

INFORMES

Desafíos legales de la inteligencia artificial en Chile

Legal challenges for artificial intelligence in Chile

Carlos Araya Paz 

Abogado, Chile

RESUMEN La inteligencia artificial es una tecnología que está revolucionando la forma en que la sociedad interactúa, consume y se expresa. Desde recomendaciones en motores de búsqueda hasta texto predictivo en correos electrónicos, esta tecnología ha llevado a un intenso debate que incluso abarca temas éticos. Su innegable impacto en la vida humana motiva una serie de interrogantes desde la perspectiva legal. Este artículo busca sumergirse en dichas interrogantes y proponer algunas soluciones, desde la misma tecnología y comprendiendo sus características básicas.

PALABRAS CLAVE Inteligencia artificial, innovación, responsabilidad, Chile.

ABSTRACT Artificial intelligence is a technology that is revolutionizing the way society interacts, consumes, and expresses itself. From recommendation systems in search engines to predictive text in emails this technology has generated intense debate that has even faced ethical issues. Its undeniable impact on human life motivates a series of questions from a legal perspective. This article seeks to immerse itself in these questions and propose some solutions, from the same technology and understanding its basic features.

KEYWORDS Artificial intelligence, innovation, liability, Chile.

Introducción

En la película *2001: Odisea en el espacio* del director Stanley Kubrick, uno de los personajes más recordados fue HAL 9000, un supercomputador de última generación que gobernaba la nave *Discovery 1* en una misión espacial a Júpiter. En el viaje, HAL 9000 se empieza a mostrar crítico con el éxito de la misión, interpela a los astronautas y, al no obtener respuesta, decide actuar por su cuenta simulando una avería. Ese es

el primer rasgo de humanidad de la máquina: la duda y el tomar decisiones de forma autónoma. El segundo rasgo claro de humanidad en la película viene dado por el temor a la muerte. Frente a la autonomía de HAL 9000, y el peligro que ello representa, el astronauta a cargo procede a «matar» o desconectar a HAL 9000. A pesar de ser una máquina, su desconexión resulta cargada de humanidad, lo que permite al espectador empatizar con la escena de desconexión, en contraste con la muerte de los tripulantes humanos que reposaban en la nave. En 1968, el director Stanley Kubrick nos dio una cátedra sobre el desarrollo de la inteligencia artificial y su interacción con los seres humanos.

Desde la aparición de las primeras máquinas, el hombre ha tenido una actitud de cautela y de temor frente al desarrollo que éstas puedan alcanzar en el futuro, sentimiento que ha sido fomentado por el cine y la literatura contemporánea. Al margen de la ficción, la inteligencia artificial es hoy una realidad irrefutable, desde traductores en línea hasta asistentes de conducción en vehículos motorizados.

Chile no se encuentra exento de esta irrupción tecnológica. En el 2017, la agencia Accenture publicó un estudio titulado «Cómo la inteligencia artificial puede generar crecimiento en Sudamérica». En el caso de Chile, según el estudio, la inteligencia artificial podría contribuir US\$ 63.000 millones al VAB del país en el 2035 y crear oportunidades en la industria del *retail*, financiera, comunicaciones y recursos naturales (Ovanessoff y Plastino, 2017: 19).

No cabe duda de que esta es una tecnología que ha venido a revolucionar la forma en que percibimos e interactuamos con nuestra realidad. Realidad que, al menos desde la perspectiva regulatoria, no ha dado los pasos firmes para intentar comprender este nuevo fenómeno.

Por lo anterior, este artículo busca generar propuestas que, a su vez, estimulen el dialogo y el debate en torno a la inteligencia artificial en Chile, en especial respecto de los desafíos legales que implica su uso. Dicho propósito no se encuentra exento de obstáculos, de los cuales el principal es abordar, desde la perspectiva legal, una tecnología que se encuentra en constante evolución.

Es importante mencionar que este artículo busca estimular el debate sobre el impacto que tiene la inteligencia artificial en distintas áreas del derecho, para centrarnos con más detalle en materia de responsabilidad derivada de los sistemas de inteligencia artificial.

Para los fines antes mencionados, el presente artículo se estructura en cuatro secciones. En la primera, trataremos de esbozar una definición de inteligencia artificial para entender, de ese modo, el objeto de análisis. En la segunda y tercera secciones, estudiaremos el impacto de la inteligencia artificial en distintos campos del derecho, y nos enfocaremos en la responsabilidad. En la cuarta sección, otorgaremos algunos criterios que estimamos deben ser considerados al momento de elaborar políticas

públicas en el ámbito de la inteligencia artificial. Por último, se exponen las conclusiones en relación con el estudio.

Inteligencia artificial: Definición y características

Definición

El término *inteligencia artificial* fue acuñado en 1956 por John McCarthy, Marvin Minsky, Nathaniel Rochester y Claude Shannon, en una conferencia en la Universidad de Dartmouth. Allí, los autores sentaron las bases de lo que se conoce como inteligencia artificial:

A los efectos actuales, el problema de la inteligencia artificial es el de hacer que una máquina se comporte de una manera que *se llamaría inteligente si un ser humano se comportara así*.¹

Por ende, el rasgo característico de la inteligencia artificial es su relación con la inteligencia humana como parámetro de comparación e imitación. Esto origina cuatro paradigmas de inteligencia artificial: 1) sistemas (de inteligencia artificial) que piensan como humano, 2) sistemas que actúan como humanos, 3) sistemas que piensan racionalmente, y 4) sistemas que actúan racionalmente cuyos detalles se muestran en la **figura 1** (Norvig y Russell, *Inteligencia Artificial: un enfoque moderno* 2004). La utilización de un paradigma u otro depende del objeto de estudio y de la capacidad que deseamos dotar a un sistema.

Sistemas que piensan como humanos	Sistemas que piensan racionalmente
«El nuevo y excitante esfuerzo de hacer que los computadores piensen... máquinas con mentes, en el más amplio sentido literal». (Haugeland, 1985) «[La automatización de] actividades que vinculamos con procesos de pensamiento humano, actividades como la toma de decisiones, resolución de problemas, aprendizaje...» (Bellman, 1978)	«El estudio de las facultades mentales mediante el uso de modelos computacionales». (Charniak y McDermott, 1985) «El estudio de los cálculos que hacen posible percibir, razonar y actuar». (Winston, 1992)
Sistemas que actúan como humanos	Sistemas que actúan racionalmente
«El arte de desarrollar máquinas con capacidad para realizar funciones que cuando son realizadas por personas requieren de inteligencia». (Kurzweil, 1990) «El estudio de cómo lograr que los computadores realicen tareas que, por el momento, los humanos hacen mejor». (Rich y Knight, 1991)	«La Inteligencia Computacional es el estudio del diseño de agentes inteligentes». (Poole <i>et al.</i> , 1998) «IA... está relacionada con conductas inteligentes en artefactos». (Nilsson, 1998)

Figura 1. Algunas definiciones de inteligencia artificial, organizadas en cuatro categorías

1. Gill Press, «Artificial intelligence (AI) defined», *Forbes*, 27 de agosto de 2017, disponible en <https://bit.ly/2ApDKM2> (el destacado es nuestro).

Debido a estos paradigmas, la inteligencia artificial es una ciencia multidisciplinaria que involucra teorías y modelos de las ciencias cognitivas, lingüística, neurociencias, matemáticas, informática y biología, entre otras. Por otro lado, con el fin de desarrollar sistemas inteligentes que utilicen capacidades cognitivas cercanas a las humanas (como la capacidad de distinguir, de clasificar, de decidir, de resolver problemas, de aprender, de adaptarse, etcétera), la inteligencia artificial se basa en el trabajo de varias ramas, como la representación de conocimiento, aprendizaje automático (*machine learning*), visión artificial, robótica, agentes autónomos, planificación y razonamiento automático, búsqueda y resolución de problemas, y procesamiento de lenguaje natural.

Cualquiera sea la rama de inteligencia artificial analizada, en general, esta va tener un impacto o un efecto material en el mundo. Es lo que el profesor Calo señala al decir que los sistemas «toman información del mundo, la procesan y actúan sobre el mismo», proceso que toma el nombre de *ciclo percepción-razonamiento-acción* (Calo, 2015: 529).

La capacidad de actuar físicamente sobre el mundo se traduce, a su vez, en la posibilidad eventual de dañar a personas o bienes (Calo, 2015: 534). Desde luego, no toda inteligencia artificial es capaz de dañar en forma física a personas o bienes. Un traductor automático que trabaje con una red neuronal difícilmente podrá herir a alguien, a diferencia de un dron autónomo.

Es precisamente dicha característica, la posibilidad de impactar en el mundo material, lo que hace necesario la elaboración de propuestas regulatorias en materia de inteligencia artificial, tomando en consideración particular la arquitectura básica que compone un sistema de estas características.

Características de la inteligencia artificial

En la presente sección analizaremos los complejos aspectos que hacen de la inteligencia artificial una tecnología única y que, a su vez, influyen en la forma en que impacta en el derecho.

Según Scherer (2016: 363), la inteligencia artificial se estructura, principalmente, sobre la base de tres elementos: autonomía, imprevisibilidad y falta de control.

Autonomía

Uno de los rasgos más distintivos de la inteligencia artificial en relación con tecnologías de automatización tradicional, es su capacidad de ejecutar actividades de diversa complejidad en forma autónoma, es decir, sin supervisión o control humano. El grado de autonomía dependerá del nivel de sofisticación del sistema de inteligencia artificial.

Imprevisibilidad

Un segundo rasgo distintivo de la inteligencia artificial es la imprevisibilidad de su comportamiento, es decir, que su actuar no sigue necesariamente una secuencia de razonamiento que un ser humano pueda prever o deducir de forma lógica. En otras palabras, los sistemas de inteligencia artificial se encuentran diseñados para tener un razonamiento creativo, ilógico o «fuera de la caja».² Un ejemplo de ello son los juegos computacionales de ajedrez, en los que ciertas jugadas pueden ir contra los principios básicos de estrategias humanas en dicho juego (Scherer, 2016: 363).

Los seres humanos, sujetos a las restricciones cognitivas del cerebro, son incapaces de analizar toda o la mayor parte de la información a su disposición en un período limitado de tiempo, para solucionar un problema dado. En ese sentido, los seres humanos muchas veces buscan una solución satisfactoria en lugar de una solución óptima. Es decir, frente a un problema dado, van a buscar una respuesta que solucione dicho problema, aunque puede que la respuesta diste de ser la óptima. Por el contrario, un sistema de inteligencia artificial puede buscar una solución a un problema complejo —desde el punto de vista cognitivo— a través del análisis de muchas más variables, en un tiempo más eficiente y de forma más efectiva, en comparación con un ser humano (Scherer, 2016: 364).

La solución que provee un sistema de inteligencia artificial para una determinada tarea por lo general no ha sido prevista por el diseñador o programador, pues la gran mayoría de los modelos funcionan a partir de la experiencia de aprendizaje posterior al diseño. Es la imprevisibilidad una característica que fortalece y hace atractiva la inteligencia artificial en los distintos campos, pues proporciona soluciones a problemas que no pudieron preverse ni resolverse inicialmente por medio de alternativas lógicas.

Falta de control

La autonomía de los sistemas de inteligencia artificial no solo genera consecuencias derivadas de su imprevisibilidad para actuar, sino que también respecto de su falta de control en ciertos casos. Esto quiere decir que podría ser difícil para los humanos mantener el control de sistemas que están diseñados para actuar con un considerable grado de autonomía.

