

# LA FUNCIÓN PREVENTIVA DE LOS DAÑOS CAUSADOS POR LA ROBÓTICA Y LOS SISTEMAS AUTÓNOMOS

## Matías Mascitti

Abogado. Doctor (PhD) en Derecho Universidad Nacional de Buenos Aires (UBA). Profesor visitante del Centro de Tecnología e Sociedade da FGV Direito Rio. Profesor Doctorado en Derecho Universidad Nacional de Rosario (UNR). Profesor Maestría en Magistratura UBA. Profesor Diplomatura de Estudios Avanzados en Estrategia Jurídica UNR. Orcid: 0000-0002-3942-8069. *E-mail:* matiasmascitti@gmail.com.

---

**Resumen:** Es una contribución al progreso del Derecho de la Responsabilidad Civil en esta era digital a través del desarrollo de la función de la prevención de los daños causados por la robótica y los sistemas autónomos (RSA). Un análisis detallado de su funcionamiento –con el auxilio del enfoque interdisciplinario– nos posibilita disminuir la producción previsible de lesiones. Sin embargo, la función precautoria y diversas medidas *ex ante* –no están contenidas en esa función preventiva– resultan necesarias para disminuir el margen de riesgo de causación de daños provocados por los RSA en virtud de la imprevisibilidad en su accionar en algunos casos. Por ello, la determinación de la función preventiva se convierte en una cuestión esencial para: la comprensión de los desarrollos jurídicos contemporáneos y el progreso del Derecho de la Responsabilidad civil reconociendo la complejidad fáctica de la era digital y los diversos valores en juego que requieren una tutela efectiva de los usuarios alentando el desarrollo adecuado de la innovación tecnológica.

**Palabras clave:** Progreso. Derecho de la Responsabilidad Civil. Función preventiva. Precaución. Era digital. IA. Robótica y sistemas autónomos. Enfoque interdisciplinario.

**Sumario:** I Introducción – II Los RSA como elementos de la complejidad de la era digital – III Los RSA como productos riesgosos – IV El aporte interdisciplinario para la construcción de la función de la prevención de los daños causados por los RSA – V La trama de las funciones de la responsabilidad civil como sustento de la prevención de los daños – VI Conclusión – Referencias

---

A robot may not injure humanity, or, through inaction,  
allow humanity to come to harm.

(Isaac Asimov's Zeroth Law of Robotics)

## I Introdução

La era digital está complejizando la cultura. A su vez, el Derecho es un sistema abierto ya que intercambia materia con el medio circundante, que exhibe importación y exportación, constitución y degradación de sus componentes materiales;<sup>1</sup> de aquí que aquel se integre en la cultura; por consiguiente, es un objeto cultural. Asimismo, el Derecho, como integrante de la filosofía práctica – con: la política y la moral– necesita herramientas para cumplir de modo adecuado su función de ser un medio para el *imperio de la justicia* en la sociedad. A tal fin, el Derecho usa a la coerción y a la cooperación, que goza de preferencia axiológica sobre la primera por la propia caracterización del homo sapiens como un *ser cooperativo* –la cooperación constituyó un pilar en su evolución (TOMASELLO, 2016)–<sup>2</sup> que usa las razones para justificarse y convencer a los demás (MERCIER y SPERBER, 2017). Ello promueve la construcción de un *Derecho racional*.<sup>3</sup> Algunos subsistemas del Derecho son más proclives a la cooperación voluntaria, mientras que otros requieren de coerción para inducir a la cooperación; como veremos, este último es el supuesto del subsistema de la responsabilidad civil. En consecuencia, se requiere un marco jurídico coercitivo para desarrollar de modo cooperativo el mercado de productos y servicios dotados de inteligencia artificial (IA) –que están dinamizando el progreso social– eliminando incertidumbres y lagunas que podrían actuar como un obstáculo no tecnológico, promoviendo su crecimiento –a su vez– conforme a los valores y los principios consagrados en los Estados constitucionales de Derecho (BARRIO ANDRÉS, 2018). Por ello, será decisivo para la *adaptación* jurídica en esta era digital atender a la regulación del Derecho de Responsabilidad civil<sup>4</sup> por daños causados por la robótica y sistemas autónomos (RSA), que en el futuro –conforme a la aceleración tecnológica– podrían crecer de modo exponencial. Precisamente en este trabajo nos enfocamos en la prevención de los daños, función primordial del Derecho de la Responsabilidad civil, causados por los RSA en esta etapa tecnológica. Los RSA son objetos o productos con

<sup>1</sup> Ver von Bertalanffy (1989, pp. 125, 263 y 146). Este sistema abierto, está sujeto a tensiones y fuerzas que lo apartan del equilibrio continuo; caso contrario, sería un edificio muerto; ver Mascitti (2022a). En ese sentido, Reale dijo que la técnica del Derecho se va orientando cada vez a aquello que llamamos sistemas o modelos abiertos prefiriendo soluciones normativas que comporten mayor plasticidad en la adaptación a la experiencia corriente (1978).

<sup>2</sup> En esa línea, ver como las ideas de: la catedral (CALABRESI y MELAMED, 1972; NINO, 1990; CALABRESI, 2014; MASCITTI, 2022a), la novela en cadena (DWORKIN, 1986, p. 229) y la orquesta (RAWLS, 1999, p. 459) nos proporcionan la visión de la elaboración del Derecho por medio de la ejemplaridad o modelo-seguimiento dentro de una comunidad determinada.

<sup>3</sup> Ver nota 11.

<sup>4</sup> Lo llamamos de ese modo en vez de Derecho de daños ya que el actual sistema de responsabilidad civil se enfoca en la prevención del perjuicio como finalidad primordial.

autonomía limitada como veremos en el capítulo II; en consecuencia, se aplican las normas ordinarias de responsabilidad por daños causados por productos. A tal efecto, describimos el estado de la institución jurídica en cuestión –que carece de una regulación sistemática en el Derecho de los Estados constitucionales–<sup>5</sup> basándonos en un enfoque interdisciplinario para luego proponer soluciones apoyados en la particularidad del funcionamiento de los RSA. Así, este artículo usa la perspectiva de la teoría general de la responsabilidad civil, aunque, también se refiere a la legislación y a la jurisprudencia pertenecientes a sistemas jurídicos diversos, de modo principal al marco regulatorio y estratégico de la UE sobre los RSA –que constituyen las bases de esta: investigación y propuesta–. Por tanto, este trabajo se relaciona con la función de prevención de los daños en el Derecho privado patrimonial de los Estados constitucionales<sup>6</sup> que gozan de un marco teórico similar en cuanto a los principios básicos de esa función. En ese sentido, coincidimos con Stonoga en que la función preventiva de daños es intrínseca a los Estados constitucionales; así, por ejemplo, el legislador constituyente brasileño reconoció, en el art. 5º, XXXV, de la Constitución Federal, el derecho material a una adecuada tutela preventiva (2003, p. 26). Por ello, nos preguntamos si ¿el sistema actual de responsabilidad civil de los Estados constitucionales resulta adecuado para prevenir los daños causados por los RSA?; es decir, si *¿toma en serio* (DWORKIN, 1977) ese derecho constitucional?

