mentiras con los que se podría evaluar a un sospechoso y determinar si miente o no, lo que de alguna forma definirá si es liberado o puesto en prisión.

En la inteligencia Artificial, el análisis de las emociones se hace combinando las micro mímicas con el tono de voz. Y en estudios de imágenes y rostros en obras de arte, se llegó a esta conclusión: "No sienten nada".

La IA no tiene papilas gustativas, por lo tanto, tampoco tiene idea del delicioso gusto de un pastel de limón que revive el recuerdo de una tía o abuela. Tampoco ha sentido adrenalina en el cuerpo y la sensación que esta causa en un buen partido bien jugado. No sabe del significado de llenarse los ojos de lágrimas al emocionarse en una película, o sentir cuando nuestra nariz gotea por pura emoción. No tiene miedo de nada, no se le eriza la piel, no conoce el dolor físico ni tampoco el placer. No tiene opinión de un arte abstracto ni tampoco algún trauma reprimido, por lo tanto, no posee ninguna emoción que quiera expresar.

Podemos evidenciar que las industrias informáticas, sueñan con resaltar en los robots humanoides, dos aspectos que distinguen las capacidades humanas, hablamos de la lógica humana, versus la lógica informática, esta última, aún presenta aspectos no desarrollados.

El verdadero talento de estas redes neuronales no es tanto imitar las cualidades humanas, sino asimilar enormes bases de datos, para clasificar, analizar, y deducir correlaciones, ayudando de esta manera, a los humanos, a comprender códigos complejos como, por ejemplo, comprender el campo magnético cuántico, o también juega un papel importante en el campo farmacéuticos que determina infinitas combinaciones de químicos para una determinada enfermedad.

Una gran desventaja desde el punto de vista social es proveniente de la psicología social, ya que sondea nuestros comportamientos

estereotipados, los que son las bases de sistemas informáticos los cuales pretenden orientarnos en decisiones personales y colectivas.

En estos tipos de sistemas con los que funciona la IA, siempre existe resultados sesgados, estos sesgos pueden deberse, por ejemplo, a la existencia de prejuicios en los datos de entrenamiento, uno es consciente de que ese dato de entrenamiento fue agregado por un ser humano, el que tal vez, tenga un juicio sesgado con un determinado análisis del dato aportado. Por lo tanto, el resultado del sesgo deja la evidencia.

El contexto social, psicológico y moral, seguirá siendo incomprensible para los ordenadores, pero si estos sistemas carecen de un criterio más completo, del as cuales el hombre suele hacerse estas preguntas: ¿cómo es qué la inteligencia Artificial se basa, para tomar una decisión?

En estadísticas se evidencia que estas conducen a discriminación racial y de género. Si el sistema penal es racista, los datos también van a estar sesgados racialmente.

El avance de la inteligencia Artificial encaja perfectamente en toda nuestra pereza fundamental, porque en estos tiempos, nos ofrece la comodidad de hacerse cargo de parte de nuestras tareas cotidianas. Pero en una mirada opuesta, vemos que, en la actualidad, uno de los mayores desafíos del hombre, es tomar las riendas de su destino individual o en colectivo, sin embargo, y con el avance de la IA, es la que nos orienta a que hagamos todo lo contrario, y en muchos ámbitos sociales.

Las inteligencias artificiales, nunca alcanzan un nivel de rendimiento total, que haga prescindibles a los humanos, originando una nueva profesión, la de asistente humano de máquinas en apuros. Esta nueva forma de trabajo humano, detrás de los llamados sistemas inteligentes artificiales, fue inventado por el gigante tecnológico Amazon, donde las personas hacen a mano, por así decirlo, el trabajo necesario para que los algoritmos funcionen. El riesgo que plantea la toma de cada decisión algorítmica está dado ya que no se conoce como es que fueron tomadas las decisiones de la IA, ya que solo son visibles sus resultados.