Según Scherer (2016: 367), una pérdida de control puede darse en dos niveles: una pérdida de control local (que ocurre cuando el sistema no puede ser controlado por la persona legalmente responsable de su operación y supervisión); y una pérdida de control general (que ocurre cuando el sistema no puede ser controlado por ninguna

2. El razonamiento «fuera de la caja» (*outside of the box*) es una metáfora que alude al razonamiento no convencional o no lógico. Es decir, para la consecución de un resultado dado se sigue una secuencia de razonamiento que no resultaría lógica si dicha secuencia fuese ejecutada por un humano.

persona). Frente a un escenario de pérdida de control, sea local o general, cobran relevancia los objetivos con los que fue diseñado inicialmente el sistema de inteligencia artificial, pues en caso de pérdida de control, el sistema igualmente actuaría sobre la base del objetivo inicial con el que fue programado. Sin perjuicio de ello, asegurar una alineación entre intereses y objetivos puede ser bastante difícil en la práctica, en particular porque los valores humanos son casi imposibles de definir con precisión, y porque el lenguaje humano admite múltiples interpretaciones³.

Entonces, autonomía, imprevisibilidad de comportamiento y eventual falta de control son los elementos que integran las características básicas de un sistema de inteligencia artificial. Cualquier sistema que no tenga alguno de los elementos antes mencionado, puede ser un sistema altamente sofisticado desde la perspectiva técnica, pero no es un sistema de inteligencia artificial propiamente tal. Las referencias que se efectúan a los sistemas de inteligencia artificial en este artículo suponen —en lo sucesivo— la concurrencia copulativa de las tres características antes mencionadas. Cómo interactúan estas características y cómo influyen en el derecho, será analizado en la siguiente sección.

Impacto de la inteligencia artificial en distintas ramas del derecho

En esta sección, analizaremos de forma general el impacto de la inteligencia artificial en distintas ramas del derecho, para profundizar en la siguiente en materia de responsabilidad legal.

Impacto en materia de propiedad intelectual

En materia de propiedad intelectual se plantean interesantes interrogantes en relación con la titularidad de creaciones desarrolladas por sofisticados sistemas de inteligencia artificial. En el ámbito del derecho de autor, cabe preguntarse qué sucederá cuando un sistema de inteligencia artificial desarrolle una obra literaria original y novedosa, o cuando desarrolle un software. ¿Podría operar una presunción de titularidad en favor de la persona jurídica que encargó el desarrollo del sistema de inteligencia artificial, como ocurre, por ejemplo, con las personas jurídicas que encargan el desarrollo de un software? Del mismo modo, en el ámbito de privilegios industriales, como en materia de patentes farmacéuticas de alto impacto en la salud pública, ¿qué sucederá cuando un sistema de inteligencia artificial —con capacidad ilimitada para analizar el arte previo— desarrolle invenciones sofisticadas en el área farmacéutica?

3. Por ejemplo, podríamos diseñar una inteligencia artificial para que «minimice el sufrimiento humano». Dado que los humanos siempre encontrarán una forma de sufrir, incluso en el mejor escenario, la solución óptima para un sistema de inteligencia artificial sería acabar con la raza humana. Sin humanos, ya no hay sufrimiento y se consigue el objetivo inicial (Scherer, 2016: 367).

La empresa que desarrolló el sistema de inteligencia artificial creador o inventivo, ¿será titular del software de inteligencia artificial o de la creación misma desarrollada por el sistema de inteligencia artificial? Cabe señalar que, para reconocerle derechos a una entidad de inteligencia artificial, tendría que reconocérsele antes como un sujeto de derecho, capaz de ejercer derechos y contraer obligaciones. Un área gris que no muchos se atreven cruzar y que abordaremos brevemente en el siguiente apartado.

Un segundo desafío que plantea esta materia es el uso de material protegido por el derecho de autor para entrenar modelos de *machine learning*. Una fotografía, un video o un texto en prosa usado para entrenar los mencionados modelos se encuentran sujetos a altos costos transaccionales para su uso y entrenamiento, pudiendo existir una eventual barrera para el desarrollo de esta tecnología en Chile.

Impacto en materia civil como sujeto de derecho: Reconocimiento de personalidad jurídica

El reconocimiento de personalidad jurídica a un sistema de inteligencia artificial ha sido tema de intenso debate. Para efectos de ser considerado un sujeto de derecho, nuestra normativa distingue entre persona natural y persona jurídica. Dentro de los atributos de la personalidad propios de las personas naturales se encuentran: el nombre, la capacidad, la nacionalidad, el domicilio, el estado civil, el patrimonio y los derechos de la personalidad. Por su parte, dentro de los atributos de la personalidad propios de las personas jurídicas se encuentran: el nombre, el domicilio, la nacionalidad, el patrimonio y la capacidad.

Cabe por ende preguntarse, ¿podría un sistema de inteligencia artificial estar dotado de los atributos mencionados? Los sistemas de inteligencia artificial tienen, en general, las siguientes cualidades: la capacidad de comunicarse; una representación del mundo exterior con el que interactúan; la capacidad de alcanzar los objetivos específicos; un cierto nivel de creatividad (pensamiento «fuera de la caja»); y se encuentran dotados de un grado de autonomía e imprevisibilidad. Por consiguiente, ¿cabe otorgar algún reconocimiento legal, como sujeto de derecho, a los sistemas de inteligencia artificial por el mero hecho de estar dotados de estas características? La respuesta dependerá de si en el futuro los sistemas de inteligencia artificial serán o no capaces de ejercer derechos y contraer obligaciones. Por de pronto, expertos de la Unión Europea publicaron una carta abierta, en que solicitaban a la Comisión de la Unión Europea desistir de la iniciativa de otorgar «personalidad electrónica» a los sistemas avanzados de inteligencia artificial, dado que el otorgamiento de un estatus jurídico para los sistemas de inteligencia artificial implicaría reconocer derechos fundamentales como integridad y dignidad a entes que no lo tienen, por lo que

quebrantarían la Carta Fundamental de Derechos Humanos de la Unión Europea.⁴ Plantearse estas interrogantes tomando en cuenta el actual estado del arte en materia de inteligencia artificial parece no tener mucho sentido, pero sin duda creemos que a futuro será un tema de intenso debate.

Impacto en materia laboral

La irrupción de sistemas de inteligencia artificial y robótica generará sin duda un impacto en empleos de baja calificación como operarios de maquinarias, operadores de *call centers* y en el área de servicios, taxistas o choferes de buses.⁵ A su vez, la irrupción de dicha tecnología también generará impacto en empleos más calificados. Un ejemplo de ello son los corredores de bolsa, pues algunos de los principales fondos de inversión y corredoras están usando modelos de *machine learning* para analizar con eficiencia los movimientos bursátiles de las acciones del mercado, con lo que logran identificar patrones que pueden significar mayores ganancias.

Lo anterior puede sonar a ciencia ficción, pero lo cierto es que ya está ocurriendo. Un ejemplo en Chile fue la huelga legal de los trabajadores de la empresa de monitoreo de medios Litoralpress,⁶ en que la empresa decidió reemplazar a los trabajadores en huelga legal con un sistema electrónico automatizado, lo que hizo surgir la duda sobre la legalidad de dicho reemplazo y motivó una consulta a la Dirección del Trabajo, la que se pronunció a través del Dictamen Ord. 448/6 del 4 de enero de 2018. Sobre este punto, el Dictamen parte señalando que las facultades empresariales no son eliminadas, sino delimitadas durante una huelga legal; en ese sentido, reconoció que

la decisión de utilizar dispositivos o sistemas electrónicos o automatizados aplicados a un proceso productivo sustituyendo la operación humana y cuyos objetivos apuntan a mejorar la productividad [...] corresponde entenderla dentro de las facultades de administración empresariales. Se trata de opciones y estrategias empresariales (*per se*) lícitas, y que encuentran fundamento tanto en la Constitución como en la ley.

4. «Open letter to the European Commission Artificial Intelligence and Robotics», Robotics Open Letter, disponible en <http://www.robotics-openletter.eu/>.

5. De hecho, en la actualidad, los vagones de la Línea 6 del Metro de Santiago incorporan pilotaje automático, es decir, no tienen conductores. «Sin conductores ni boleterías: Así es la nueva Línea 6 del Metro que conecta a siete comunas», *ADN Radio*, 2 de noviembre de 2017 disponible en <https://bit.ly/2ziutcl>.

6. Litoralpress es una empresa dedicada al monitoreo de medios. Sus trabajadores comenzaron una huelga legal exigiendo una serie de beneficios al empleador, entre los que se destacan bonos de reconocimiento de trabajo nocturno, seguro de salud y días de permiso. Gabriel Angulo González, «Periodistas de Litoralpress en huelga ante eventual “automatización” de sus funciones», *Fortín Mapocho*, 5 de julio de 2017, disponible en <https://bit.ly/2XR97Hn>.

Sin embargo, concluyó:

la utilización por parte de la empresa de un sistema automatizado, con ocasión y como respuesta a la huelga, cuyo resultado es eludir o mitigar sus naturales efectos, determinaría un ejercicio abusivo de las potestades empresariales y una conducta contraria a derecho, desde que tal medida empresarial incumple las condiciones que impone la ley al regular las atribuciones funcionales del empleador durante la huelga, provocando la consiguiente afectación ilícita de este derecho fundamental.

En definitiva, a juicio de la Dirección del Trabajo, el reemplazo de trabajadores en huelga legal resulta ilícito, independiente de si éste lo hacen personas o a través de máquinas, dispositivos o medios tecnológicos autónomos.

Impacto en materia de privacidad y tratamiento de datos personales

Tal como nuestro cerebro trabaja sobre la base de información, la inteligencia artificial se estructura sobre la base de datos, y para los efectos de este artículo, datos personales. En Chile, los datos personales y su tratamiento se encuentran regulados en la Ley 19.628 Sobre Protección de la Vida Privada y protegidos a nivel constitucional por el artículo 19 numeral 4 de la Constitución de la República de Chile. Algunos problemas que plantea la normativa antes señalada en relación con el tratamiento de datos personales al alero de la inteligencia artificial son los siguientes:

Finalidad en el tratamiento de datos personales

De acuerdo con lo señalado en la primera sección de este artículo, existen técnicas de *machine learning* que presentan complejidad ya sea en el modelo o en los algoritmos, lo que hace que la interpretabilidad de dichas técnicas por parte de humanos sea limitada o nula. Es por dicha razón que el tratamiento de datos personales por sofisticadas técnicas de inteligencia artificial, como el mencionado *machine learning*, puede hacerse de una forma y una finalidad distinta de la que en principio se había programado. Lo anterior implica que los titulares de los datos personales no puedan controlar la finalidad con que entregan estos datos, lo que muchas veces es contrario al principio de finalidad, pero necesario para que el sistema logre el objetivo para el que fue diseñado.

Autorización para el tratamiento de datos personales

Un supuesto general de admisibilidad del tratamiento de datos personales lo supone la autorización de su titular y la posibilidad que éste tiene de retirar libremente dicha autorización. El problema puede generarse si el retiro de autorización por parte del titular de los datos afectase o comprometiese el resultado y precisión de un modelo

determinado. De igual manera, no resultaría fácil en la práctica retirar su autorización cuando los datos personales ya han sido tratados y se encuentran implicados con la información ya procesada.