Para contestar esa pregunta y brindar una propuesta sobre el tópico en cuestión, el trabajo se estructura del modo siguiente: en el capítulo II ofrecemos algunos rasgos característicos de los RSA que resultan necesarios para la argumentación esgrimida durante el desarrollo del artículo; a su vez, en el capítulo III, nos referimos a los niveles de riesgo de los RSA y a los métodos para esa calificación. Luego, en el capítulo IV, ejemplificamos la comunicación del Derecho con otras ramas de la cultura (Economía, Neurociencia y Ciencia de la computación), demostrando –de ese modo– la importancia de un enfoque interdisciplinario para la adaptación de la prevención de los daños causados por los RSA en la era

<sup>5</sup> El Derecho de los Estados constitucionales es un objeto cultural que consta de tres dimensiones: normológica, sociológica y axiológica, dentro de un ámbito temporal-espacial, que nos permite el diseño y la evolución del Derecho dentro de la tradición de cada comunidad; ello facilita la ductilidad –ver Zagrebelsky (2011)– de su normativa. El Derecho de los Estados constitucionales es un sistema abierto, como dijimos, que, a su vez, lo caracterizamos como una totalidad o unidad ya que el conocimiento de cualquier objeto dentro de ese sistema implica necesariamente el reconocimiento de su unidad (Pérez Bermejo, 2006). Esta unidad se refleja en el principio supremo de justicia –ver el último párrafo del capítulo V–, como el elemento que brinda coherencia a ese sistema, a través del resultado del balance de sus componentes en el caso concreto. Sobre la tridimensionalidad del Derecho en la era digital, ver Mascitti (2022b).

<sup>6</sup> Un ordenamiento jurídico constitucionalizado se caracteriza por una Constitución extremadamente invasora, entrometida, capaz de condicionar tanto la legislación como la jurisprudencia y el estilo doctrinal, la acción de los actores políticos, así como las relaciones sociales (GUASTINI, 2003, p. 153).

digital. En el capítulo V, delimitamos las funciones: preventiva y precautoria por daños causados por los RSA; asimismo, destacamos la utilidad de la adopción de otras medidas –que no quedan encuadradas en las funciones del Derecho de la responsabilidad civil– para la prevención de esos perjuicios. Por último, en el capítulo VI, finalizamos el trabajo con una conclusión de todo lo expuesto.

## II Los RSA como elementos de la complejidad de la era digital

Como paso previo al desarrollo de la función preventiva de los daños resulta oportuno caracterizar a los RSA, como entes que podrían causar esos perjuicios. Los RSA –funcionan a través de la IA encarnada y de la IA incorpórea–<sup>7</sup> son herramientas interconectadas, interactivas, cognitivas y físicas, capaces de percibir de diversas formas sus entornos, hacer o revisar planes y controlar sus acciones; realizan tareas útiles para nosotros en el mundo real, ampliando nuestras capacidades y aumentando nuestra productividad. Calificamos a la IA existente como estrecha; ella es la inteligencia de las máquinas que se limita a un área específica. Por otro lado, la inteligencia artificial general (IAG) –que hoy no existe– se refiere a un “hipotético programa informático que puede realizar tareas intelectuales tan bien o mejor que un humano” (HODSON, 2019). La IAG presentaría una nueva tecnología de uso general (TRAJTENBERG, 2019). Varios científicos –por ejemplo: Kurzweil (2005), Van de Gevel y Noussair (2013, p. 2), Chalmers (2010) y Brynjolfsson *et al.* (2017)– han pronosticado que con los avances en: la potencia de cálculo, la ciencia de los datos, la Neurociencia cognitiva y la bioingeniería, se alcanzará un punto de *singularidad* en un futuro no muy lejano, momento en el que la IAG superará la inteligencia de nivel humano (NAUDÉ y DIMITRI, 2020). La razón para no predecir la llegada de la IAG es que se trata de un cisne negro, que constituye un evento con tres atributos: rareza, impacto extremo e imprevisibilidad, aunque es previsible retrospectivamente (TALEB, 2007).

La autonomía es la característica distintiva de los RSA como surge de sus propios términos; ella consiste en su capacidad para realizar por sí misma una función. Se pueden clasificar a los sistemas a lo largo de un espectro de autonomía, dependiendo de la medida en que el sistema toma decisiones sobre sus propias acciones. Así, si un humano toma todas las decisiones más importantes, el sistema tiene poca o nada de autonomía. En el otro extremo, si un ordenador

<sup>7</sup> El primero se manifiesta en un objeto, por ejemplo, un robot como Alexa de Amazon, mientras que el segundo no se exterioriza en un objeto, sino en un servicio que utiliza IA. Por ejemplo, los servicios de *chatbot* son programas diseñados para simular una conversación natural.

toma todas las decisiones más significativas, la autonomía es total. En el medio, están los sistemas parcialmente o *semi* autónomos, en los que algunas acciones importantes son decididas por los humanos y otras por el ordenador (SURDEN Y WILLIAMS, 2016). La autonomía de las máquinas tiene tres dimensiones: el tipo de tarea que realiza la máquina; la relación entre el humano y una máquina en la realización de la labor y la sofisticación de la decisión de la máquina al realizar la tarea. Estas dimensiones son independientes entre sí y cuando se incrementa cualquiera de ellas, la máquina se torna más autónoma. Ante un grado mayor de autonomía, mayor será la probabilidad de que las acciones o decisiones de los RSA se tornen imprevisibles o azarosos para sus diseñadores, fabricantes, propietarios y operadores.<sup>8</sup> En ese sentido, es probable que en el futuro los RSA se *comporten* con mayor autonomía en base a la evolución tecnológica (MARCHISIO, 2021).

Los RSA son meros agentes ya que gozan de autonomía estrecha –es decir, la capacidad de decidir, sin intervención externa ni supervisión humana, entre modos diversos de realizar una tarea o alcanzar un objetivo determinado–; por tanto, los RSA carecen de autonomía fuerte –o sea, la capacidad de decidir libremente y coordinar la propia acción hacia un fin elegido– (BERTOLINI Y EPISCOPO, 2022). Así, los RSA no serían agentes morales<sup>9</sup> ya que al carecer de conciencia no tienen las tres capacidades de la agencia moral: la racionalidad,<sup>10</sup> la capacidad de conocer la diferencia entre el bien y el mal, y la capacidad de aplicar correctamente estas reglas a determinada situación paradigmática que constituye el significado de la regla (HIMMA, 2009).<sup>11</sup> Por consiguiente, desde la perspectiva jurídica, ellos

<sup>8</sup> Esa autonomía es puramente tecnológica y será mayor cuanto mayor sea el grado de sofisticación con que se haya diseñado el RSA para interactuar con su entorno (BARRIO ANDRÉS, 2018). Ver capítulo IV.

<sup>9</sup> En el capítulo I dijimos que el ser humano es cooperativo por la importancia de la cooperación para su evolución. Por consiguiente, la agencia moral no es ajeno a ello; en consecuencia, dicha agencia es el conjunto de mecanismos biológicos y culturales para facilitar esa cooperación (CHURCHLAND, 2017).

<sup>10</sup> Según Kahneman (2011), existen dos sistemas de pensamiento: rápido y lento; este último es el sistema racional o deliberativo, es el único que puede seguir reglas, comparar objetos en varios de sus atributos y hacer elecciones deliberadas entre opciones. Sin embargo, neurocientíficos –por ejemplo ver Slovic *et al.* (2004) y Feldman Barrett (2017)– cuestionan esa dicotomía ya que si la emoción se construye para contribuir al éxito de la anticipación y de la acción, entonces la función principal de la emoción no será la agitación, sino la información y la evaluación, es decir, la orientación y la guía (PESSOA, 2008). Por consiguiente, la agencia moral basada en la “razón kantiana” –que refleja el dualismo cartesiano– está siendo cuestionada por la Neurociencia; ver Cornejo Plaza (2022).

<sup>11</sup> Por el contrario, Floridi y Sanders (2004) sostienen, por ejemplo, que los sistemas de IA, pueden ser agentes morales si superan el test de un nivel mínimo de abstracción constituido por: la interactividad, la autonomía y la adaptabilidad. La interactividad significa que el agente y su entorno (pueden) actuar entre sí. La autonomía denota que el agente es capaz de cambiar de estado sin respuesta directa a la interacción: puede realizar transiciones internas para cambiar su estado. Por último, la adaptabilidad significa que las interacciones del agente pueden cambiar las reglas de transición que causa su cambio de estado.