Estamos ante una situación paradójica, por un lado, se pide a las personas que hagan lo que los robots o los procesos automáticos no son capaces de hacer, por otro lado, los empleados se enfrentan a un trabajo cuyo margen de acción o autonomía es menor que antes, controlados por una inteligencia artificial que estudia parámetros de objetivos y métricas.

Estos sistemas interpretativos sirven para dinamizar la optimización y la productividad sin permitir la negociación de quien interactúa en esa dinámica. El trabajo de las personas está sometido a los controles de las máquinas que calculan la optimización del flujo de productos, ellas determinan el ritmo de los procesos y las personas son reducidas a funcionar como robots de carne y hueso.

¿Hasta dónde llegará el avance de la IA, y en qué punto el hombre, querrá colaborar con ella, para ser sometido por estos algoritmos, en su rendimiento como una maquina Humana?

PREVENCIÓN DE DAÑOS EN MATERIA DE ACTIVIDADES RIESGOSAS DESARROLLADAS CON I.A.

Por Fernando A. Ubiría[1]

I. CONCLUSIONES

1. Los sistemas de I.A. cumplen un rol central en la gestión profesional del plan prestacional pues incrementan la expertise o know how empresario que hacen al dominio o control de la causalidad, valioso activo intangible que robustece la previsibilidad de daños en el desarrollo de actividades peligrosas, y que permite una mejor estratificación de los riesgos involucrados a partir de "datos duros" (estadísticas) que sustentan la exigibilidad de medidas preventivas.

2. No debe ser la víctima quien absorba las contingencias dañosas aunque se cumplan los "estándares" aplicables (legales o fruto del soft law materializados en severos protocolos y manuales de conducta), no alcanzan entidad de "pago" en atención a la naturaleza objetiva del sistema de responsabilidad en el que únicamente el casus tiene virtualidad fracturaria del nexo causal.

II. FUNDAMENTOS

1. LA I.A. COMO VALIOSO ACTIVO INTANGIBLE QUE ROBUSTECE LA PREVISIBILIDAD DE DAÑOS

El CCyCom. presenta una ingeniería jurídica moderna, a partir de los parámetros de tipología "abierta" o "en blanco" que identifica a la normatividad propia de la disciplina, brinda una base regulatoria generosa, dúctil, y que en términos generales logra captar adecuadamente innovaciones tecnológicas como la inteligencia artificial (arts. 1757/8).

---

[1] Profesor titular de Derecho de las Obligaciones y Derecho de Daños (UCA, Austral y UNLZ). Profesor de doctorado y de posgrados. Director del Doctorado en Ciencias Jurídicas UCA y Director del Centro de Derecho Civil UCA. Autor de libros y artículos de su especialidad. Conferencista nacional e internacional.

Ante la comprobada ineptitud del anterior sistema de responsabilidad del Código de Vélez por la estrechez de su finalidad amarrada a la dimensión reparatoria, los cambios sustantivos que se precipitaron en las últimas décadas permitió la demorada desintoxicación de nuestra disciplina de cierta "lógica" del Derecho penal (siendo un punto de inflexión la conocida "crisis de la antijuridicidad"), hasta lograrse el encumbramiento del "daño injusto" que irrumpió con el alcance de modificar ciertas bases estructurales de la disciplina para transformarla en el progresista Derecho de Daños actual.

Se impone consolidar la necesaria "cultura preventiva" erigida a partir del *alterum non laedere* y de la buena fe, principios que cimentan el novel deber de prevención legal del art. 1710 CCyCom. y la tácita obligación de seguridad del art. 961 del mismo cuerpo legal, y que imponen a todo sujeto la adopción de conductas evitatorias conforme a cierto "estándar" o "patrón", variable en función de la naturaleza del deber comprometido o de la obligación exigible, y según las circunstancias del caso.