Calidad de los datos en el tratamiento de datos personales

La calidad supone que los datos sean exactos, actuales y veraces. ¿Qué sucederá cuando un paciente omite por ignorancia información clave para un diagnóstico correcto por un sistema de inteligencia artificial en el ámbito de la salud? ¿Qué ocurre cuando ese mismo paciente omite que tuvo una enfermedad de transmisión sexual al proporcionar sus datos personales, en un contexto del diagnóstico de una enfermedad, y ello incide en el tratamiento automatizado efectuado por un sistema de inteligencia artificial? ¿Qué sucede cuando la información que proporciona una persona sobre sus datos no se encuentra actualizada o no es fidedigna?

En la actualidad existe un proyecto de ley en el Congreso que plantea una serie de desafíos en esta materia, sobre todo en materia de interés legítimo, transparencia y el derecho de oposición en valoraciones automatizadas. Desafíos que resultan relevantes si se consideran los problemas que derivan de las ramas científicas que involucran tomas de decisiones autónomas, principalmente, la transparencia de los modelos computacionales generados y los sesgos de los métodos y/o conocimientos utilizados por modelos previos en el caso de algoritmos de *machine learning*.

Inteligencia artificial en el ámbito de la responsabilidad legal: Regímenes de responsabilidad legal

Uno de los temas más problemáticos que enfrenta la inteligencia artificial consiste en el régimen de responsabilidad legal aplicable. Como mencionamos, la inteligencia artificial genera un impacto en la vida cotidiana, y ese impacto puede eventualmente traer consigo daños para los seres humanos que acceden a dicha tecnología. Para ilustrar lo anterior, supongamos el ejemplo de los vehículos totalmente autónomos. Una persona conduce un vehículo totalmente autónomo cuando, de pronto, un grupo de seis niños se cruzan jugando por la calle. No hay tiempo para que el vehículo se detenga. Puede virar bruscamente fuera de la vía y causar la muerte de su pasajero, o puede atropellar a los seis niños que se cruzan en la vía. Otro ejemplo: un dron autónomo de vigilancia cae sobre un patio donde unos niños juegan, lo que causa la muerte de uno de ellos. En el plano de la medicina, un programa que funciona con inteligencia artificial diagnostica de manera errada a un paciente, lo que causa su muerte, o suministra un remedio inapto para la enfermedad que padece. O, quizás más común en el futuro, un marcapasos conectado al corazón que deja de funcionar correctamente y termina matando a la persona que tiene el aparato. Asumiendo que

en dichos casos no existe un control humano sobre los dispositivos implementados con inteligencia artificial, cabe preguntarse quién es el responsable tras los daños. ¿Existe en la actualidad un esquema de responsabilidad que nos permita establecer con claridad quién es el responsable tras los hechos dañosos?

Para dar respuesta a la pregunta, debemos examinar —aunque sea brevemente— el marco normativo actual de responsabilidad legal en Chile, para luego determinar si puede o no resultar aplicable al ámbito de la inteligencia artificial.

Cuando hablamos de responsabilidad legal, hay que distinguir dos sistemas: la responsabilidad penal y la responsabilidad civil, y, dentro de esta última, la responsabilidad contractual y la responsabilidad extracontractual.

Responsabilidad penal en Chile

La responsabilidad penal en Chile deriva de la comisión de un delito, es decir, es la consecuencia de un delito. En palabras del profesor Felipe de la Fuente, la responsabilidad penal es «una situación jurídica que afecta a las personas que han cometido un delito y que consiste en la obligación de soportar la pena asignada a ese hecho, en el grado que la ley determine para cada una de ellas» (De la Fuente Hulaud, 1990: 123). Los elementos que componen dicha responsabilidad penal son, a grandes rasgos: i) una conducta humana, que puede ser una acción o una omisión (Politoff, Matus y Ramírez, 2003: 163);⁷ ii) un tipo penal, es decir, los elementos que describen un delito determinado, y que puede a su vez incorporar un elemento objetivo (descripción de la conducta punible) y un elemento subjetivo (modalidades de la conducta punible, dolo, culpa o preterintención); iii) antijuricidad, es decir, contrariedad de la acción con todo ordenamiento jurídico; y iv) culpabilidad, esto es, juicio de reproche que se le dirige al autor de un delito, por haber actuado como actuó, en circunstancias en que podía haber conformado su actuar al mandato de la norma.

Como ya hemos señalado, el derecho penal solo es aplicable a las personas naturales. Sin embargo, la Ley 20.393 establece la responsabilidad penal de las personas jurídicas en los delitos de lavado de activos, financiamiento del terrorismo y delitos de cohecho. La Ley establece un modelo de prevención de ciertos delitos que, implementada correctamente, puede eximir de responsabilidad penal a las empresas que lo implementan. Las penas a las que se expone la persona jurídica pueden incluir:

- i) la disolución o cancelación de la persona jurídica; ii) la prohibición temporal o perpetua de celebrar actos y contratos con los organismos del Estado; iii) la pérdida

7. Esto es relevante porque para que un delito sea punible debe tratarse de una conducta humana, ni los animales ni las cosas que actúan son capaces de generar responsabilidad penal.

parcial o total de beneficios fiscales o prohibición absoluta de recepción de éstos por un período determinado; iv) multa a beneficio fiscal; y vi) las penas accesorias.⁸

Un sistema de inteligencia artificial no podría ser susceptible de responsabilidad penal, pues no se satisfacen los elementos de dicha responsabilidad, partiendo de la base que no estamos frente a una conducta humana. Subsiste la pregunta: ¿podría perseguirse responsabilidad penal contra el desarrollador o del fabricante del sistema de inteligencia artificial?

Para dar con la respuesta, cabe recordar que una de las características de los sistemas de inteligencia artificial es que funcionan de forma autónoma, es decir, no existe un control humano de ellos, y que, además, son imprevisibles, por lo que su comportamiento no puede ser previsto por su desarrollador. Además, gracias al procedimiento de *deep learning*, un sistema de inteligencia artificial puede desarrollar un código de conducta propio más allá del que se le impuso en un principio al ser programado. No podría, por ende, caberle responsabilidad penal al desarrollador o al fabricante, porque no desplegó ninguna conducta punible. No podría considerársele tampoco autor, ni cómplice, ni encubridor en el hecho delictivo.

Ahora bien, puede sonar a ciencia ficción, pero ¿qué sucede si alguien diseña y desarrolla un dron implementado con un sistema de inteligencia artificial, con reconocimiento facial, para asesinar? Hoy existen las herramientas para ello. Creemos que, en ese caso, el escenario es distinto. El dron diseñado con inteligencia artificial sería asimilable a un arma, y habría que tener en consideración lo prescrito por el Decreto 400 Sobre Control de Armas, control que radica en el Ministerio de Defensa a través de la Dirección General de Movilización, y que sanciona a los que fabrican, arman, modifican o internan al país armas sometidas a control sin la autorización respectiva.⁹

Del mismo modo, ¿qué sucede si una empresa desarrolla un algoritmo con un sistema de inteligencia artificial programado para el lavado de activos? Al igual que en el caso anterior, el sistema de inteligencia artificial acá tiene un rol meramente instrumental, y en este caso, no solo estaríamos ante una asociación ilícita, sino también habría infracción a las normas de la Ley 20.393.

En definitiva, respecto de la responsabilidad penal en el ámbito de la inteligencia artificial, debemos distinguir: i) cuando ésta se ocupa como un mero instrumento

8. Artículo 8 de la Ley 20.393 que Establece la Responsabilidad Penal de las Personas Jurídicas en los delitos que indica.

9. Artículo 10 inciso primero del Decreto 400, que prescribe: «Los que sin la competente autorización fabricaren, armaren, elaboraren, adaptaren, transformaren, importaren, internaren al país, exportaren, transportaren, almacenaren, distribuyeren, ofrecieren, adquirieren o celebraren convenciones respecto de los elementos indicados en las letras b), c), d) y e) del artículo 2 serán sancionados con la pena de presidio mayor en su grado mínimo».

para la comisión de un delito, en cuyo caso el responsable será quien usó o diseñó la inteligencia artificial para dichos fines; y ii) cuando es el sistema de inteligencia artificial el que directamente genera un hecho ilícito, en cuyo caso, estimamos que no podría perseguirse la responsabilidad penal de la máquina ni del desarrollador, al fallar elementos básicos que configuran el delito. En este segundo caso, estimamos que el derecho penal resulta insuficiente para proveer soluciones a la víctima de un hecho ilícito. En la siguiente sección, analizaremos si el derecho civil es capaz de proporcionarnos una solución actual a la problemática de la responsabilidad legal derivada de los sistemas de inteligencia artificial.

Responsabilidad civil en Chile

Responsabilidad civil contractual

La responsabilidad civil contractual supone: i) que entre las partes exista un contrato válido; ii) que el daño sea ocasionado por una de las partes en perjuicio de la otra; y iii) que el daño provenga del incumplimiento y no de otra actuación del deudor. En la actualidad, ya existen sistemas de inteligencia artificial que pueden preparar y revisar contratos más eficiente y rápidamente que un abogado.¹⁰ Sin embargo, una cosa es preparar y redactar un contrato, y otra cosa es concurrir con facultades de representación para suscribir y obligarse por un contrato y luego infringirlo. Este último escenario es el que surge con ocasión de la responsabilidad civil contractual.

Por ende, cabe preguntarse: ¿tiene legalmente capacidad para obligarse y suscribir un contrato un sistema de inteligencia artificial, comprendiendo a cabalidad las obligaciones que asume y las consecuencias de su incumplimiento? Podría ser un escenario probable, pero ¿quién suscribiría en la actualidad un contrato con un sistema de inteligencia artificial? ¿Qué tipo de capacidad legal tendría un sistema de inteligencia artificial para concurrir a la celebración de un contrato? Este escenario, al igual que en el caso del derecho de autor, supone reconocer personalidad jurídica al sistema de inteligencia artificial. Por consiguiente, la responsabilidad civil contractual en materia de inteligencia artificial sería difícil de configurar en la actualidad.

Responsabilidad civil extracontractual: Fundamentos de la responsabilidad

Distinto es el caso respecto de la responsabilidad civil extracontractual. Este tipo de responsabilidad deriva de los delitos o cuasidelitos civiles, esto es, aquellos hechos ilícitos, dolosos o culpables que causan daño a un tercero. La responsabilidad civil se

10. York Perry, «Inteligencia artificial vence a escuadrón de abogados analizando contratos», *Fayerwayer*, 28 de febrero de 2018, disponible en <https://bit.ly/3eHzW7C>; Beverly Rich, «How AI is changing contracts», *Harvard Business Review*, 12 de febrero de 2018, disponible en <https://bit.ly/2U6g3iy>.

traduce en la obligación de indemnizar ese daño, el cual, a su vez, puede emanar del hecho propio, o bien del hecho de un tercero por el cual se es civilmente responsable.

Tradicionalmente, se ha sostenido que el fundamento de la responsabilidad civil extracontractual reside en dos modelos: responsabilidad por culpa o negligencia (que hace responsable al que causa el daño actuando con dolo o culpa) y responsabilidad estricta u objetiva (que establece la obligación de reparar un daño ocasionado en el ejercicio de cierta actividad, independiente del grado de dolo o culpa o de la diligencia empleada). Existe, por lo demás, una tercera forma de atribución de responsabilidad, ligada con la responsabilidad civil contractual, y se refiere al seguro privado obligatorio, en virtud del cual, se establece la obligación legal de contratar un seguro de responsabilidad por parte de quien realiza una actividad susceptible de generar daño o de quien corre el riesgo de accidente, para garantizar así la reparación de la víctima.