Sin embargo, en términos de consecuencias prácticas, no es claro cuál es el beneficio de considerar a los RSA como agentes morales, ya que –como demuestra la responsabilidad objetiva– solo es posible orientar el producto hacia valores específicos influyendo en los diseñadores y fabricantes (MANTELERO, 2022, p. 102).

no son sujetos sino objetos o productos –artefactos elaborados por el diseño y el trabajo humano, con el fin de satisfacer necesidades humanas identificables (FOSSA, 2018)–.

### III Los RSA como productos riesgosos

Los RSA, en su calidad de meros agentes, tienen la capacidad de actuar físicamente sobre el mundo real. Ello refleja, a su vez, el potencial de dañar a las personas o a las cosas. Por consiguiente, consideramos adecuado clasificar los RSA según su riesgo potencial de causar daños: inaceptable, alto y bajo. Esto se basa en la distinción que hace la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas sobre la IA y se modifican determinados actos legislativos de la Unión (Propuesta de ley sobre IA de la UE). El título II de esta Propuesta considera inaceptables a los RSA que contravengan los valores de la UE, por ejemplo, por violar los derechos fundamentales –la dignidad constituye su núcleo irreductible, como veremos en el capítulo V–. A su vez, el título III de la Propuesta contiene normas específicas para aquellos RSA que acarreen un alto riesgo para la salud y la seguridad o los derechos fundamentales de las personas físicas. Por último, la Propuesta califica como de bajo riesgo a los RSA no incluidos en alguna de las categorías mencionadas; por ejemplo: el uso de *chatbots* y el uso gratuito de juegos o filtros de *spam* (CANTARINI, 2021).

Apoyamos la iniciativa de enumerar legalmente los RSA de riesgo inaceptable y de alto riesgo para brindar mayor certeza –por tanto, mayor seguridad jurídica– a la industria tecnológica respectiva y a los usuarios. Sin embargo, una enumeración taxativa obstaculizaría la actualización de los riesgos en virtud de la aceleración del desarrollo tecnológico que, de modo exponencial, genera y modifica los riesgos existentes y sus niveles de impacto en el individuo y en la sociedad.<sup>12</sup> Por consiguiente, proponemos que el centro algorítmico –que desarrollamos en el capítulo V– evalúe el nivel de riesgo en las etapas: estática y dinámica; así, la evaluación no impedirá que en cualquier momento de la evolución del algoritmo, la parte interesada tenga derecho a la modificación de la clasificación riesgosa de la

---

<sup>12</sup> En el mismo sentido Mantelero expresa que teniendo en cuenta la velocidad de la evolución de la tecnología de la IA y de los descubrimientos inesperados en relación con sus capacidades, puede resultar difícil mantener una lista cerrada de las aplicaciones típicas de alto riesgo de modo adecuado o puntual. Además, la decisión de delegar ese aspecto clave en la Comisión, el órgano ejecutivo de la UE, puede plantear problemas de reparto de competencias. Un enfoque de lista cerrada (aunque utilizando definiciones amplias y abiertas a la actualización) parece ser reactivo más que preventivo a la hora de anticiparse al desarrollo tecnológico (2022).

RSA –que contenga como base de funcionamiento a dicho algoritmo– por medio de petición fundada. Asimismo, resaltamos que cualquier empresa solicitante podrá reclamar la modificación del nivel del riesgo del RSA que es titular, pese a que este se encuadre en la lista de alguno de los tres niveles citados.

La lista de prácticas prohibidas del Título II de la Propuesta de ley sobre IA de la UE incluye al uso de sistemas de IA para la identificación biométrica remota *en tiempo real* de personas físicas en espacios de acceso público con fines policiales, excepto en: la búsqueda de víctimas, la prevención de amenazas a la vida o seguridad de las personas, y la identificación de un autor o sospechoso de un delito. La distinción entre el uso en tiempo real y el uso *a posteriori* corre el riesgo de ser arbitraria, no solo porque la categorización biométrica mediante el uso de múltiples características puede permitir la identificación, sino también porque los resultados de la identificación biométrica a distancia en espacios públicos sobre la libertad de reunión y la normalización de la vigilancia serían equivalentes en ambas circunstancias. Por ejemplo, el RSA de Clearview AI<sup>13</sup> se calificaría como un uso posterior que encuadraría dentro de los sistemas de alto riesgo. Asimismo, la Propuesta de ley sobre IA de la UE (art. 5 1.c) prohíbe los sistemas de IA que proporcionen el cómputo social de las personas físicas con fines generales por parte de las autoridades públicas o en su nombre. Sin embargo, el texto de compromiso del Consejo Europeo sobre el proyecto de ley de IA de la UE (2021) también prohíbe que las empresas privadas usen los RSA con fines de puntuación social.

A su vez, las categorías de aplicaciones de alto riesgo que figuran en el anexo III de la Propuesta de ley sobre IA de la UE<sup>14</sup> se definen a partir de una base de evaluación de la tecnología, que se apoya en cuatro elementos clave: a) características del sistema de IA (finalidad del sistema y alcance de su uso

<sup>13</sup> Clearview AI ha desarrollado un software de reconocimiento facial cuya base de datos se alimenta de la extracción de fotografías y de videos disponibles públicamente en Internet. Esta empresa ofrece el servicio a las autoridades policiales con el fin de identificar a los autores o víctimas de delitos. Clearview AI ha sido sancionada en varios países, por ejemplo: en Francia, CNIL (2021a) y en Italia, GPDP (2022). Ver CNIL (2021b).

<sup>14</sup> El anexo III de dicho documento establece áreas de alto riesgo. Estos ámbitos incluyen los RSA relativos a: 1) los sistemas biométricos; 2) las infraestructuras críticas y la protección del medio ambiente; 3) la educación y la formación profesional; 4) el empleo, la gestión de los trabajadores y el acceso al autoempleo; 5) el acceso y el disfrute de los servicios privados y de los servicios y prestaciones públicas; 6) la aplicación del Derecho; 7) la gestión de la migración, el asilo y el control de las fronteras; y 8) la administración de justicia y los procesos democráticos.

Por su parte, Canadá implementó la herramienta de Evaluación del Impacto Algorítmico, que es un cuestionario que determina el nivel de impacto de un RSA. Se compone de 48 preguntas de riesgo y 33 de mitigación. Las puntuaciones de la evaluación se basan en muchos factores, como: el diseño de los sistemas, el algoritmo, el tipo de decisión, el impacto y los datos. Ver <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html>.

probable); b) daño/impacto (perjuicio causado o previsto para la salud y para la seguridad o impactos adversos en los derechos fundamentales; alcance potencial de esos daños; reversibilidad); c) condición de las personas afectadas (dependencia o vulnerabilidad); d) protección jurídica (medidas de: reparación, prevención o minimización sustancial de esos riesgos). La clasificación se basa en un ejercicio abstracto del legislador (y de la Comisión en el futuro) por medio de un enfoque de escenario futuro o de generalización o enumeración de casos con relación a las prácticas existentes. Estos diferentes tipos de evaluación sugieren que las aplicaciones enumeradas en el anexo III, en su uso específico en el contexto adecuado, pueden no entrañar el alto nivel de riesgo que presume el Reglamento (MANTELERO, 2022). En cambio, podría ser útil para la determinación del nivel de riesgo de los RSA, la Evaluación del impacto social y ético de los derechos humanos (EISEDH) –constituye un modelo híbrido que tiene en cuenta el impacto: jurídico, ético y social de la tecnología–.<sup>15</sup> El encargado de aplicar este modelo será el centro algorítmico. Desde una perspectiva metodológica, el EISEDH se basa en: a- cuestionarios y herramientas de evaluación de riesgos en relación con la evaluación de los derechos humanos; b- el uso de expertos para abordar los retos sociales asociados al desarrollo y la aplicación de soluciones de IA; c- la participación, que permite comprender mejor los diferentes intereses contrapuestos y los valores de la sociedad; y d- la transparencia (MANTELERO, 2022). El EISEDH está alineado con el enfoque interdisciplinario como un medio para la protección de los derechos humanos.<sup>16</sup> A tal efecto, el EISEDH influirá en el diseño de los sistemas de IA especialmente en lo que respecta a la aceptabilidad<sup>17</sup> –se refiere a la conformidad de un RSA con los valores sociales y con los valores individuales, en el caso de los productos personalizados; por ejemplo, los sistemas policiales predictivos, aunque estén autorizados por el Derecho e incluyan garantías específicas, pueden ser considerados inaceptables por algunas comunidades– y a la tasa de sustitución de los sistemas de IA propuestos –se alude a la capacidad de ofrecer alternativas viables a los RSA, cuando estos últimos conllevan impactos posibles sobre los individuos y la sociedad– (MANTELERO, 2022); robusteciendo, así, el componente central del EISEDH, es decir, el modelo base de evaluación del impacto de los derechos humanos –ver Mantelero y Esposito (2021)–, para