En este marco las empresas que utilizan I.A. para mejorar la calidad de sus productos o servicios (y ganar más mercado), y que como deudor obligacional se valen de sistemas operados por I.A. en la gestión de sus actividades riesgosas, lo hacen a partir de un "plan de negocio" (jurídicamente "plan prestacional"), decisión de política comercial que apareja consecuencias: se trata del "apetito de riesgo" empresario, fruto de una evaluación y decisión de negocio, que por tanto fundamenta la consecuente imputación de las contingencias dimanantes: como reza el sabio proverbio, "donde está el beneficio está la carga" (*ubi emolumentum, ibi onus*).

Tal decisión se direcciona hacia la obtención del mayor lucro posible en el plano económico, y en lo que respecta a nuestra disciplina jurídica se destaca la "probabilidad" de producción de perjuicios, que como dato duro (más propio de las "ciencias duras" y amigo de las matemáticas) confiere sustento a la exigibilidad de medidas preventivas, análisis enmarcado en las reglas de la causalidad adecuada (arts. 1710/1713, 1726/1728 y ccds. CCyCom.).

Se verifica entonces una dinámica y simétrica interrelación entre los elementos "objeto" y "prestación" de la obligación pues la ensancha, enriquece y confiere volumen, y en la dimensión conformante del sistema general se verifica una tensión (en sentido de conflicto o puja), estamos convencidos que el tenor del interés creditorio que se tutela (el de las potenciales víctimas de daños, mayormente vulnerables) debe aparejar un

rigor simétricamente proporcional en la exigibilidad de conductas evitatorias en actividades riesgosas, medible de acuerdo a la probabilidad de producción de daños.

Por tanto resulta obligación del deudor obligacional adoptar continuas mejoras en los procedimientos para asegurar el más elevado "control" o "dominio" de la causalidad de la praxis en cuestión, que consecuentemente mejora el *know how* como valioso activo intangible que robustece la previsibilidad de daños en el desarrollo de las actividades peligrosas, y autoriza a aplicar un mayor estándar en la ejecución prestacional. Las empresas que se valen de esta tecnología –eventualmente conformantes de un pool de responsables concurrentes– logran mejorar el circuito de producción y comercialización de sus productos y servicios, y en este trance practican un "mapeo de riesgos" de sus actividades, alcanzando la referida comprensión más acabada del negocio y por tanto de sus probables implicancias dañosas que están precisadas a gestionar eficazmente.

En suma, queda de manifiesto la interactuación de los presupuestos "daño injusto" y "causalidad adecuada", mientras que el "riesgo provecho" opera como criterio de atribución o fundamento de ponderación (el que siempre fluye, resulte o no carga legal su prueba).

En esta inteligencia los algoritmos, con su capacidad para procesar grandes volúmenes de datos en la identificación de patrones y elaboración de estadísticas, mejora la actividad riesgosa en desarrollo, y es una herramienta eficaz en la identificación de probables eventos dañosos; y al incrementarse la *expertise*, el *know how* del negocio, permite una mejor estratificación de los riesgos involucrados, una suerte de "semáforo de riesgosidad" base de gestión profesional para cualquier actividad productiva.

2. VIRTUALIDAD DEL CUMPLIMIENTO DE LOS PROTOCOLOS APLICABLES

Cuando nos encontrarnos en el terreno de las actividades que categorizan como "riesgosas", cuyo amperímetro reside en la "significativa probabilidad de peligro" para terceros ponderable según criterios de causalidad adecuada, la ley es clara al disponer que *No son eximentes la autorización administrativa para el uso de la cosa o la realización de la*

actividad, ni el cumplimiento de las técnicas de prevención (art. 1757 *in fine* del CCyCom.).

En efecto, por tanto si se producen daños a pesar de haberse cumplimentado los elevados estándares existentes, sean estos legales o fruto del *soft law* que se materializan en severos protocolos y manuales de conducta fruto de políticas empresarias de *compliance*, no es la propia víctima quien deba absorberlos ya que atenerse a los protocolos no alcanza entidad de "pago" ni produce la extinción obligacional consecuente.