La *responsabilidad civil extracontractual por culpa o negligencia* es la regla general en el derecho chileno. De acuerdo con lo ya señalado, la razón para atribuir responsabilidad a un tercero bajo este modelo es que ha causado un daño por una acción culpable o negligente. Los elementos que integran este régimen de responsabilidad son: i) acción u omisión (hecho voluntario); ii) culpa (negligencia) o dolo; iii) el daño; y iv) relación de causalidad entre la acción u omisión dolosa o culpable y el daño.

En cuanto al primer elemento, la regla general en materia de responsabilidad civil es la capacidad, según se desprende del artículo 1.446 del Código Civil.¹¹ La excepción, es decir, quiénes son considerados incapaces de delito o cuasidelito civil, son los casos que señala el artículo 2.319 del mismo cuerpo legal: los dementes, los infantes y los mayores de siete, pero menores de dieciséis años.¹²

Un obstáculo que deriva del primer elemento de la responsabilidad, es decir, de la capacidad, es que según la regla general del Código Civil, toda *persona* es legalmente capaz. Para que un sistema de inteligencia artificial sea considerado persona, primero tendría que reconocérsele personalidad jurídica, esto es, la facultad de contraer obligaciones y ejercer derechos. Como antes se señaló, reconocerle personalidad jurídica a un sistema de inteligencia artificial resulta problemático y legalmente cuestionable, y es un paso que, hasta ahora, ningún país ha dado.

Por ende, al no poder concurrir el primer elemento de la responsabilidad extracontractual, difícilmente podríamos atribuir responsabilidad a un sistema de inteli-

11. Artículo 1.446 del Código Civil: «Toda persona es legalmente capaz, excepto aquellas que la ley declara incapaces».

12. Artículo 2.319 del Código Civil: «No son capaces de delito o cuasidelito los menores de siete años ni los dementes; pero serán responsables de los daños causados por ellos las personas a cuyo cargo estén, si pudiere imputárseles negligencia. Queda a la prudencia del juez determinar si el menor de dieciséis años ha cometido el delito o cuasidelito sin discernimiento; y en este caso se seguirá la regla del inciso anterior».

gencia artificial bajo el régimen de responsabilidad por culpa. Subsiste la pregunta de qué sucede con aquellos sistemas de inteligencia artificial diseñados para causar daño, como un dron totalmente autónomo que dispara balas y causa daños en la población, o la máquina robótica que en una cirugía funciona de forma imperfecta y causa la muerte del paciente. ¿Puede decirse que el dron causó un daño actuando con dolo? ¿Puede afirmarse que la máquina robótica actuó con negligencia?

En el caso del dron totalmente autónomo, cabe hacer presente que fue diseñado para causar daño, por lo que es la empresa que lo diseñó la responsable en cualquier evento, el sistema de inteligencia artificial es solo la herramienta de perpetración del hecho ilícito. Lo anterior se asemeja a un régimen de responsabilidad objetiva, que examinaremos más adelante. En el caso de la máquina robótica que efectuaba la cirugía, cabe preguntarse si operaba de forma autónoma o bajo instrucciones humanas, y en ambos casos, si se encontraba debidamente mantenida. Independiente de los factores mencionados, se ha sostenido en estos casos que por lo general la responsabilidad médica es de tipo contractual, pues la fuente de las obligaciones deriva del contrato de prestación de servicios de médicos. Tal como señala Vidal, “en estos, es posible construir una relación jurídica obligatoria entre médico y hospital con el paciente, la que producirá efectos propiamente contractuales en caso de incumplimiento y daños subsecuentes” (2002).¹³

En este punto también surge la interrogante respecto del consentimiento de la eventual víctima y la aceptación de riesgos. Supongamos el caso de quien juega un videojuego violento de realidad virtual, en el que el jugador simula experiencias extremas que el mismo juego le dispone, y como consecuencia de dichas experiencias fuertes, le da un paro cardíaco. La realidad virtual, en ese contexto, puede ser una actividad riesgosa. El juego ha funcionado de forma correcta, no existe una alteración en su código fuente, solo que las condiciones de salud del jugador no eran compatibles con el videojuego de realidad virtual. No resultaría inusual que entre el usuario del juego y el diseñador existan acuerdos previos sobre responsabilidad, por medio de los cuales, por ejemplo, se acepta un cierto riesgo por parte del usuario, se modifiquen las condiciones de responsabilidad o se limitan los daños indemnizables. La suscripción de dichos acuerdos excluye la culpabilidad del diseñador que creó el juego y que funcionó de forma correcta, en la medida que se tenga en consideración ciertos límites: dichos acuerdos no pueden validar un acto ilegal o contrario a las buenas costumbres (artículo 1.461 del Código Civil); tampoco pueden importar la condonación del dolo futuro (artículo 1.465 del Código Civil); por último, no pueden significar la

13. En Chile, muchos hospitales cuentan con protocolos de mantenimiento preventivo de equipos, los que son constantemente actualizados. Por su parte, el Ministerio de Salud tiene disposiciones, como la Resolución Exenta 1.341 del 24 de noviembre de 2017, que aprueba la Norma de Seguridad del Paciente y Calidad en la Atención respecto a Mantenimiento Preventivo de Equipamiento Crítico.

renuncia a derechos indisponibles, como la vida o la integridad física (artículo 12 del Código Civil) (Barros, 2010: 138). De igual forma, en estos casos existe un deber de información acerca de la entidad del riesgo cuando existe asimetría de información entre quien ofrece la actividad riesgosa (diseñador) y el conocimiento de quien ejecuta la actividad (jugador). No puede entenderse que asume en forma voluntaria un riesgo quien no está en situación de medirlo. En ese sentido, resultaría clave que el juego de realidad virtual disponga de advertencias claras para cualquier usuario.

En materia de responsabilidad extracontractual por culpa, ésta debe ser probada por quien la alega, lo cual con frecuencia genera un problema para la víctima frente a la desventaja en que se encuentra en relación con el autor del daño. En estos casos, la ley altera el principio antes enunciado, pues le corresponde a la víctima probar la existencia del hecho y del daño causado, y al demandado, probar que el perjuicio no deriva de sus actos, o que ha empleado la debida diligencia o cuidado. En Chile existen tres tipos de presunciones por culpabilidad: i) presunción de culpabilidad por el hecho propio; ii) presunción de culpabilidad por el hecho de las cosas; y iii) presunción de culpabilidad por el hecho ajeno. Estas presunciones son de derecho estricto y no cabe, por consiguiente, aplicarlas por analogía. De igual manera, hemos señalado que la responsabilidad por culpa no resultaría aplicable a los sistemas de inteligencia artificial, pues éstos carecen de capacidad en los términos señalados en la ley; sin embargo, dado que para desarrollar un sistema de inteligencia artificial existe detrás un programador, un diseñador o un fabricante, sería tentador intentar aplicarles un régimen de presunción de responsabilidad. Examinaremos cómo los actuales regímenes de presunción de responsabilidad resultan insuficientes para ser aplicados a los sistemas de inteligencia artificial.

La presunción por el hecho propio se encuentra regulada en el artículo 2.329 del Código Civil y contiene tres hipótesis.¹⁴ Se ha señalado por la doctrina que el mencionado artículo reconoce dos grupos de casos: las actividades particularmente peligrosas; y aquéllas en que las circunstancias indican que el daño ha sido causado por negligencia (Barros, 2010: 152). En este caso, resulta válido preguntarse: ¿es la actividad desarrollada por un sistema de inteligencia artificial una actividad peligrosa por sí misma? ¿Puede compararse con la actividad de disparar en forma imprudente un arma de fuego? Creemos que no. Para que opere la presunción resulta necesario que la cosa o la actividad hayan estado bajo el control del demandado, pues no puede pre-

14. Artículo 2.329 del Código Civil: «Por regla general todo daño que pueda imputarse a malicia o negligencia de otra persona, debe ser reparado por ésta. Son especialmente obligados a esta reparación: 1) el que dispara imprudentemente un arma de fuego; 2) el que remueve las losas de una acequia o cañería en calle o camino, sin las precauciones necesarias para que no caigan los que por allí transitan de día o de noche; 3) El que, obligado a la construcción o reparación de un acueducto o puente que atraviesa un camino lo tiene en estado de causar daño a los que transitan por él».

sumirse la culpa si el daño ocurre fuera de su ámbito de cuidado. Del mismo modo, es necesario que, tal como señala Barros, “el accidente sea de aquellos que en el curso ordinario de los acontecimientos no ocurren en ausencia de negligencia” (2010: 155). De acuerdo con lo señalado en la primera sección de este artículo, precisamente dentro de las características de un sistema de inteligencia artificial se encuentran la falta de control, la autonomía y la imprevisibilidad. Por consiguiente, malamente podría aplicarse esta presunción al fabricante o desarrollador de un sistema de inteligencia artificial, cuando ésta no se encuentra bajo el control y dominio de su creador o diseñador. De hecho, la idea de control de la fuente de daño por parte del demandado excluye que el daño se deba a alguna acción de la propia víctima. Por ende, la presunción no puede operar si la víctima pudo en forma razonable haber tenido un rol decisivo en el accidente. Donde se ha aplicado esta presunción en el derecho comparado —tal como Barros apunta— es respecto de “la responsabilidad por productos defectuosos: acreditado el daño y el defecto del producto, se puede presumir, en principio, que la causa del daño fue el defecto del producto y que dicho defecto se debió a culpa del fabricante o productor” (Barros, 2010: 156). Sobre asimilar la responsabilidad derivada de acciones ejecutadas por sistemas de inteligencia artificial con la responsabilidad por productos defectuosos, lo analizaremos en detalle más adelante.

La presunción por el hecho ajeno supone que cualquier persona es responsable no solo de sus propias acciones, sino de las de quienes estuvieren a su cuidado.¹⁵ Para hacer aplicable dicha presunción se requiere: i) una relación de dependencia o cuidado entre el autor del daño y la persona responsable; ii) que ambas partes sean capaces de delito o cuasidelito civil (en el caso de los menores o dementes, privados de capacidad, el tercero que los tiene a su cargo responde exclusivamente por el hecho propio y su culpa debe ser acreditada); y iii) que se acredite la culpabilidad del subordinado. Como es posible advertir, este modelo tampoco sería aplicable a un sistema de inteligencia artificial, pues no solo supone que el sistema sea legalmente capaz, sino que, además, exista una relación de dependencia o cuidado entre éste y su creador, desarrollador o fabricante, lo cual no se condice con la naturaleza misma de la inteligencia artificial, según lo analizado en la primera sección del presente artículo.