<sup>15</sup> Conforme el carácter tridimensional del Derecho –ver nota 5–, algunos componentes axiológicos y sociológicos del EISEDH, que algunas concepciones iusfilosóficas ubican en la Ética y en la Sociología, integran su dimensión jurídica evaluativa.

<sup>16</sup> Ver el último párrafo del capítulo V.

<sup>17</sup> Una evaluación de la aceptabilidad social implica que la EISEDH ya ha determinado que el impacto sobre los derechos humanos no es perjudicial (MANTELERO, 2022).

la promoción de RSA que los respeten; previniendo, en consecuencia, lesiones a esos derechos.

## **IV El aporte interdisciplinario para la construcción de la función de la prevención de los daños causados por los RSA**

El moderno Derecho de la Responsabilidad civil se construye con la incorporación de las nociones preventivas (MORENO, 2017).<sup>18</sup> Las funciones predominantes del Derecho de la Responsabilidad civil se reducen a dos: la compensación y la prevención (ALPA, 1999); asimismo, el Derecho de la Responsabilidad civil contiene a la función punitiva y a la función precautoria. El término función significa una relación por la cual a cada estado o valor de alguna cosa (entendida como variable) le corresponde solo un estado o valor de la segunda. Descartes, Newton y Leibniz establecieron la idea de función como dependencia entre dos cantidades variables (ROYSTER, 2008, p. 61). Aplicando esa noción al Derecho de la Responsabilidad civil, las variables de la función llamada prevención son: 1) la vigencia de sanciones ya sean resarcitoria, punitiva, precautoria o preventiva directa o propiamente dicha y la 2) disminución en la causación de daños en una actividad determinada. La variable 2) es dependiente<sup>19</sup> de la variable 1). Por consiguiente, no hay función preventiva cuando no existe esa dependencia entre dichas variables.

La interacción de las variables 1) y 2) de la función preventiva denota la necesidad del uso del método interdisciplinario para una concepción adecuada de la figura objeto del presente trabajo. Por ejemplo, para observar las correlaciones que acaecen por el juego de esas variables resulta procedente el uso del análisis económico del Derecho<sup>20</sup> –cuya misión fundamental consiste en analizar y en reformar la totalidad del sistema jurídico mediante la aplicación de un número relativamente pequeño de conceptos económicos fundamentales (MINDA, 1991)– ya que nos permitirá conjeturar sobre la eficacia de la variable 1) como causa de la variable 2). En consecuencia, ello facilitará el ajuste de los medios para lograr el fin de la prevención de los daños ya que ella cumple un rol eficiente desde el punto de vista económico. Hoy la responsabilidad civil es contemplada como un fenómeno global, que posibilitó la incorporación de elementos de reflexión de

---

<sup>18</sup> Ello está dispuesto en el art. 1227 del Código Civil italiano. 1995)italiano—esta normativa sucontnes con causa desconocida o por

<sup>19</sup> Una variable dependiente es aquella cuyos valores dependen de los que tomen otra variable (DICCIONARIO DE MATEMÁTICAS).

<sup>20</sup> Como contrapunto del análisis económico del Derecho, ver Mascitti (2016).

orden económico (sobre todo macroeconómico) en el Derecho (DE ÁNGEL YÁGUEZ, 1995). Según el análisis económico del Derecho, el objetivo central del Derecho de la responsabilidad civil es reducir al mínimo el coste de los accidentes, es decir, la suma total de los recursos empleados en prevenir y resarcir los perjuicios (DÍEZ-PICAZO, 1999). Así, la responsabilidad civil puede entenderse como una regulación indirecta del mercado ya que el riesgo de incurrir en responsabilidad por daños proporciona un incentivo para invertir en seguridad (MARCHISIO, 2021). En cambio, el método de mercado dejaría que el nivel de actividades y accidentes se determinara enteramente por las decisiones individuales del mercado. Cuanto más costes de accidentes se atribuyan a una actividad o a una forma de hacerla, mayor será la presión para que cambie o disminuya. Pero en cualquier caso, el grado en que esto ocurra será el resultado de las decisiones individuales del mercado tomadas a la luz de los costes, incluidos los de los accidentes, que se produzcan (CALABRESI, 1968). El modelo del análisis económico básico de la responsabilidad civil parte de diversos supuestos que permiten analizar los efectos de las reglas de responsabilidad en los niveles de prevención adoptados por el agente generador del daño (bajo el supuesto de la prevención unilateral, relativa a aquellos supuestos en los cuales la prevención solo está en manos del posible victimario) o por este y la potencial víctima (en el modelo de la prevención bilateral, se refiere a aquellos supuestos en los que el potencial agente generador del daño y la víctima posible pueden reducir el riesgo de un accidente). Los supuestos metodológicos del modelo del análisis económico básico de la responsabilidad civil incluyen la elección racional de los agentes, a partir del cálculo de las probabilidades de que ocurra un daño, y el costo del accidente (MAQUEO RAMÍREZ, 2020). Sin embargo, la teoría económica del comportamiento cambió estas premisas, principalmente, en virtud de la atenuación del supuesto de la elección racional.<sup>21</sup> Ello se conecta con el enfoque neurocientífico, que desarrollaremos en el párrafo siguiente. Ahora bien, con relación a la aplicación de las categorías del análisis económico del Derecho de la responsabilidad civil por daños causados por los RSA, ella consiste en una táctica de incentivos aunque dentro de los límites prefijados por el objetivo estratégico de protección de los derechos fundamentales,<sup>22</sup> es decir, los derechos humanos que gozan de jerarquía constitucional. Un medio para ello sería el desarrollo de RSA eficientes y seguros, que obtendrían mayores beneficios y atraerían más capital en el mercado, expulsando a los RSA menos eficientes e inseguros de los mercados (GUERRA *et al.*, 2021). En ese sentido, la Propuesta de ley sobre IA de la UE busca garantizar la seguridad general del producto final,

<sup>21</sup> Ver Jolls *et al.* (1998) y Thaler (2018).

<sup>22</sup> Ver capítulo V.

ya sea exclusivamente un RSA o sea una cosa riesgosa integrada por un RSA.<sup>23</sup> Por último, resaltamos que el Derecho debe promover: a- la educación para el uso correcto de los RSA y b- la cooperación entre el hombre y la máquina<sup>24</sup> en los casos de prevención bilateral para que los RSA operen en entornos humanos de modo que mejoren nuestra humanidad;<sup>25</sup> a diferencia de los supuestos de prevención unilateral, como serían los escenarios donde los posibles daños previsibles de los RSA provengan del diseño y del entrenamiento algorítmico.