Técnicamente no resulta posible asignarle tamaña virtualidad pues nos encontramos dentro de un esquema fuertemente objetivo en el que sólo reviste entidad eximitoria el *casus*, complejo escenario que nos deriva hacia el fangoso terreno de los "riesgos del desarrollo".

Cabe recordar que el abordaje y direccionamiento de esta desafiante tensión o puja debe realizarse dentro del marco del Derecho del consumidor que tiene raigambre constitucional, por tanto se impone concluir que el uso de la I.A. debe siempre alinearse con la protección de derechos como principio sistémico, en el siempre difícil diálogo entre derecho y economía…

La aporía excede y en mucho el estrecho marco de nuestra especialidad, además de los ribetes constitucionales que presenta se abre hacia una dialéctica superior, enriquecida no solo por la filosofía del Derecho sino también por su politicidad y economicidad como integrantes del complejo entramado jurídico.

En suma, el desafío de integrar la inteligencia artificial en el marco jurídico existente es significativo pero no insuperable. La clave radica en desarrollar un Derecho que se adapte a las innovaciones tecnológicas con la debida protección de los derechos. La función preventiva debe por tanto prevalecer para asegurar que los avances tecnológicos no se traduzcan en perjuicios para la sociedad (declaro que este último párrafo ha sido elaborado con el auxilio de la herramienta "ChatGPT").

BIEN COMÚN Y DERECHO CIVIL. SUPUESTOS CLAVES DE LAS INSTITUCIONES CIVILES EN LAS QUE ESTÁN COMPROMETIDO EL BIEN COMÚN. EN ESPECIAL LOS DERIVADOS DE LA RESPONSABILIDAD CIVIL POR EL USO DE LAS TECNOLOGÍAS DE LA INTELIGENCIA ARTIFICIAL

Por Héctor José Miguens[1]

I. RESUMEN

Autores contemporáneos han explorado y reinterpretado la doctrina aristotélico-tomista del bien común en el contexto del derecho. Algunas referencias clave incluyen a, entre otros: 1. John Finnis (*Natural Law and Natural Rights*, 1980). 2. Alasdair MacIntyre (*After Virtue*, 1981; *Whose Justice? Which Rationality*?, 1988): (*Dependent Rational Animals*, 1999) 3. Jacques Maritain (*The Person and the Common Good*, 1946), *Man and the State*, (1951). 4. Robert P. George (*In Defense of Natural Law*, 1999).

Estos autores y otros exploran en estas y otras obras, la ley natural desde una perspectiva contemporánea, insistiendo en la importancia del bien común como criterio fundamental para evaluar la legitimidad de las leyes y de las políticas.

Lo propio ocurre respecto de los Filósofos de la Economía. Aristóteles, el Aquinate y los filósofos de la Economía modernos han elaborado una filosofía de la Economía conforme a la concepción del Bien Común, precedentemente explicada, que se sintetiza en la Ponencia.

Estos autores, entre otros, han contribuido a la revitalización de la doctrina del bien común en la teoría jurídica contemporánea, proporcionando una base para la crítica y la elaboración de sistemas legales que buscan tanto el bienestar colectivo como el individual.

---

[1] Profesor Doctor contratado en la Facultad de Derecho de la Universidad de Buenos Aires en el área del Postgrado. Doctor en Derecho por la Universidad de Navarra, España. Master en Derecho de los Estados Unidos. Facultad de Derecho de la Universidad de Santo Tomás de Aquino, Minnesota, Estados Unidos. Profesor Extraordinario del claustro académico de la Facultad de Derecho de la Universidad Austral.

Esto es aplicable a todo el régimen de protección de los consumidores y en concreto en el régimen de responsabilidad civil por el uso de las tecnologías de la Inteligencia Artificial.