La presunción por el hecho de las cosas hace responsable al dueño de las cosas, quien debe vigilarlas y mantenerlas en el estado que no cause daño. El Código Civil

15. Artículo 2.320 del Código Civil: «Toda persona es responsable no solo de sus propias acciones, sino del hecho de aquellos que estuvieren a su cuidado. Así el padre, y a falta de éste la madre, es responsable del hecho de los hijos menores que habiten en la misma casa. Así el tutor o curador es responsable de la conducta del pupilo que vive bajo su dependencia y cuidado. Así los jefes de colegios y escuelas responden del hecho de los discípulos, mientras están bajo su cuidado; y los artesanos y empresarios del hecho de sus aprendices o dependientes, en el mismo caso. Pero cesará la obligación de esas personas si con la autoridad y el cuidado que su respectiva calidad les confiere y prescribe, no hubieren podido impedir el hecho».

contempla tres casos: i) presunción de culpa por el hecho de animales;¹⁶ ii) presunción de culpa por ruinas de edificios; y iii) presunción de culpa por caída de objetos desde la parte superior de un edificio. De las hipótesis ya señaladas, quizás la que aparece más interesante para la materia de estudio es la presunción por el hecho de animales, pues podría asimilarse el hecho de un animal con el hecho de un sistema de inteligencia artificial. Sin embargo, dicho enfoque resulta completamente errado.

En primer lugar, de aplicar la presunción de culpa por el hecho de los animales, haríamos responsable al «dueño» del sistema de inteligencia artificial. En este punto surge la duda: ¿quién es el «dueño» de un sistema de inteligencia artificial? ¿El diseñador? ¿El fabricante? ¿El usuario? ¿Estamos frente a un contrato de licencia o no? En segundo lugar, no es posible asimilar el comportamiento animal con el comportamiento de un sistema de inteligencia artificial. Desde la perspectiva racional, la comunicación de ideas complejas o pensamientos resulta más fácil en un sistema de inteligencia artificial que en un animal. De hecho, los sistemas de inteligencia artificial están diseñados para interactuar con humanos. Del mismo modo, los animales han coexistido con los seres humanos desde tiempos ancestrales y pueden vivir fácilmente sin la presencia de humanos. La inteligencia artificial, por su parte, es creada por humanos, quienes también pueden deshabilitarla. Por otro lado, los animales cazan otros animales o especies vivas para sobrevivir, mientras que los sistemas de inteligencia artificial, en general, no necesitan matar para sobrevivir.

Otro problema que suscita la aplicación de responsabilidad civil por culpa en sistemas de inteligencia artificial se da respecto del vínculo de causalidad entre la acción u omisión dolosa o culpable y el daño. En particular en dos áreas: la complejidad de los sistemas de inteligencia artificial, que hace en extremo difícil probar cómo ha tomado una decisión determinada; y la pluralidad de causas.

El funcionamiento de sistemas de inteligencia artificial que utilizan técnicas de aprendizaje automático difícilmente podrán ser explicados por sus creadores o diseñadores, dado los distintos tipos de complejidad que subyacen a dichas técnicas. Lo anterior, justamente, constituye la principal ventaja de dichas técnicas y lo que las diferencia de la programación convencional. Por ende, si ya resulta complejo para el creador determinar la causa que motiva la ejecución de una tarea determinada, con mayor razón va a resultar complejo para un usuario consumidor determinar la causalidad de acción en un sistema de inteligencia artificial complejo. Prueba que

16. Artículo 2.326 del Código Civil: «El dueño de un animal es responsable de los daños causados por el mismo animal, aun después que se haya soltado o extraviado; salvo que la soltura, extravío o daño no pueda imputarse a culpa del dueño o del dependiente encargado de la guarda o servicio del animal. Lo que se dice del dueño se aplica a toda persona que se sirva de un animal ajeno; salva su acción contra el dueño, si el daño ha sobrevenido por una calidad o vicio del animal, que el dueño con mediano cuidado o prudencia debió conocer o prever, y de que no le dio conocimiento».

no podría ser superada ni con una presunción de derecho, ni con un perito experto en la materia. Lo anterior, sin perjuicio del anhelado principio de transparencia que muchas autoridades han abogado en materia de inteligencia artificial.

En definitiva, el actual modelo de responsabilidad civil por culpa resulta insuficiente para abordar la problemática de la responsabilidad por ilícitos ocasionados por sistemas de inteligencia artificial. Cabe en lo sucesivo determinar si el sistema de responsabilidad estricta u objetiva resulta idóneo a dichos fines.

Pasamos ahora a la *responsabilidad civil extracontractual estricta u objetiva*. En este tipo de responsabilidad, se prescinde del elemento de culpabilidad del actor a efectos de hacerlo responsable. En este caso, la atribución de responsabilidad reside, más bien, en el ejercicio de una actividad considerada riesgosa por parte del autor. Tal como señala Barros:

Este es un régimen especial, y como tal, de derecho estricto, que opera sólo respecto de ciertos ámbitos de conducta o de tipos de riesgos previamente definidos por el legislador. En consecuencia, su fuente es la ley. Ejemplos de este tipo de responsabilidad encontramos en: la responsabilidad del propietario del vehículo motorizado por accidentes de tránsito (a condición de que quien lo conducía haya incurrido en negligencia); la del causante de derrames de hidrocarburos y otras sustancias nocivas en el mar; la del explotador de instalaciones nucleares; la del empresario de aeronaves; y la del que utiliza plaguicidas (Barros, 2010: 471).

En definitiva, lo que hace aplicable este régimen de responsabilidad es la mera causalidad entre la acción y el daño, con prescindencia de la voluntad del actor, pues la acción desplegada resulta, por sí, riesgosa.

Los partidarios de aplicar este régimen de responsabilidades:

Argumentan que este sistema obliga a quienes desarrollan una actividad riesgosa a internalizar el costo de los accidentes, es decir, el costo de indemnizar a las víctimas de accidentes causados por la actividad será considerado como uno más de los componentes del precio del bien o servicio respectivo, distribuyéndose entre todos sus usuarios o consumidores. De igual manera, se argumenta que, desde la perspectiva de la prevención, la mejor regla para prevenir accidentes es la que aplica los incentivos en aquél que genera el riesgo, de manera que sea éste quien determine el grado óptimo de cuidado. Por regla general, quien desarrolla la actividad riesgosa está en mejores condiciones para evitar el daño, y este sistema de responsabilidad estricta lleva a adoptar los resguardos más eficientes para evitar los accidentes, es decir, lleva a adoptar aquellos resguardos que tengan un costo comparativamente menor que las indemnizaciones que deberá pagar a las víctimas de los accidentes (Barros, 2010: 461-462).

Dentro de los partidarios de aplicar este régimen de responsabilidad estricta a sistemas a los fabricantes de sistemas de inteligencia artificial se encuentra el profe-

sor Horst Eidenmüller, quien en una exposición respecto de autos autónomos para BMW, señaló que éste es un mejor modelo porque: i) para su aplicación, no se requiere el elemento de culpabilidad, sino la mera causalidad entre la acción y el daño; y ii) desde la perspectiva de la prevención, el fabricante es el que se encuentra mejor posicionado para controlar el riesgo que supone la actividad. Descarta de esa forma la responsabilidad por culpa, dada la dificultad para determinar el estándar de cuidado, e igualmente descarta la responsabilidad del productor del sistema de inteligencia artificial.¹⁷

Sin perjuicio de lo señalado, creemos que un régimen de responsabilidad estricta para fabricantes de sistemas de inteligencia artificial no es la solución óptima. A dichos efectos, cabe considerar los siguientes problemas que plantea su aplicación:

Un factor clave para la aplicación del régimen de responsabilidad estricta es el riesgo de la actividad desplegada. Sobre este punto, no todo sistema de inteligencia artificial ejecuta una actividad riesgosa. Existen distintas soluciones de inteligencia artificial, cuyo impacto y potencialidad de riesgo difiere sustantivamente. Así, tenemos:

- Aplicaciones o venta de inteligencia artificial como SaaS (*software as a service*, software como un servicio), cuyo riesgo inmediato para los humanos que manipulan o acceden a dichos sistemas es nulo o muy bajo. Ejemplos de este tipo de sistemas son Google IA, Amazon, Microsoft Azure e IBM Watson, entre otros.
- Inteligencia artificial como innovación propiamente tal, cuyo riesgo es mayor para los humanos que manipulan o acceden a estos sistemas. Ejemplos de este tipo de sistemas son Tesla, Uber IA y drones autónomos, entre otros.

Por ende, calificar cualquier actividad desplegada por un sistema inteligencia artificial como riesgosa, resulta una aproximación deficiente desde la técnica legislativa, pues el impacto y riesgo es sustantivamente distinto. En efecto, no causa el mismo riesgo un vehículo o un dron totalmente autónomo que un sistema de texto predictivo en mi correo electrónico. De igual manera, ambos casos no resultan homologables a las hipótesis de responsabilidad objetiva señaladas en nuestra legislación, como los derrames de hidrocarburos o la explotación de instalaciones nucleares. Por consiguiente, una primera dificultad viene dada por la calificación del riesgo en la actividad desplegada por un sistema de inteligencia artificial, pues resultaría ineficiente aplicar un régimen de responsabilidad estricta único a aplicaciones cuya actividad suponen un riesgo nulo para el usuario de dicha tecnología.

17. Horst Eidenmüller, «Whose fault? Firms products and liability in the age of artificial intelligence», Faculty of Law, Oxford University, disponible en <https://bit.ly/2BpwcsZ> (video privado).

En segundo lugar, hay que considerar quién se encuentra en mejor posición para controlar el riesgo y prevenir el daño. De acuerdo con lo señalado, la aplicación de este régimen se justifica porque quien desarrolla la actividad riesgosa es quien generalmente se encuentra en una mejor posición para controlar el riesgo y prevenir el daño que la actividad genera, pues puede evaluar el costo del riesgo que sus acciones causan.

En materia de inteligencia artificial, no siempre el fabricante del sistema se encontrará en mejor posición para controlar el riesgo y prevenir el daño de la actividad desplegada por el mismo, dado que éstos son esencialmente imprevisibles en la ejecución de sus actos para alcanzar el objetivo con los que fueron diseñados —a diferencia de un sistema computacional convencional, que funciona a partir de órdenes y secuencias lógicas programadas por su creador—. Por otro lado, en ciertos casos, va a ser el usuario quien se encuentre en mejor posición para determinar el riesgo. Tomemos el caso del operador de un sistema de inteligencia artificial utilizado en el ámbito de la medicina. Por lo general, quien guía un dispositivo robótico implementado con inteligencia artificial es un médico, que se encuentra en una mejor posición de conocimientos para controlar el riesgo y prevenir el daño que podría eventualmente ocasionar.

Por consiguiente, a diferencia de otras actividades riesgosas sujetas a responsabilidad estricta, en que quien genera esa actividad se encuentra en mejor posición para determinar el riesgo, en los sistemas de inteligencia artificial, dado su rasgo esencialmente imprevisible, el fabricante no siempre va a poder determinar de forma previa y con claridad el riesgo que el sistema puede ocasionar.

Otro problema que genera la aplicación de este régimen es que ignora el grado de responsabilidad que tiene el usuario, quien en muchas ocasiones es el responsable y el generador del riesgo en la actividad.¹⁸ Aplicar este régimen prescindiendo de la actividad desplegada por el usuario haría responsable al fabricante o al desarrollador de un riesgo que escapa por completo de su esfera de control, lo que sería del todo injusto y generaría un fuerte desincentivo al desarrollo de esta tecnología.