Asimismo, el enfoque neurocientífico nos aclara como las técnicas usadas por las empresas influyen en la toma de decisión de los usuarios. A su vez, esta perspectiva, también nos auxilia para conjeturar sobre la eficacia de las diversas sanciones o medidas (variable 1) para la disminución de los daños causados (variable 2) por los RSA. En ese sentido, se requiere investigar las herramientas que están siendo usadas por las empresas en el mercado digital para luego intervenir en este con el objetivo de proteger a los usuarios. Así, por ejemplo, observamos que durante al menos dos décadas, los diseñadores de sistemas digitales en línea han incorporado el conocimiento sobre heurísticos y sesgos para aumentar la capacidad de dichos sistemas de captar las emociones de los consumidores y neutralizar la cognición deliberativa (LUPIÁÑEZ-VILLANUEVA *et al.*, 2022). Así, los profesionales del marketing digital han desplegado tecnologías de gran alcance para la recogida de datos, la elaboración de perfiles y la selección de objetivos en línea, incorporando los últimos avances del mercado en campos como: la semántica, la IA, la teoría de las subastas, el análisis de las redes sociales, la minería de datos y la Neurociencia (CHOI Y LIM, 2020). Aquí se entrelazan claramente la protección: a la data de los usuarios y a su persona, en el caso de la toma de decisiones automatizadas ya que en base a los datos de los consumidores se los perfila en grupos o personalmente para luego, por medio de la decisión de los RSA, influir en su decisión de compra en el ámbito del *e-commerce*. Verbigracia, Uber, fija precios más elevados para aquellos usuarios con teléfonos con batería baja, ya que ellos pueden estar más desesperados; por tanto, dicha empresa podría eludir el RGDP ya que la información sobre la carga de la batería no puede identificar a un usuario específico (LI, 2022).<sup>26</sup> A su vez, por ejemplo, el usuario puede ver afectado su libre consentimiento –que constituye

<sup>23</sup> En cuanto a los RSA de alto riesgo que son componentes de seguridad de productos, la Propuesta de ley sobre IA de la UE se integrará en la legislación sectorial vigente en materia de seguridad para garantizar la coherencia –ver nota 5–, evitar duplicidades y reducir al mínimo las cargas adicionales.

<sup>24</sup> Ver capítulo V.

<sup>25</sup> Ver Charisi *et al.* (2021).

<sup>26</sup> Ver capítulo V.

una de las excepciones que permite la toma de decisión automatizada<sup>27</sup> por los patrones oscuros; por consiguiente, ello no equivale a una indicación específica, informada e inequívoca de la voluntad del interesado respecto al tratamiento de sus datos [Art. 4(11) Reglamento de protección de datos europeo, RGDP]. En esa línea, la CNIL consideró que Google infringió los requisitos de transparencia del art. 12(1) del RGDP en virtud del uso de patrones oscuros.<sup>28</sup> Ello podría causar daño patrimonial al usuario al quedar –en principio– sujeto al contrato respectivo. Asimismo, los avances en el ámbito del metaverso generan un potencial adicional de patrones oscuros más inmersivos y de personalización manipuladora, que pueden diferir significativamente de los patrones oscuros clásicos o de las técnicas de personalización usadas hasta hoy, y pueden tener implicaciones profundas para la toma de decisiones de los consumidores en el entorno digital.<sup>29</sup> Así, se requiere un marco regulatorio adecuado para prevenir los daños causados al consumidor por medio de los patrones oscuros<sup>30</sup> y mediante la personalización manipuladora. La regulación desde el diseño se torna imprescindible ya que las sanciones resultarán insuficientes para tutelar al consumidor como veremos en el capítulo V. A tal efecto, la arquitectura de diseño algorítmico deberá implicar directamente a las empresas y a la comunidad de diseñadores –representadas en el centro algorítmico–, por ejemplo, elaborando directrices y ejemplos prácticos que les permitan determinar *ex ante* si las prácticas que están considerando pueden ser desleales con el fin de proteger las capacidades humanas en lugar de reducir su agencia (HILDEBRANDT, 2021),<sup>31</sup> cuya tutela como neuroderecho es reclamada por la doctrina.<sup>32</sup>

<sup>27</sup> Según el artículo 22 del RGDP todo interesado tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

Para un análisis jurisprudencial de las tres excepciones [artículo 22(2)] del artículo 22(1) [a- se refiere a la toma de decisiones automatizada que es necesaria para celebrar o ejecutar un contrato con el interesado; b- cubre la toma de decisiones automatizada que está legalmente autorizada; y c- abre la posibilidad de confiar en el consentimiento del interesado; y en las situaciones en las que cualquier tratamiento de datos implicado en las prácticas de toma de decisiones automatizadas no están cubiertas por el artículo 22 –debe tener una base legal para el tratamiento como se requiere en el artículo 6(1) y, si el tratamiento incluye categorías especiales de datos, una condición adicional derivada del artículo 9(2)–], ver Barros Vale y Zanfir-Fortuna (2022).

<sup>28</sup> Ver <https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf>.

<sup>29</sup> Por ejemplo, algunos adultos sin trastornos de la personalidad pueden acentuar su comportamiento de modo intimidatorio en las redes sociales creando un avatar separado de su identidad cotidiana. Ver Suler (2015).

<sup>30</sup> Existen seis tipos de patrones oscuros: sobrecarga, omisión, agitación, obstaculización, inconstante y dejada en la oscuridad. Ver European Data Protection Board (2022).

<sup>31</sup> Ver capítulo II.

<sup>32</sup> Ver: Yuste *et al.* (2021), Cornejo Plaza (2021) y Mascitti (2022b).

En 2019, 25 expertos en Medicina, Bioética, Derecho y otras disciplinas propusieron añadir nuevos neuroderechos a la Declaración Universal de DDHH de Naciones Unidas. Esa declaración sentó las bases

Por otra parte, la Ciencia de la computación nos asiste para determinar la insuficiencia de la teoría de la causalidad adecuada como presupuesto de la responsabilidad civil por los daños causados por los RSA. Las cuestiones relativas al nexo causal resultan comunes –en principio– a todos los ordenamientos jurídicos.<sup>33</sup> La teoría de la causalidad adecuada es adoptada por el Derecho ya que el azar –como imprevisibilidad– constituye un límite para el Derecho privado patrimonial (MASCITTI, 2019). La relación de causalidad adecuada juega como una previsibilidad del riesgo de daño que es relevante para responder a la pregunta de si una persona prudente habría tomado alguna precaución contra el riesgo de la cosa de causar daño a terceros; es decir, una previsibilidad en abstracto a diferencia de la culpa como factor de atribución que exige una previsión en concreto. Desde un enfoque estratégico, la finalidad del Derecho de la Responsabilidad civil –que, en este caso, consiste en exigir a los diseñadores, fabricantes, propietarios y operadores una conducta diligente para reducir el riesgo de los RSA puestos en el mercado, que se infiere de la indemnización de los daños causados de forma previsible– sería imposible de cumplir en el caso de los daños causados por los RSA en los casos descriptos, precisamente por ser imprevisibles para esos individuos, afectando –de ese modo– al requisito del *rule of law* –“es el nombre que se da comúnmente al estado de cosas en el que un sistema jurídico está en buen estado” (FINNIS, 1980, p. 270)– de no sancionar prescripciones imposibles.<sup>34</sup> Una regla puede ser comprensible y no incoherente pero, en la práctica, imposible de seguir; una regla que la gente no puede seguir es una regla que no puede guiar la conducta humana, incluso si se entiende perfectamente bien (MARMOR, 2016, p. 21). El núcleo argumental de la idea de la insuficiencia de la causalidad adecuada radica en que los RSA funcionan mediante correlaciones<sup>35</sup> que operan como límite a la previsibilidad de diseñadores, fabricantes, propietarios y operadores; ello constituye un elemento esencial para calificar la causalidad adecuada como presupuesto del Derecho de la responsabilidad civil. La dificultad para precisar por qué un sistema de IA logró un determinado resultado o decisión puede hacer que los procesos de toma de

---

para el primer paso normativo. Hoy, Chile es el único país con una propuesta de ley y una enmienda constitucional que ordena la neuroprotección. Ver los proyectos chilenos de: a) ley sobre la protección de los neuroderechos, la integridad mental y que regula el desarrollo de la investigación y el avance de las neurotecnologías, boletín 13.828-19 y b) el proyecto de reforma constitucional, que modifica el artículo 19, número 1º, de la carta fundamental, en materia de protección sobre la integridad y la indemnidad mental en relación al avance de las neurotecnologías, boletín 13.827-19. Ver capítulo V.