II. FUNDAMENTOS

1. FILOSOFÍA DEL DERECHO EN ARISTÓTELES

Aristóteles desarrolló su doctrina sobre el bien común principalmente en su obra *Política* y, también, en la *Ética a Nicómaco*. Para Aristóteles, el bien común se refiere al bienestar y la felicidad de la comunidad política, que es el objetivo final de toda acción política y jurídica. En este sentido, el derecho tiene como finalidad promover y proteger el bien común, asegurando que la organización social y las leyes estén orientadas hacia el florecimiento de la comunidad en su conjunto.

Elementos clave de la doctrina aristotélica del bien común en el derecho son, a saber:

1. Naturaleza social del hombre: Aristóteles considera que el hombre es un ser político por naturaleza (*zoon politikon*), lo que significa que solo puede alcanzar su pleno desarrollo viviendo en comunidad. El derecho, por tanto, debe reflejar esta naturaleza social y promover la armonía y la justicia en la vida colectiva o social.

2. Justicia distributiva y correctiva: En su Ética Nicomáquea, Aristóteles diferencia entre justicia distributiva (la distribución justa de los bienes y honores dentro de la comunidad) y justicia correctiva (la rectificación de los desequilibrios y daños causados en las relaciones individuales). Ambas formas de justicia son esenciales para el bien común, ya que aseguran tanto la equidad en la distribución de los recursos como la corrección de las injusticias.

3. El gobierno de la ley: Aristóteles defiende la primacía del gobierno de la ley sobre el gobierno de los hombres. Para él, las leyes, cuando están bien hechas, son una expresión de la razón y deben guiar la vida política hacia el bien común. Esto implica que el derecho debe ser racional y orientado hacia el bien colectivo, más allá de los intereses particulares.

4. Finalidad teleológica del derecho: Según Aristóteles, todo en la naturaleza tiene un propósito o fin (*telos*). En el contexto jurídico, el fin del derecho es ordenar la vida en común de modo que se alcance el bien común.

Las leyes y normas deben, por tanto, estar diseñadas para fomentar la virtud y la felicidad de los ciudadanos, considerados en su conjunto.

2. FILOSOFÍA DEL DERECHO EN TOMÁS DE AQUINO

Tomás de Aquino desarrolló su doctrina sobre el bien común como un principio central tanto en su ética como en su filosofía política y jurídica. Influenciado por Aristóteles, pero incorporando elementos cristianos, Tomás define el bien común como el fin último de la sociedad y, por ende, de la ley. En su obra principal, la *Suma Teológica*, (y también en *De Regno*) Tomás argumenta que el derecho natural y el derecho humano deben estar orientados hacia el bien común, entendiendo este como el conjunto de condiciones sociales que permiten a todos los miembros de la comunidad alcanzar su perfección y felicidad.

Elementos clave de la doctrina tomista del bien común aplicada al derecho son, a saber:

1. Ordenación de la ley al bien común: Según Tomás, la ley es una ordenación de la razón dirigida al bien común, promulgada por quien tiene a su cargo el cuidado de la comunidad. Esto implica que cualquier ley justa debe tener como fin el bien común, entendiendo que la justicia en el derecho se mide por su contribución al bienestar colectivo. Este bien no se refiere simplemente a la suma de los bienes individuales, sino a un bien que es compartido y al que todos contribuyen y del que todos participan. La ley, así concebida, debe ser una ordenación de la razón dirigida al bien común, abarcando por igual todos los aspectos generales o comunitarios y los particulares o de los individuos.

2. El bien común y la ley natural: En la *Suma Teológica*, Tomás sostiene que el bien común está arraigado en la ley natural, la cual es una participación de la criatura racional en la ley eterna de Dios. Las leyes humanas derivadas de la ley natural promueven el bien común, reflejando el orden moral universal. Cualquier ley que se aparte de este objetivo pierde su carácter de ley para convertirse en una ley injusta o no-ley.

3. Subordinación del bien particular al bien común: Tomás enseña que el bien particular debe estar subordinado al bien común, ya que este último es más perfecto. Esto significa que las leyes deben priorizar el interés de la comunidad por encima de los intereses individuales cuando estos entran en conflicto. No obstante, ello no excluye el fin legal de atender a los intereses particulares o excluirlos en favor del bien común.