18. Un claro ejemplo lo constituyen los vehículos Tesla. De los escasos accidentes ocasionados por este tipo de vehículos, la responsabilidad de los conductores ha sido un factor. Así, en el caso del conductor Walter Huang, desatendió las alertas de seguridad visuales y auditivas que el sistema del vehículo advirtió en reiteradas ocasiones, lo que llevó al accidente fatal (Raúl Álvarez, « El accidente fatal del Model X se complica: Tesla culpa al conductor del accidente mientras la familia se prepara para demandar», *Xataka*, 12 de abril de 2018, disponible en <https://bit.ly/2ZYLj77>). De igual manera, en el caso de Joshua Brown, incluso llegó a alterar el sistema operativo del vehículo para ver una película mientras conducía su vehículo Tesla (Denís Iglesias, «Tesla, declarada “no responsable” del accidente mortal de un Model S», *El Mundo*, 20 de enero de 2017, disponible en <https://bit.ly/2U5U9fr>).

Otras soluciones disponibles en nuestra normativa

De conformidad con lo estudiado, los regímenes de responsabilidad estricta y por culpa resultan insuficientes para aplicarlos a sistemas de inteligencia artificial. Cabe en lo sucesivo examinar otras soluciones que provee nuestro ordenamiento jurídico.

Responsabilidad civil del proveedor del artículo 23 de la Ley de Protección de los Derechos de los Consumidores

Una clase de responsabilidad que existe en el derecho comparado es aquella cuyos daños derivan de productos defectuosos, en la que, como señala Barros,

basta que el daño sea injusto —entendido como injusto el daño causado por el vicio del producto— para que el fabricante sea responsable, sin que pueda excusarse alegando haber actuado con diligencia. En otras palabras, acreditado el daño y el defecto del producto, se puede presumir, en principio, que la causa del daño fue el defecto del producto y que el defecto se debió a la culpa del fabricante o productor (2010: 156).

La única solución que provee nuestro ordenamiento jurídico en relación con productos defectuosos, en el marco de una relación de consumo, la otorga el artículo 23 inciso primero de la Ley 19.496, que Establece Normas sobre Protección de los Derechos de los Consumidores:

Comete infracción a las disposiciones de la presente ley el proveedor que, en la venta de un bien o en la prestación de un servicio, actuando con negligencia, causa menoscabo al consumidor debido a fallas o deficiencias en la calidad, cantidad, identidad, sustancia, procedencia, seguridad, peso o medida del respectivo bien o servicio.

Lo que hace la norma transcrita es establecer una sanción infraccional que viene a proteger la seguridad en el consumo. A primera vista podría ser una atractiva opción para hacer responsable a los proveedores vendedores de sistemas de inteligencia artificial (Barrientos Camus, 2010: 20).¹⁹ Después de todo, los sistemas de inteligencia artificial son —muchas veces— *servicios* que se prestan, a veces, en una relación de consumo. Sin embargo, este régimen resulta igualmente complejo en materia de inteligencia artificial.

En efecto, su aplicación supone que, en la prestación del servicio, el sistema de inteligencia artificial tenga una falla o deficiencia en la calidad, cantidad, identidad, sustancia, procedencia, seguridad, peso o medida. Dicho requisito no presenta pro-

19. La norma hace referencia al proveedor «en la venta». Pese a que algunos, como Francisca María Barrientos, estiman que esta norma puede aplicarse en extensión al fabricante.

blemas cuando en efecto el sistema presenta una falla o deficiencia, es decir, cuando el servicio no es apto para el consumo. Sin embargo, el problema subsiste cuando el sistema no presenta falla alguna, es decir, cuando por su carácter autónomo e imprevisible no funciona como era esperado o funciona de una manera distinta de la originalmente diseñada, pero de todos modos cumple su fin.

Por otro lado, la aplicación de este régimen de responsabilidad genera una complicación para el consumidor, pues no solo debe probar que existe una falla en un sistema de inteligencia artificial (prueba extremadamente compleja incluso para sus desarrolladores), sino que además debe probar que el proveedor vendedor actuó con culpa. Esto hace que aplicar este régimen de responsabilidad en la práctica sea imposible.

La exigencia de culpa por parte del proveedor supone que éste debió, en cierta forma, prever que el producto vendido adolecía de alguna falla o deficiencia en sus características, cuando de acuerdo con lo ya señalado, un rasgo característico de los sistemas de inteligencia artificial es la imprevisibilidad y el grado de autonomía que detentan.

Un último problema se da con el tipo de solución que abordamos. Hemos mencionado ya que existen soluciones de inteligencia artificial como SaaS o software en que la falla del producto se soluciona a través de parches que el mismo proveedor otorga en el marco de un contrato de licencia, en relaciones contractuales que no siempre son de consumo, y que, por lo mismo, excluyen la aplicación del artículo 23 de la Ley.

Seguro privado obligatorio

El seguro privado obligatorio no es un sistema de atribución de responsabilidad, sino más bien un contrato forzoso, que garantiza que el riesgo causado por una determinada actividad será asumido por un tercero (asegurador), cualquiera sea la causa. Las áreas más importantes del derecho nacional en que opera este seguro son: el seguro automotriz obligatorio (Ley 18.490, sobre Seguro Obligatorio de Accidentes Personales Causados por la Circulación de Vehículos Motorizados)²⁰ y el seguro por accidentes del trabajo (Ley 16.744, de seguro social contra riesgos de accidentes del trabajo y enfermedades profesionales).

El seguro automotriz obligatorio está destinado a cubrir daños corporales a terceros en accidentes de tránsito en los que intervenga un vehículo motorizado, y opera

20. En materia automotriz, el artículo 170 de la Ley 18.290 establece la responsabilidad del conductor del vehículo, lo que se complementa por las presunciones de responsabilidad contenidas en el artículo 172 del mismo cuerpo legal. Además, la legislación contempla dos mecanismos de protección a las víctimas de accidentes: i) responsabilidad estricta del dueño del vehículo por los daños causados por el conductor (artículo 174 de la Ley 18.290); y ii) un sistema de seguro privado obligatorio.

con prescindencia del juicio de culpabilidad del conductor. La solución de un seguro privado obligatorio parece idónea para la regulación de sistemas de inteligencia artificial. De hecho, en el 2017, el Parlamento Europeo propuso una serie de recomendaciones para la regulación de estos sistemas, entre las que destacan:

- i) establecer un régimen de seguro obligatorio en los casos en que sea pertinente y necesario para categorías específicas de robots, similar al existente para los automóviles, en el que los fabricantes o los propietarios de robots estarían obligados a suscribir un contrato de seguro por los posibles daños y perjuicios causados por sus robots.²¹

La primera crítica que se puede deslizar a este tipo de sistemas, bien la señala Barros (2010: 53) al analizar la justicia distributiva como fin de responsabilidad civil, y que dice relación con lo que él llama “el debilitamiento de los lazos de recíproca responsabilidad que unen a una comunidad de personas, bajo el principio de que cada uno carga con las consecuencias de sus propios actos. En ese sentido, un sistema de seguros generalizados y compulsivos puede contribuir a que se debilite el sentido de lo correcto, pues la funcionalización del riesgo nos aleja del discernimiento de lo justo”.

Otra complejidad que puede surgir producto de la exigencia de un seguro obligatorio para cualquier sistema de inteligencia artificial es ignorar la existencia de sistemas que no generan un daño o impacto para los usuarios, como el texto predictivo en correos electrónicos o un traductor automático. Del mismo modo, va a resultar complejo determinar la prima del seguro a pagar, o qué sucederá cuando no existe un daño material físico para una persona, sino, por ejemplo, una filtración de datos personales o una afectación a su privacidad.

Por último, la recomendación del Parlamento Europeo no distingue si el seguro se le haría obligatorio al usuario de un sistema de inteligencia artificial o al fabricante de dicho sistema. En ambos casos resulta complejo. Para el usuario consumidor, la exigencia de contratación de un seguro privado obligatorio operaría como en la práctica opera el seguro automotriz obligatorio, esto es, cubriría parte de los daños ocasionados en accidentes (pues el legislador en ese caso ha preferido exigir un seguro de mínima cobertura para no gravar el uso del vehículo como transporte, con la exigencia de pago de una prima más gravosa). Para el fabricante, la exigencia de contratación de seguro obligatorio establecería una exigencia adicional para producir una solución que incorpore inteligencia artificial, lo que puede ser un estímulo al desarrollo de sistemas seguros, pero a la vez puede implicar una barrera de entrada para fabricantes que son pequeñas *startups* y, de esa forma, desincentivaría que pe-

21. «Informe con recomendaciones destinadas a la Comisión sobre normas de derecho civil sobre robótica», Parlamento Europeo, 27 de enero de 2017, disponible en <https://bit.ly/3gRC1Qk>.

queñas empresas proporcionen soluciones innovadoras en el campo de la inteligencia artificial.

Recomendaciones de política pública en materia de inteligencia artificial

Elaborar recomendaciones de política pública en materia de inteligencia artificial no es una tarea sencilla, porque es una tecnología que está en constante desarrollo, y porque un mal diseño de políticas públicas puede perjudicar seriamente el desarrollo del país en esta materia.

Sin perjuicio de lo anterior, existen medidas que estimamos pueden ser consideradas al momento de elaborar políticas públicas en materia de inteligencia artificial. Para los efectos de este artículo, estas recomendaciones pueden agruparse en aquellas que tienen un carácter preventivo, es decir, buscan prevenir la generación de accidentes y sus efectos litigiosos, y una recomendación de carácter correctivo, es decir, cuando el hecho dañoso generado por un sistema de inteligencia artificial se ha verificado.

Dentro de las medidas preventivas enfocadas en política pública, podemos mencionar la elaboración de una base de principios que guíen el desarrollo de sistemas de inteligencia artificial, proveer fondos para apoyar el desarrollo y uso de aplicaciones de inteligencia artificial en áreas de gran necesidad social (salud, educación, etcétera), proveer incentivos para los investigadores que reciben financiamiento público para que publiquen el conjunto de datos asociados a su investigación en un formato legible por máquinas (código objeto) con respeto a las normas de privacidad, reforzar el lazo entre empresas de tecnología con las universidades y centros de formación técnica, aumento significativo de open data del gobierno y disponibilidad de datos en ámbitos estratégicos para Chile (como astronomía, minería, energía, agricultura, oceanografía, etcétera), entre otras muchas medidas.

En lo sucesivo analizaremos las medidas de carácter regulatorio que pueden tener impacto en el desarrollo de la inteligencia artificial.

Autorregulación

Una herramienta que podría coadyuvar en el desarrollo de una política pública saludable en materia de inteligencia artificial es la autorregulación de la industria. En Chile, la autorregulación funciona de forma eficiente cuando se establecen normas claras que se sustentan en un marco normativo ampliamente reconocido por los regulados. Es lo que sucede en materia publicitaria con el Consejo de Autorregulación y Ética Publicitaria (CONAR).

El CONAR, tal como su sitio web indica:

Es una corporación de derecho privado sin fines de lucro, cuyo objetivo principal es autorregular, desde la perspectiva ética, la actividad publicitaria nacional, de manera que se desarrolle en armonía con los principios y normas consagradas en el Código Chileno de Ética Publicitaria. Para estos efectos, a través de sus actuaciones vela por que los mensajes publicitarios se encuadren dentro de los principios de legalidad, honestidad, moralidad y veracidad. El CONAR es en esencia un tribunal arbitral de honor, al cual se recurre de manera voluntaria, para que resuelva las controversias que se susciten en materia de publicidad comercial y que termina, eventualmente, con un dictamen ético que, en caso de infracción, recomienda el retiro de la pieza publicitaria. El CONAR está integrado por las instituciones y empresas privadas más importantes y representativas de la actividad publicitaria y comunicacional del país, a través de las asociaciones que las agrupan.²²

Si bien asociarse al CONAR es voluntario, en la industria su asociación da un fuerte mensaje de seriedad y prestigio, por lo que las firmas de publicidad tienden a asociarse y regirse por normas que la misma industria ha dictado, y que velan por un correcto y ético funcionamiento.