<sup>33</sup> Ver Mascitti (2021b).

<sup>34</sup> La esencia del *rule of law* es la previsibilidad (WALDRON, 2008) y su objetivo es evitar la arbitrariedad del poder tanto como sea posible.

<sup>35</sup> Ver Mayer Schonberger y Cukier (2013).

decisiones de la IA sean impenetrables, tornándolos en cajas negras. Por ejemplo, el modelado de aprendizaje profundo<sup>36</sup> suele realizarse por medio del desarrollo de cajas negras: el algoritmo toma muchos puntos de datos como entradas y correlaciona características específicas de los datos para producir una salida. Ese proceso es en gran medida autodirigido y suele ser difícil de interpretar para los científicos de datos, los programadores y los usuarios (WIGMORE, 2019). En cambio, los modelos de aprendizaje automático también pueden ser de caja blanca. El funcionamiento interno de los modelos de caja blanca es transparente. Los modelos de aprendizaje automático son más complejos que los modelos estadísticos clásicos, pero existen técnicas para aumentar considerablemente la transparencia y transformar aquellos modelos en cajas blancas.<sup>37</sup> Así, la comprensión de las causas y correlaciones de las decisiones algorítmicas es uno de los principales retos de la Ciencia de la computación, que se aborda bajo el término *IA explicable*; también ella es reconocida por el Derecho, por ejemplo cuando este exige la explicación de la lógica de las decisiones automatizadas, como veremos en el capítulo siguiente.<sup>38</sup> Como señalamos en el capítulo II, la relación entre la previsibilidad de la máquina y la intervención humana es directamente proporcional; es decir, la máquina es menos previsible cuanto menos necesita la intervención humana. En definitiva, el aprendizaje automático de algunos RSA transforma su sistema operativo en un conjunto de algoritmos que lleva a las RSA a causar daños en algunos casos imprevisibles para sus diseñadores, fabricantes, propietarios y operadores, ya que entre el evento original (el comportamiento de la RSA) y el daño hay otro u otros eventos (las correlaciones realizadas por la RSA a través del aprendizaje de la máquina) que no son previsibles según el curso normal de los acontecimientos. En consecuencia, consideramos que debe crearse la figura del fondo de garantía independiente de la contratación de un seguro obligatorio por responsabilidad civil,<sup>39</sup> que será útil para adjudicarle a la víctima

<sup>36</sup> Aunque el aprendizaje profundo ha dado resultados impresionantes en dominios de alta intensidad computacional, la palabra “profunda” se refiere a una propiedad técnica (es decir, el número de capas ocultas o convolucionales) y no implica sofisticación conceptual (MARKOU y DEAKIN; 2020).

<sup>37</sup> Existen dos modos de proporcionar comprensibilidad en el aprendizaje automático: la comprensibilidad intrínseca se adquiere cuando se usan modelos que son comprensibles por naturaleza en virtud de su estructura simple, que son los denominados modelos de caja blanca, mientras que la comprensibilidad *post-hoc* tiene como objetivo explicar las predicciones sin acceder a la estructura interna del modelo o las explicaciones contrafactuales (GOETHALS *et al.*, 2022).

<sup>38</sup> En ese sentido, sobre una perspectiva de los distintos tipos de explicación en correlación con los factores técnicos y jurídicos que inciden en la viabilidad de la explicación e información ofrecida a la persona afectada por una decisión algorítmica, ver Brkan y Bonnet (2020).

<sup>39</sup> En esa línea, Bertolini afirma que todos los fabricantes deberían tener un seguro obligatorio contra terceros con el objetivo de cubrir todos los costes, ya que son los actores principales desde la perspectiva de la disuasión y la gestión de riesgos. El seguro es una herramienta fundamental y se convertirá en una herramienta importante para permitir la transferencia de tecnología de la investigación al mercado (2017).

de los perjuicios producidos por estos mecanismos autónomos precisamente cuando a raíz del sistema de correlaciones la imprevisibilidad impide la asignación correspondiente de responsabilidad. Por otra parte, el fondo de garantía será sustentado por los aportes de las empresas que colocan RSA en el mercado, y de aquellas empresas que tienen su dirección, control y uso. Proponemos que la cantidad de ese aporte sea efectuado en grado decreciente desde aquellos sujetos vinculados a los RSA de alto riesgo a los RSA de menor riesgo ya que se genera una situación de peligro comunitario por los RSA puestos por ellos en el mercado. De este modo, el Estado incentivará el desarrollo de RSA menos riesgosos porque estos serán productos cuyo precio final reflejará el traslado de un costo menor –en comparación con productos de riesgo más elevado– por el aporte para el fondo de garantía efectuado por los empresarios. A su vez, el carácter privado, público o mixto del ente encargado de administrar dicho fondo dependerá del contexto jurídico e institucional en el que opere, especialmente en lo que respecta a la forma en que se diseña la red de seguridad social en cada país (DICKSON *et al.*, 2016). Asimismo, el fondo de garantía bajará los costos de litigación, que representan un costo social importante.<sup>40</sup> En fin, proponemos que en el caso de que el funcionamiento del RSA sea normal se aplique la responsabilidad objetiva<sup>41</sup> basada en la teoría de la causalidad adecuada; pero en el supuesto de que exista un daño provocado que ha sido imprevisible para el diseñador, fabricante, propietario y operador, en virtud del accionar del RSA en base a correlaciones, estas impiden analizar la causalidad;<sup>42</sup> por consiguiente al no poder asignar responsabilidad a aquellos, operará el fondo de garantía.<sup>43</sup> En

<sup>40</sup> Sin embargo, el fondo de garantía posibilita que se produzca el tipo de lagunas de retribución que Danaher (2016) analiza sobre los daños causados por los RSA. Cuando alguien resulta lesionado por la acción de otra persona (ya sea un humano o un RSA), la gente tiende a querer encontrar a uno o a varios individuos que puedan ser sancionados por ello (NYHOLM, 2018).

<sup>41</sup> Los sistemas de responsabilidad civil basados en el factor de atribución objetivo están mostrando deficiencias en términos de incentivos de seguridad, en ausencia de la disuasión provocada por la responsabilidad civil *tradicional*. Ver Wallis (2013). Por ello, la principal debilidad de los sistemas sin culpa es la dificultad de garantizar que los potenciales causantes de pérdidas tengan la cantidad de cuidado socialmente óptima, ya que se cortan los vínculos entre su potencial para causar pérdidas y los costes de sus acciones (HOWELL *et al.*, 2002).

<sup>42</sup> Pero en el aprendizaje por refuerzo, no hay culpa por parte de los humanos ni previsibilidad de tal lesión, de ese modo, el Derecho de la Responsabilidad civil tradicional diría que el desarrollador no es responsable (ELMAN y CASTILLA, 2017). La previsibilidad genera que la responsabilidad objetiva sea poco adecuada para las lesiones causadas por los RSA (BARFIELD, 2018).

<sup>43</sup> En ese sentido, la Comisión sobre normas de Derecho civil sobre robótica de la UE (2015) solicita la necesidad de establecer: a) seguros obligatorios; b) fondos de compensación ante la inexistencia de seguros; c) que el fabricante, programador o usuario puedan beneficiarse de un régimen de responsabilidad limitada en caso de contribución a un fondo o suscripción de seguros; d) la creación de patrimonios individuales por robot o para todos los robots con el pago único por su introducción al mercado o pagos periódicos; e) la creación de un número de matrícula o registro del robot que lo vincule con un fondo en particular; y f)

estos casos se reconocería efectos al azar o imprevisibilidad del sistema de las correlaciones pero contenido a través de la certidumbre de la existencia de un fondo de garantía que cubra al lesionado.