4. La justicia como virtud social y el bien común: La justicia, para Tomás, es la virtud que regula las relaciones humanas en función del bien común. Las leyes justas son aquellas que distribuyen los recursos y los derechos de manera equitativa, promoviendo la paz y la armonía sociales.

5. El rol del gobernante: Tomás considera que el gobernante, como el encargado del bien común, debe legislar de manera que las leyes sirvan a este fin. La autoridad del gobernante se legitima en la medida en que sus acciones y leyes buscan el bien común, y cualquier ejercicio de poder que no lo haga es ilegítimo. La autoridad política, por tanto, se justifica en la medida en que busca el bienestar de la comunidad en su conjunto, y no otros intereses, vg. los personales del gobernante.

3. APLICACIÓN MODERNA DE LA DOCTRINA ARISTOTÉLICO-TOMISTA DEL BIEN COMÚN EN EL ÁMBITO JURÍDICO

Autores contemporáneos han explorado y reinterpretado la doctrina aristotélico-tomista del bien común en el contexto del derecho. Algunas referencias clave incluyen a, entre otros: 1. John Finnis (*Natural Law and Natural Rights*, 1980): Finnis, filósofo jurídico influenciado por la tradición tomista y aristotélica argumenta que el bien común es central para entender la ley natural. Según Finnis, las leyes son legítimas si promueven el bien común, entendido como el conjunto de condiciones que permiten a los individuos y a la comunidad florecer. En tal sentido, el bien común comprende un conjunto de bienes básicos que permiten a las personas y a la comunidad prosperar. 2. Alasdair MacIntyre (*After Virtue*, 1981; *Whose Justice? Which Rationality*?, 1988): MacIntyre destaca la importancia de las virtudes y del bien común en la vida política y jurídica, criticando la fragmentación moral de la modernidad. Para MacIntyre, una comunidad política debe orientarse hacia un bien compartido, que se alcanza a través de prácticas y tradiciones comunes. Este autor, en su obra (*Dependent Rational Animals*, 1999) también trata sobre la importancia del bien común en la vida social y política. Critica la modernidad por su fragmentación moral y subraya la necesidad de comunidades que se orienten hacia bienes comunes compartidos, las virtudes personales, en consonancia con la tradición tomista. 3. Jacques Maritain (*The Person and the Common Good*, 1946): Maritain, integra la visión aristotélica del bien común con una perspectiva cristiana, enfatizando la dignidad de la persona humana. Para Maritain, el derecho debe equilibrar el respeto por la persona individual con la promoción del bien común. En su obra *Man and the State*, (1951), Maritain

desarrolla la idea de que el bien común es el fin último del derecho y de la política. Sostiene que la ley debe proteger tanto el bien común como la dignidad de la persona humana, considerando este equilibrio como central para una sociedad justa. Su teoría política integra el bien común tomista con una concepción moderna de los derechos humanos. 4. Robert P. George (*In Defense of Natural Law*, 1999): George explora, en esta y otras obras, la ley natural desde una perspectiva contemporánea, insistiendo en la importancia del bien común como criterio fundamental para evaluar la legitimidad de las leyes y de las políticas.

Estos autores, entre otros, han contribuido a la revitalización de la doctrina del bien común en la teoría jurídica contemporánea, proporcionando una base para la crítica y la elaboración de sistemas legales que buscan tanto el bienestar colectivo como el individual.

4. LOS FILÓSOFOS DE LA ECONOMÍA Y EL BIEN COMÚN

Aristóteles, el Aquinate y los filósofos de la Economía modernos han elaborado una filosofía de la Economía conforme a la concepción del Bien Común, precedentemente explicada, que puede sintetizarse como sigue.