Esta fórmula podría igualmente aplicarse en la industria de la inteligencia artificial, en la que los *stakeholders* buscan generar tecnologías que sean seguras y que cumplan con los más altos estándares. Resulta del todo ilógico asumir un enfoque contrario, sustentado en la desconfianza, por una simple razón: ningún productor o creador quiere desarrollar un producto o prestar un servicio que dañe a su público consumidor.

Certificación de seguridad de ciertas soluciones de inteligencia artificial

La seguridad de los productos ha sido históricamente un tema de suma relevancia en el diseño de políticas públicas. La inteligencia artificial no es la excepción. Una de las áreas que ha generado preocupación en la sociedad es la seguridad de los dispositivos implementados con inteligencia artificial.

Una recomendación en esta área partiría por distinguir entre: i) sistemas de inteligencia artificial como SaaS o software, es decir, como soluciones informáticas, cuyo daño material inmediato al usuario resulta más improbable y menos tangible; y ii) dispositivos implementados con inteligencia artificial que tienen una materialidad y que, por lo mismo, podrían causar daño material directo a sus usuarios, por ejemplo, un dron o una patineta totalmente autónoma.²³ En el primero de estos casos, la ame-

22. «Qué es CONAR», disponible en <https://www.conar.cl/sobre-conar/que-es-conar/>.

23. En el caso de los vehículos autónomos la regla sería distinta, porque los fabricantes de vehículos incorporan en su diseño una serie de medidas de seguridad previo a su comercialización, como el New Car Assessment (NCA), que es un reconocido mecanismo de certificación de vehículos. Por lo demás, en Chile los vehículos motorizados se encuentran sujetos a controles periódicos de seguridad en las plantas de revisión técnica.

naza vendría desde el área de ciberseguridad donde deberían adoptarse protocolos internos en cada empresa desarrolladora de soluciones de inteligencia artificial. En el segundo de estos casos, sería recomendable una certificación de seguridad previa a su comercialización.

Un ejemplo de lo anterior, y que tiene su correlato en Chile, son las certificaciones de seguridad obligatoria previa que exige la Superintendencia de Electricidad y Combustible (SEC) para la comercialización de ciertos productos y materiales eléctricos, de gas y combustibles líquidos, entre otros.²⁴ Dicha certificación es obligatoria y previa a la comercialización del producto determinado, lo que garantiza un cierto estándar de seguridad para el usuario. Su inobservancia puede acarrear multas o el eventual retiro del producto del mercado, con auxilio de la fuerza pública en caso de ser necesario.

A grandes rasgos, el sistema de certificaciones de la SEC funciona en un entorno colaborativo entre distintos actores. La normativa legal obliga a los fabricantes, importadores y comerciantes a conseguir que su producto —independiente de su origen— posea un certificado que pruebe cumplir con alguno de los sistemas de certificación permitidos, en cumplimiento con el protocolo de análisis y ensayos establecidos por la Superintendencia. Dicho certificado de aprobación sólo puede ser otorgado por un organismo de certificación autorizado por la SEC específicamente para el producto en trámite. De esta forma, el fabricante, importador o comerciante no tiene que certificar sus productos en un organismo público como la SEC, sino que lo hace en organismos de certificación privados autorizados por ella, de su propia elección.

El esquema de certificaciones de la SEC ha generado un entorno saludable y seguro para los consumidores y para la industria. A los primeros les ha dado la posibilidad de acceder a una mayor gama de productos seguros. Para las empresas, la certificación no ha significado una merma en su producción y venta, por el contrario, les ha dado solidez y mejorado su reputación en el mercado al vender productos de calidad y seguros.

Este marco normativo de certificaciones podría replicarse para generar un mecanismo de certificación de ciertos dispositivos implementados con inteligencia artificial, coordinado por otra agencia gubernamental o por un ente creado a dichos fines.

Esquemas regulatorios flexibles

En la actualidad vivimos una paradoja en términos regulatorios: mientras la tecnología avanza y evoluciona constantemente a un acelerado ritmo, las normas legales que buscan regular dichas tecnologías se mueven lentamente y en esquemas por comple-

24. Artículo 3 numeral 14 de la Ley 18.410, que Crea la Superintendencia de Electricidad y Combustibles estableciendo sus funciones y ámbitos de competencia.

to rígidos, lo cual muchas veces genera un detrimento directo en la innovación y, por ende, en el desarrollo del país. Como respuesta, han surgido esquemas regulatorios flexibles, como las *sunset laws* y las *regulatory sandboxes*.

Las *sunset laws* son normas legales con una vigencia temporal, es decir, normas que contemplan una fecha de derogación («atardecer» u «ocaso») establecida en el momento de entrada en vigor de la ley. Normalmente se establecen períodos de entre uno y cinco años de duración. Esto obliga al legislador a evaluar la idoneidad de la regulación una vez que ha transcurrido el plazo pactado, valorando éxitos y fracasos. Este tipo de regulación flexible ha permitido eliminar barreras de entrada en el sector de la innovación tecnológica y ha proporcionado incentivos para el desarrollo de tecnologías, aplicado con éxito en el campo de I+D, en el que se han promulgado numerosas leyes para promover la cooperación universitaria industrial y la cooperación empresarial. Un ejemplo fue la Ley del Impuesto sobre la Recuperación Económica de 1981 (Economic Recovery Tax Act) de Estados Unidos, que estableció un crédito fiscal a la investigación y la experimentación, y concedió a las empresas una mayor deducción por las donaciones de equipos utilizados en la investigación científica en instituciones académicas y por la donación de nuevos equipos por parte de un fabricante. Se suponía que esta ley se iba a extinguir en 1985, pero debido a las sucesivas renovaciones, sigue vigente (Ranchordas, 2015: 218).

Los *regulatory sandboxes* son una especie de prueba piloto legislativa. Se trata de «espacios de experimentación, que permiten a empresas innovadoras operar temporalmente, bajo ciertas reglas que limitan aspectos como el número de usuarios o el período de tiempo en que se pueden ofrecer el producto» (Herrera y Vadillo, 2018: 5). Este marco regulatorio permite crear una «caja de arena» (*sandbox*) para poner en marcha proyectos que no cuentan con la autorización oficial para ello ni cumplen —al menos no por completo— con la normativa sectorial pertinente. El objetivo de estas cajas es minimizar la incertidumbre respecto de la normativa aplicable a algún producto o servicio, pues permite a las empresas con modelos de negocios innovadores en fase de desarrollo, conocer y adecuarse a la regulación de forma gradual y anticipada, y al regulador, entender de mejor manera el funcionamiento de una nueva tecnología.

Los requisitos para que una compañía pueda ser parte de un *sandbox* son bastante estrictos, ya que no solo deberá probar que el proyecto es innovador, sino también que producirá efectos positivos en el mercado y para los consumidores. Así, por ejemplo, en el Reino Unido se exige que los postulantes acrediten:

- i) que están proponiendo una solución novedosa en un sector regulado, o al menos que sirva de soporte a una actividad regulada; ii) que los productos, servicios o tecnología que ofrecen sean inéditos en el país; iii) que su comercialización pueda llegar a beneficiar a los consumidores; iv) que han invertido recursos para analizar

la regulación vigente y mitigar los riesgos que la actividad pueda producir; y v) que están en condiciones de operar y probar sus innovaciones en un entorno real.²⁵

Si bien estos modelos parecen lejanos de la realidad chilena, lo cierto es que en el año 2018, el presidente de la Comisión para el Mercado Financiero (CMF) propuso un marco regulatorio para las empresas *fintech*, entre los que destacó los *sandboxes* para fomentar *startups*. Por su parte, la Superintendencia de Bancos e Instituciones Financieras (SBIF) ha señalado al respecto:

La posibilidad de establecer modelos de *sandbox* regulatorio en Chile es una opción que aún requiere mayor discusión y por cierto de cambios legales y normativos. No obstante lo anterior, se destaca que existen en nuestro ordenamiento legal disposiciones que facultan al supervisor para eximir de exigencias o requisitos a las entidades supervisadas. En efecto, el artículo 4 de la Ley 18.045 faculta al supervisor de valores para eximir de requisitos a los supervisados, atendiendo al número y tipo de inversionistas o a los medios a través de los cuales se comunican o materializan las transacciones, y el monto de los valores ofrecidos. Esto podría ser base para una futura regulación sobre la materia. Adicionalmente se requiere, generar pasos adicionales para resguardar la estabilidad y la protección de los consumidores (Yáñez, 2018: 12-13).

Si bien estos modelos regulatorios flexibles se encuentran más vinculados a la industria *fintech*, no vemos inconveniente alguno para que sea aplicable para fomentar modelos de negocio y el desarrollo de soluciones innovadoras que apliquen inteligencia artificial. Por último, al igual que en las recomendaciones previas, encuentra un correlato en Chile.

Un modelo de *safe harbor* o puerto seguro para soluciones de inteligencia artificial

Las recomendaciones enunciadas tienen un carácter preventivo a la comisión del hecho dañoso por parte de un sistema de inteligencia artificial. Sin embargo, cabe situarse en el caso de que las medidas preventivas señaladas no hayan funcionado y el litigio civil o criminal sea inminente.

En lugar de aplicar los esquemas de responsabilidad tradicionales ya estudiados, creemos necesario incorporar una especie de *safe harbor* o puerto seguro. Un *safe harbor* es una disposición legal que especifica que cierta conducta no transgrede una determinada norma, siempre que concurran ciertos requisitos. En Chile, el capítulo 3 del título 4 de la Ley 17.336 sobre Propiedad Intelectual, contiene una especie de *safe*

25. Rodrigo Ferrada y Catalina Irrarrázaval, «Los *sandbox* regulatorios como respuesta a la innovación», *El Mercurio*, 7 de noviembre de 2018, disponible en <https://bit.ly/2zYgB3h>.

harbor al regular la limitación de responsabilidad de los proveedores de servicio de internet, por las infracciones a los derechos de propiedad intelectual que se cometan por usuarios de estos servicios a través de sus redes y sistemas. La aplicación de estas reglas es sin perjuicio de las normas generales sobre responsabilidad.

La norma exige a dichos prestadores de servicios de la obligación de indemnizar perjuicios por los daños que sufran los titulares de derechos de autor por las infracciones que se cometan por o a través de sus redes o sistemas, en la medida que los prestadores cumplan una serie de requisitos, los que variarán dependiendo de la naturaleza del servicio prestado.

En virtud de lo estudiado, se podría elaborar una especie de *safe harbor* en materia de inteligencia artificial. Siguiendo el modelo del profesor Rachum-Twaig, si se reúnen ciertos requisitos copulativos, el fabricante o diseñador no será responsable por el daño ocasionado por sus sistemas de inteligencia artificial; sin perjuicio de ello —y al igual que en la Ley 17.336— el demandante podría invocar las normas generales sobre responsabilidad general, haciendo presente que en este caso el mérito probatorio va a ser complejo, dado lo ya analizado respecto de los modelos generales de responsabilidad existentes en Chile.