Así, observamos que existen condicionantes (por ejemplo: seguro, fondo de garantía y personalidad jurídica de los RSA) que impiden la aparición de la función preventiva ya que *vacían* de potencia a la variable 1); es decir, inhiben el costo económico que disuade a los actores a la adopción de medidas que disminuyan los riesgos de causación de daños –variable 2)–. En consecuencia, en el ámbito de actuación de los RSA el seguro obligatorio sería un condicionante o inhibidor de la disuasión de la prevención de daños. Los regímenes de seguro obligatorio sin culpa –gozan de varias ventajas económicas como la reducción de los costes administrativos y la obtención de resultados más equitativos (LIAO y WHITE, 2002, p. 259)– relacionados a los RSA padecen de dificultad para fijar las primas<sup>44</sup> y evaluar el riesgo potencial de daños en virtud de la complejidad de su funcionamiento que desarrollamos en el capítulo II. Ahora bien, el seguro obligatorio de responsabilidad civil contiene el deber de prevención de daños que abarca cuestiones no inminentes e inminentes. Así, las primeras son pasibles de exclusión de cobertura, no así las restantes. Por ejemplo, la cláusula de exclusión de cobertura llamada *recall*, o sea, el retiro del mercado de los productos, entre ellos los RSA, que pueden producir daños a terceros, se refiere a cuestiones inminentes por ello resulta contraria a la normativa de orden público, por tanto es nula. Por el contrario, las cláusulas de exclusión de cobertura relativas a cuestiones

---

finalmente, el expediente de recurrir a la creación de una personalidad electrónica responsable de reparar los daños que pueda causar (con un patrimonio que respalde a la misma).

Por su parte, la Resolución del grupo de expertos en responsabilidad y nuevas tecnologías de la UE (2018) sugiere que las normas de responsabilidad civil sigan un enfoque de dos niveles: establecer seguros y no derogar lo establecido por la directiva 85/374/CEE de responsabilidad por los daños causados por productos defectuosos, basado en el nivel de riesgo que conlleva el uso de una tecnología determinada:

(1) Si esta no plantea riesgos graves de daños a terceros, el usuario debería cumplir con los deberes de seleccionar, operar, supervisar y mantener cuidadosamente dicha tecnología y ser considerado responsable de su incumplimiento según un régimen basado en la culpa. Cuando se trata de RSA, la responsabilidad no debe ser menos severa que la prevista para los daños causados por auxiliares humanos.

(2) Si la tecnología conlleva un mayor riesgo de daños a terceros, el operador debería ser considerado estrictamente responsable de los daños derivados de su funcionamiento y posiblemente estar sujeto a un seguro obligatorio. Dicho operador debería ser identificado como el sujeto que más controla la tecnología y se beneficia de ella. Cuando puedan identificarse varios operadores, la responsabilidad objetiva debe recaer en el “sujeto que tiene más control sobre los riesgos de la operación”, que –según las circunstancias– puede ser el usuario final u otro sujeto, al que el grupo de expertos designa como operador final (BERTOLINI y EPISCOPO, 2021).

En esa línea, el Parlamento Europeo (2020) regula: la responsabilidad objetiva por los daños causados por los RSA de alto riesgo (art. 3) y la responsabilidad subjetiva por los daños causados por los RSA que no son de alto riesgo (art. 8).

<sup>44</sup> Asimismo, cuando los RSA son gobernados por sus diseñadores, operadores y usuarios, la cuestión de quién paga las primas del seguro se torna compleja (RACHUM-TWAIG, 2020).

no inminentes son válidas, verbigracia: protección contra incendios causados por los RSA. Por último, en la Argentina, la exclusión genérica de cobertura, es decir, sin límites ni especificaciones, resulta nula en virtud de lo dispuesto por el art. 989 del Código Civil y Comercial (CCCA) (SOBRINO, 2017). Por otra parte, como dijimos, el fondo de garantía operaría ante los supuestos no encuadrables en el régimen de responsabilidad civil por incumplimiento de uno de sus presupuestos: la causalidad adecuada. Por consiguiente, aquí la responsabilidad civil no induciría (ni podría inducir) inversiones virtuosas en seguridad –variable 1)– para disminuir los daños causados por los RSA –variable 2)–. De ese modo, aplicar las sanciones provenientes del régimen de la responsabilidad civil eliminaría incentivos para la introducción en el mercado de los RSA, reduciendo la eficiencia general y la seguridad. A su vez, es probable que dicha regulación impida a las empresas introducir a los RSA en el mercado o desarrollarlos, obstaculizando así el progreso tecnológico –ello es denominado riesgo de *technology chilling*– (MARCHISIO, 2021).<sup>45</sup> Asimismo, no solo no se prevendrían los daños –es decir no acaecería la variable 2) derivada de la variable 1)– sino que se generaría una externalidad negativa significativa porque las sanciones prescriptas en el sistema de responsabilidad civil funcionarían como un desincentivo ya que los productores podrían abandonar la investigación y el desarrollo de los RSA que operen en entornos de riesgo, impidiendo –así– un aumento importante de la seguridad y reducción del número global y la relevancia de los accidentes, conculcando –de ese modo– al bien común como veremos en el capítulo V. Por el contrario, la creación del fondo de garantía tendría un efecto sistémico, es decir, proporcionaría un buen funcionamiento del mercado en su conjunto. Por último, destacamos que el Comité Económico y Social Europeo, en su dictamen de 2017 sobre la IA, se opuso a la introducción de una forma de personalidad jurídica para los RSA, ya que consideró que dicha solución obstaculizará el efecto preventivo del Derecho de la responsabilidad civil. Por consiguiente, inferimos que, según dicho Comité, la personalidad jurídica de los RSA impedirá una internalización adecuada de los costes por parte de quienes controlan los riesgos y se benefician de ellos.<sup>46</sup>

<sup>45</sup> Ver, entre otros: Magrani (2019); Pellegatta (2019) y Palmerini y Bertolini (2016).

<sup>46</sup> Por el contrario, Bertolini y Episcopo (2022) consideran que –pese a que hoy no existen razones ontológicas para categorizar a los RSA como sujetos jurídicos– hay motivos funcionales para otorgarle formas limitadas y estrechas de personalidad jurídica a los RSA en circunstancias determinadas; por ejemplo, entre otras razones, para: a) la simplificación de las relaciones jurídicas, b) la trazabilidad, el registro y la transparencia de la entidad y de quienes poseen intereses en ella y en su funcionamiento, c) la segregación de activos y las limitaciones de responsabilidad.

## V La trama de las funciones de la responsabilidad civil como sustento de la prevención de los daños

La adscripción de funciones uno a uno (asignar a una institución exclusivamente función preventiva; a otra, solo función resarcitoria, etc.), parte de una restricción que no tiene por qué constreñir a los legisladores, ni parece una guía adecuada para legislar o para interpretar el ordenamiento jurídico. Ello no significa que algunas instituciones no tengan un rol prioritariamente vinculado a una función, en el sentido de que sean más importantes o eficaces en relación con una función, que respecto de otra (ACCIARI, 2013). De aquí la pluralidad de categorías jurídicas que quedan subsumidas bajo la figura de la prevención de daños; a ellas las incluimos en la variable 1) enunciada en el capítulo IV: a) la adopción de medidas técnicas idóneas para evitar un daño, es decir, el ejercicio de la función preventiva directa; b) la prevención como función indirecta de la precaución; c) la prevención como función indirecta de la sanción resarcitoria;<sup>47</sup> y d) la prevención como función indirecta de los *punitive damages*.