Aristóteles abordó el tema del bien común en relación con la economía en sus obras *Política* y *Ética Nicomáquea*. Para él, la economía, como cualquier otra actividad humana, debe estar orientada hacia el bien común, que es el fin último de la sociedad. Aristóteles distingue entre la economía (*oikonomiké*), que es la administración del hogar y de los recursos en beneficio de la comunidad, y la crematística (*chrematistiké*), que se enfoca en la acumulación de riqueza por sí misma. La primera está subordinada al bien común, mientras que la segunda, cuando se convierte en un fin en sí mismo, es criticada por Aristóteles por ser contraria a la virtud y al orden natural.

Elementos clave en la aplicación del bien común a la economía en Aristóteles son, a saber:

1. La subordinación de la economía al bien común: Aristóteles ve la economía como una actividad natural y necesaria para el bienestar de la comunidad, pero siempre debe estar subordinada a la política y al bien común. La acumulación de riqueza no es un fin legítimo en sí mismo, sino que los recursos deben ser utilizados para satisfacer las necesidades y promover la virtud dentro de la comunidad.

2. La justa distribución de los recursos: En su concepción de la justicia distributiva, Aristóteles argumenta que los bienes deben ser distribuidos de acuerdo con el mérito y la necesidad dentro de la comunidad. Esta distribución justa es esencial para el mantenimiento del bien común y la estabilidad social.

Por otra parte, Tomás de Aquino, siguiendo a Aristóteles y a otros autores, también incorpora la noción del bien común en su análisis de la economía. Para Tomás, la actividad económica es legítima y necesaria, pero debe estar siempre orientada hacia el bien común, es decir, hacia el bienestar de la comunidad en su conjunto y no meramente hacia el enriquecimiento individual. Tomás de Aquino defiende la propiedad privada, pero sostiene que esta debe estar al servicio del bien común.

Elementos clave en la aplicación del bien común a la economía en Tomás de Aquino son, a saber:

1. Propiedad privada y bien común: Tomás de Aquino justifica la propiedad privada como un medio eficiente para gestionar los recursos, pero subraya que su uso debe estar orientado hacia el bien común. Esto implica que, aunque una persona posea bienes, debe usarlos de manera que beneficien a la comunidad, respetando el principio del destino universal de los bienes.

2. Justicia en las transacciones económicas: Tomás de Aquino aplica la noción de justicia conmutativa a la economía, insistiendo en que las transacciones deben ser justas y equitativas. Esto significa que el precio de los bienes y servicios debe reflejar su verdadero valor y que ninguna de las partes en la transacción debe ser explotada.

3. El papel del Estado en la economía: Según Tomás, el Estado tiene un papel importante en regular la economía para asegurar que esta sirva al bien común. Esto incluye la intervención en el mercado cuando sea necesario para corregir injusticias y garantizar que los recursos sean distribuidos de manera justa.

En cuanto a los Filósofos de la Economía modernos y actuales mencionamos aquí, entre otros, a Ricardo F. Crespo y la doctrina del bien común en la economía. Este autor argumenta que la economía moderna ha perdido de vista el bien común al enfocarse demasiado en la eficiencia y la maximización del beneficio, y propone una reorientación hacia una economía que sirva al bienestar integral de la sociedad.

Son obras y contribuciones de Crespo, entre otras:

- "*Aristotle's Principles for Modern Economic Science*" (2019) Este artículo es un intento de iluminar la ciencia económica actual a la luz de la filosofía de la economía de Aristóteles. El autor describe en primer lugar el pensamiento de Aristóteles sobre la economía. A continuación, distingue y discute tres principios aristotélicos: (a) la economía debe ser una ciencia práctica o moral clásica, (b) la economía no debe buscar una riqueza ilimitada, sino la riqueza necesaria para la vida buena, y (c) la economía debe tener como objetivo el bien común.

- "*Philosophy of the Economy: An Aristotelian Approach*" (2014): Crespo utiliza el marco aristotélico para defender una economía que reconozca la importancia de la ética y el bien común. Según Crespo, la economía no puede ser considerada como una ciencia autónoma, sino que debe estar subordinada a la política y a la ética.