Bajo el esquema sugerido, los requisitos para que el fabricante o desarrollador de un sistema de inteligencia artificial no sea responsable por los daños ocasionados por sus sistemas vienen dados porque en su diseño: i) hayan incorporado mecanismos de monitoreo en el diseño del sistema para alertar al usuario; ii) hayan incorporado mecanismos de pausa de emergencia obligatoria que deshabiliten las funciones autónomas; y iii) otorguen soporte continuo en caso de detectar y notificar anomalías en el sistema de inteligencia artificial (Rachum-Twaig, 2019: 33-35).

En relación con el primer elemento, esto es, la implementación de mecanismos de monitoreo en el diseño de sistemas de inteligencia artificial, que permitan generar alertas o advertirle al usuario del sistema cuando éste funcione de forma anómala, debemos mencionar que presenta dos grandes desafíos para los fabricantes o desarrolladores: i) implementar sistemas de monitoreo y alerta que no afecten la funcionalidad, características y propósito básico de un sistema de inteligencia artificial; y ii) las herramientas de monitoreo y alerta no deben afectar o intervenir en la privacidad de los usuarios.

En relación con el segundo elemento, esto es, la implementación de mecanismos de pausa de emergencia que permitan al usuario que ocupa el sistema deshabilitar las funciones autónomas y retomar el control, presenta los siguientes desafíos para el fabricante o desarrollador: i) existen ciertos tipos de sistemas de inteligencia artificial que no pueden incorporar mecanismos de pausa de emergencia, como aquellos sistemas vendidos como software (deshabilitarlos supondría que el usuario tuviese que manejar y desarrollar manualmente el programa, lo cual no tendría sentido), pero sí sería útil en el caso de los automóviles autónomos y en el caso de drones autónomos;

y ii) existen casos en que inhabilitar la función autónoma podría generar un daño mayor, pues precisamente es la autonomía de un sistema de inteligencia artificial el que genera un resultado óptimo. Por lo mismo, este elemento debe ser sopesado con cierta flexibilidad.

En relación con el tercer elemento, esto es, la provisión de soportes y parches para ciertos productos implementados con inteligencia artificial, hacemos presente su correlación con el primer elemento, dado que, si en el monitoreo de un sistema se detectan anomalías y éstas son notificadas al usuario, surge el deber para el fabricante de solucionar o proveer parches para arreglar la anomalía detectada, es decir, como una especie de servicio posventa.

Esta limitación de responsabilidad permite abordar de forma eficiente la inteligencia artificial en el contexto litigioso, sin verse afectada la potencial responsabilidad del fabricante o del desarrollador, por consideraciones relacionadas con los elementos de la inteligencia artificial, como la autonomía, imprevisibilidad y la falta de control. Por otro lado, la limitación de responsabilidad por *safe harbor* ya existe en nuestro ordenamiento jurídico en materia de propiedad intelectual, y por ende, no implica incorporar un elemento ajeno a nuestra tradición jurídica.

Conclusiones

En la ficción de Kubrick, se advierte la complejidad del lenguaje humano al momento de impartir una orden. La instrucción dada a Hal 9000 implicaba el éxito de la misión, sin advertir a qué costa. Lo cierto es que en el ejemplo de Hal 9000 hay un desajuste en los valores con que fue diseñado Hal: al diseñar la máquina y dotarla con un objetivo, no se le establecieron límites a ese objetivo, por lo mismo, la máquina llevó a cabo decisiones desafortunadas. Límites, reglas, de eso trata este artículo. Debemos decidir entre dos caminos: el primer camino nos dice que la tecnología es enemiga del ser humano y que la única salvación es el control de las máquinas, a través de una excesiva regulación; la segunda nos dice que la tecnología se encuentra al servicio del humano, y que cualquier sobrerregulación puede tener efectos perniciosos para el futuro.

Si tomamos el primer camino, el del temor, partiremos regularizando todos los sistemas de inteligencia artificial sin distinguir entre ellos. Estableceremos impuestos a las empresas que utilicen sistemas de inteligencia artificial en lugar de trabajadores humanos. Exigiremos que las decisiones de los algoritmos de aprendizaje automático sean transparentes y comprensibles para cualquier persona y, en cualquier caso, con lo que se prohibirían como consecuencia las «cajas negras» en los sistemas de inteligencia artificial. Si existe una innovación que amenace a un gremio, la prohibiremos o estableceremos barreras de entrada tan altas que al final no se podrá desarrollar dicha actividad. Exigiremos que las compañías tecnológicas que operan en Chile se

establezcan en el país y que contraten a gente en Chile, y que, por lo mismo, paguen sus impuestos en Chile. Y en el caso de que esas empresas se constituyan en Chile, exigiremos tantos requisitos que su operación en el país será compleja y burocrática. El resultado lógico y natural es que desincentivaré la innovación en tecnología en el país (que ya es precaria) y nos mantendrá como dependientes de tecnologías desarrolladas por terceros; las empresas no se querrán arriesgar a invertir en un país que pone tantas trabas; los pequeños empresarios y desarrolladores no podrán competir con las grandes empresas dadas las altas barreras de entrada; la inteligencia artificial desarrollada será predecible y en nada se distinguirá de los programas computacionales ya existentes. En el fondo, esta vía nos conduce a un oscurantismo tecnológico brutal.

La segunda vía implica, en primer término, entender la tecnología y, en segundo término, desde allí ver qué se puede regular y qué no. Esta segunda vía entiende que no hay tecnología que sea malvada o perversa, sino que ésta es neutra y muchas veces va a obedecer a cómo ha sido configurada. Este segundo camino no aboga por una total desregulación, sino por una regulación inteligente, porque entiende la tecnología y entiende que desde el punto de vista del fabricante o desarrollador es importante tener reglas claras. En definitiva, esta segunda vía va a aumentar la rapidez de los procesos y apoyar la toma de decisiones; va a crear nuevas formas de participación en los procesos democráticos; va a mejorar la eficiencia en el sector público y la industria; va a lograr una distribución más equitativa de los recursos y las oportunidades; va a ofrecer nuevos métodos y soluciones en diversos ámbitos, como la salud pública, la atención médica, la seguridad, el desarrollo sostenible, el consumo, la minería, la agricultura y el transporte; va a abrir nuevas oportunidades en la investigación científica y la educación; y va proporcionar a los individuos servicios más personalizados. Tomemos como ejemplo los vehículos autónomos, que no solo van a reducir la tasa de accidentes, sino que además van a promover la movilidad de personas con discapacidades y adultos mayores que hoy ven restringida dicha capacidad, es decir, va a generar una inclusión que puede complementar de mejor forma las políticas públicas de inclusión generadas a través de la ley. Bajo esta segunda vía, la cirugía robótica en Chile podría masificarse y, con ello, los beneficios que derivan para la población en general.

Por último, no olvidemos que el gran poder de la inteligencia artificial radica en su aprendizaje, ya que es por medio del aprendizaje que se perfecciona en su rendimiento, es decir, cómo se optimiza. Si obstaculizamos en exceso su desarrollo con exigencias que priven al sistema de sus características esenciales, vamos a perjudicar el desarrollo de esta tecnología. Vamos a conducir a Chile por el camino del miedo, y el miedo nos encierra, no nos permite avanzar. Esperemos como país no permitirnos quedar encerrados en esa prisión, sino salir de la oscuridad tecnológica.

Agradecimientos

Quiero agradecer todo el invaluable apoyo y los comentarios del profesor John Atkinson-Abutridy de la Facultad de Ingeniería y Ciencias de la Universidad Adolfo Ibáñez, que permitieron otorgar luz en la materia estudiada.

Referencias

- ABELIUK, René (2008). *Las obligaciones*. Santiago: Jurídica de Chile.
- BARRIENTOS CAMUS, Francisca María (2010). «La responsabilidad civil del fabricante bajo el artículo 23 de la Ley de Protección de los Derechos de los Consumidores y su relación con la responsabilidad civil del vendedor». *Revista Chilena de Derecho Privado*, 14: 109-158. DOI: [10.4067/S0718-80722010000100004](https://doi.org/10.4067/S0718-80722010000100004).
- BARROS, Enrique (2010). *Tratado de responsabilidad extracontractual*. Santiago: Jurídica de Chile.
- CALO, Ryan (2015). «Robotics and the lessons of Cyberlaw». *California Law Review*, 103 (3): 513-563. DOI: [10.2139/ssrn.2402972](https://doi.org/10.2139/ssrn.2402972).
- DE LA FUENTE HULAUD, Felipe (1990). «Sobre el concepto de responsabilidad criminal en nuestro Código Penal». *Revista de Derecho de la Universidad Católica de Valparaíso*, 13: 113-123. Disponible en <https://bit.ly/2AzysNV>.
- HERRERA, Diego y Sonia Vadillo (2018). «Regulatorio en América Latina y el Caribe para el ecosistema FinTech y el sistema financiero». Banco Interamericano del Desarrollo. Disponible en <https://bit.ly/2XXCBTV>.
- OVANESSOFF, Armen y Eduardo Plastino (2017). «Cómo la inteligencia artificial puede generar crecimiento en Sudamérica». Accenture. Disponible en <https://accntu.re/3ct7Uen>.
- POLITOFF, Sergio, Jean Pierre Matus y María Cecilia Ramírez (2003). *Lecciones de derecho penal chileno: Parte general*. Santiago: Jurídica de Chile.
- RACHUM-TWAIG, Omri (2019). «Whose robot is it anyway? Liability for artificial-intelligence-based robots». *University of Illinois Law Review*, 40: 1-40. Disponible en <https://bit.ly/300MWBc>.
- RANCHORDAS, Sofia (2015). «Innovation-friendly regulation: The sunset of regulation, the sunrise of innovation». *Jurimetrics*, 55 (2): 201-224. DOI: [10.2139/ssrn.2544291](https://doi.org/10.2139/ssrn.2544291).
- SCHERER, Matthew (2016). «Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies». *Harvard Journal of Law & Technology*, 29 (2): 353-400. DOI: [10.2139/ssrn.2609777](https://doi.org/10.2139/ssrn.2609777).
- VIDAL, Álvaro (2002). «Responsabilidad civil del profesional médico». Seminario sobre Responsabilidad Médica, organizado por la Auditoría General de la Armada de Chile y el Consejo de Defensa del Estado. Viña del Mar.

YÁÑEZ, Álvaro (2018). *FinTech en la industria financiera: Nuevos espacios de desarrollo y convergencia regulatoria*. Santiago: Superintendencia de Bancos e Instituciones Financieras. Disponible en <https://bit.ly/2XYJrZh>.

Sobre el autor

CARLOS ARAYA PAZ es abogado. Licenciado en Ciencias Jurídicas y Sociales de la Facultad de Derecho de la Universidad Adolfo Ibáñez, Chile. Diplomado en Propiedad Intelectual de la Pontificia Universidad Católica de Chile. International Professional Summer Program Understanding U.S. Intellectual Property Law, Stanford University, Estados Unidos. Abogado del estudio jurídico Magliona Abogados. Su correo electrónico carlosarayapaz@gmail.com.  <https://orcid.org/0000-0002-0420-8314>.

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

EDITOR GENERAL

Daniel Álvarez Valenzuela
(dalvarez@derecho.uchile.cl)

SITIO WEB

rchdt.uchile.cl

CORREO ELECTRÓNICO

rchdt@derecho.uchile.cl

LICENCIA DE ESTE ARTÍCULO

Creative Commons Atribución Compartir Igual 4.0 Internacional



La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipografía
(www.tipografica.io).