- *A Re-Assessment of Aristotle's Economic Thought* (2014). En este libro el autor argumenta que las ideas de Aristóteles sobre la Economía y el bien común son muy relevantes para la economía contemporánea.

- *The Common Good and Economics* (2015). En esta obra el autor analiza el significado del "Bien Común" y su impacto en la Economía. Compara la noción clásica de Aristóteles y Tomás de Aquino con las principales corrientes modernas sobre este concepto, a saber: la economía de la felicidad y el enfoque de las capacidades.

Sintéticamente podemos concluir con este autor los siguientes postulados, a saber:

1. Crítica del reduccionismo económico: Crespo critica la visión reduccionista de la economía que se enfoca exclusivamente en la eficiencia y el crecimiento material. Propone una economía que tenga en cuenta el bien común, la justicia, y las necesidades humanas en su sentido más amplio, siguiendo la tradición aristotélica-tomista. El objeto de la Economía es así, el de alcanzar el Bien Común.

2. Economía como ciencia práctica: Siguiendo a Aristóteles y Tomás de Aquino, Crespo argumenta que la economía debe ser entendida como una ciencia práctica, cuyo objetivo es guiar las acciones hacia el bien común, más allá del simple cálculo de costos y beneficios. Crespo sostiene que la economía no debe ser vista como una ciencia autónoma, puramente técnica o matemática, sino como una ciencia práctica y ética. Esto significa que la

economía debe ser guiada por principios éticos y orientada hacia el bien común, en lugar de estar dominada por la lógica de la maximización del beneficio individual.

3. Integración de ética y economía: Crespo destaca la necesidad de reintroducir la ética en la economía, para que esta ciencia pueda contribuir verdaderamente al florecimiento humano. Según él, la economía debe ser una herramienta para alcanzar el bien común, respetando la dignidad humana y las necesidades de todas las personas. Esta integración es crucial para alcanzar una economía más justa y humana.

4. El bien común como fin último de la economía: Crespo, siguiendo a Aristóteles y Tomás de Aquino, argumenta que el bien común es el fin último de la economía. Para él, la economía debe contribuir al florecimiento de la comunidad, lo que implica un enfoque en el desarrollo integral de las personas, abarcando no solo sus necesidades materiales, sino también su bienestar moral y espiritual.

Todos estos postulados y teorías citados *supra* los hacemos nuestros. Veamos ahora los campos del derecho civil a los que pueden ser aplicados.

5. APLICACIONES AL DERECHO CIVIL ARGENTINO Y COMPARADO. ALGUNOS SUPUESTOS CRUCIALES DEL DERECHO CIVIL EN LOS QUE ESTÁ ESPECIALMENTE COMPROMETIDO EL BIEN COMÚN. EN ESPECIAL RESPECTO DE LOS DAÑOS DERIVADOS DEL USO DE LA INTELIGENCIA ARTIFICIAL.

La ética económica y el bien común están intrínsecamente entrelazados. Por otra parte, en otros casos no existe contenido económico en la cuestión pero sí un especial vínculo con el Bien Común. A continuación mencionados diversos supuestos en los que, *prima facie* están más estrechamente vinculados con el Bien Común, especialmente por sus raíces metafísicas, antropológicas y éticas que pueden plantearse en los distintos casos. Lógicamente, esta lista no es exhaustiva.

1. Presupuestos metafísicos, antropológicos y éticos respecto de la fundamentación de la protección de los consumidores de la Inteligencia Artificial.
2. Presupuestos metafísicos, antropológicos y éticos respecto de la fundamentación de la responsabilidad civil objetiva, es decir, toda responsabilidad que excluya el dolo o la culpa del agente causante del daño en casos de la Inteligencia Artificial.

3. *Ídem* anterior en especial en el tema de la responsabilidad civil en el ámbito de la actuación del causante del daño mediante el uso de las tecnologías de la Inteligencia Artificial.