En la prevención de daños a) nos referimos a situaciones donde ella tiende a la evitación de un daño futuro, inminente y cierto. Aquí, por ejemplo, la creación de un centro algorítmico sería conveniente para la determinación de esa situación y de su solución posible. Propiciamos que este ente sea de naturaleza mixta –público y privado–<sup>48</sup> y esté integrado por personal interdisciplinario; y tenga como misión el control de la dinámica de los RSA –es decir de su funcionamiento– y el registro de ellos –o sea, la etapa previa a su puesta en marcha–. El centro algorítmico estará integrado por expertos y tendrá participación ciudadana en los casos que impliquen riesgos altos para la ciudadanía, especialmente, representación de la población vulnerable. Así, serán actores destacados los: representantes de los consumidores, empresarios, expertos (por ejemplo: académicos) y funcionarios públicos especializados. Proponemos que el centro algorítmico asesore a las autoridades: ejecutiva, judicial y legislativa. El centro algorítmico será fundamental en el análisis de las bases técnicas para el dictado de cualquier medida, ya sea: preventiva directa, precautoria, resarcitoria o punitiva; por consiguiente, por ejemplo, aquel deberá proponer que los *datasets* contengan datos de alta calidad, que son

<sup>47</sup> Sin embargo, por ejemplo, el sistema de Responsabilidad civil en Europa continental concede indemnizaciones que quedan muy por debajo de los costes sociales de los daños causados; es decir no se aplica efectivamente el principio de la reparación integral de daños (SALVADOR CODERCH, 2019).

<sup>48</sup> En esa línea, Brownsword dice que como las soluciones tecnológicas se desarrollarán a menudo en el sector privado, parece que es necesaria una asociación público-privada o algún modo de corregulación en la que los organismos públicos fijen los objetivos normativos deseados pero facilitando el progreso tecnológico por medio de la industria privada (2022, p. 51).

esenciales para los algoritmos de alta calidad,<sup>49</sup> porque ser transparente sobre los datos que se utilizan en los sistemas de IA ayuda a prevenir posibles violaciones de derechos; por ejemplo, esto se refleja en el art. 9 del RGDP. Asimismo, ese centro algorítmico podría detectar –verbigracia– la existencia de líneas de código que reflejen los sesgos de sus diseñadores; de ese modo, ello sería un medio para prevenir la discriminación hacia terceros.<sup>50</sup> A su vez, resaltamos que un modelo puede estar sesgado con respecto a la edad, el género, etc., pese a que esas características no se usen como entrada a aquel. Existen dentro del código muchas medidas de equidad aunque puede resultar imposible satisfacer alguna combinación de ellas simultáneamente. De este modo, los sesgos humanos se filtran en los datos usados para entrenar los modelos de aprendizaje automático. Por ejemplo, para una demostración de como el algoritmo COMPAS -programa que intenta predecir las tendencias delictivas de las personas- puede estar sesgado en base a los datos incorporados al sistema pese a que ellos no estén vinculados a las etiquetas incorporadas al código, ver Farhan Rahman (2020). Por otra parte, el derecho a la protección contra el sesgo algorítmico constituye un neuroderecho.<sup>51</sup> Además, la vigilancia selectiva de las categorías de personas basada en inferencias computacionales ignora los fundamentos de la presunción de inocencia,<sup>52</sup> que, junto con el derecho a la intimidad y a la no discriminación,<sup>53</sup> se relaciona de modo directo con el debido proceso<sup>54</sup> –requerimiento del *rule of law*, ver el último párrafo de este capítulo–. Por otra parte, el centro algorítmico podría “estresar” al algoritmo a través de otros datos para buscar los resultados por medio de tests en ambientes diversos. Asimismo, el centro algorítmico podría asesorar al órgano administrativo correspondiente –en una instancia previa a dicho juicio– y al juez en los procesos judiciales sobre las medidas técnicas adecuadas para disminuir la probabilidad de la causación del daño a terceros, teniendo en cuenta el principio de la continuidad empresarial y el progreso científico con el norte de balancear los intereses en juego, siempre considerando a la dignidad como elemento nuclear del Derecho.<sup>55</sup> Así, por ejemplo, el centro algorítmico podría aconsejar al juez sobre

<sup>49</sup> Ver, entre otros, Stalla *et al.* (2020) y Hildebrandt (2020a). En ese sentido, una acción judicial contra el tratamiento de datos sensibles no requiere pruebas de que se haya producido un daño; es decir, tienen carácter preventivo. Frenar la reutilización de los datos personales, limitando también su recogida, es un modo de evitar la dataficación de todo y las amenazas que ello conlleva (HILDEBRANDT, 2015).

<sup>50</sup> Ver Mascitti (2021a).

<sup>51</sup> Ver capítulo IV.

<sup>52</sup> En esa línea, ver la Propuesta de ley sobre IA de la UE (38) y Galli (2021).

<sup>53</sup> Ver O’Neil (2016).

<sup>54</sup> Incluso desde la perspectiva del análisis económico del derecho, el debido proceso podría ser ventajoso en la medida en que crea una igualdad de condiciones (HILDEBRANDT, 2015).

<sup>55</sup> En un sentido similar, el Centro de Tecnología y Sociedad de la Facultad de Derecho de la FGV señaló en su contribución a la consulta pública de la Estrategia Brasileña de IA que “[la] creación de un organismo

la probabilidad del daño en el caso concreto que justifique el peligro en la demora como requisito para la adopción de una medida preventiva; dentro de ese género de resoluciones procesales destacamos a las medidas autosatisfactivas –ver Peyrano (1998)– y a la tutela anticipada –ver Papo y González (2006)–.<sup>56</sup> Por otro lado, el centro algorítmico podría asesorar a los jueces sobre la adopción de una medida cautelar que ofrezca cierta flexibilidad –siempre dentro de un lapso relativo a la urgencia que provoca el accionar de la función preventiva– a la empresa para que ella reescriba su código. De aquí que en vez de ordenar que el código se escriba de un modo específico, resulta aconsejable que el juez ordene a la empresa que encuentre el modo adecuado de lograr un resultado específico<sup>57</sup> teniendo en cuenta que: el contexto tecnológico para la creación de un modelo o sistema de IA embebido en un hardware es un proceso complejo que requiere su iteración en diversos ambientes. Un medio apropiado para aumentar esa flexibilidad consiste en ampliar el plazo de cumplimiento de la orden judicial a las empresas en virtud de la complejidad del sistema de aprendizaje automático.<sup>58</sup> De este modo, la extensión temporal constituye una medida que procura prevenir los daños causados por los RSA.<sup>59</sup> Por otra parte, las órdenes judiciales que implican la reescritura de código pueden enviarse con carácter retroactivo. Por ejemplo, Tesla actualiza periódicamente el *software* de los coches vendidos. A diferencia de los productos tradicionales, en los que una orden judicial se limita generalmente a la venta de productos en el futuro, las órdenes judiciales contra los RSA pueden

---

regulador especializado e independiente, capaz de revisar y autorizar los sistemas de decisión algorítmica” sería una forma de mitigar los problemas derivados de los sistemas de IA y la aplicación de la normativa. Dicha autoridad podría definir “qué tipos de auditorías pueden llevarse a cabo; qué requisitos técnicos y/o legales deben cumplirse en cada caso” y determinar en qué casos deben permitirse las decisiones automatizadas y en cuales no, mediante la evaluación de los riesgos de violación de los derechos y la evaluación de la “opacidad intrínseca” de los sistemas, un enfoque parecido al proyecto de reglamento de la UE antes mencionado. La autoridad también podría abordar qué tipos de “decisiones o contextos (...) requieren una explicación más precisa de la decisión [automatizada] o la posibilidad de una revisión humana” y definir “los requisitos técnicos que deben seguir las organizaciones tanto en el desarrollo como en el uso de los sistemas de IA”. Ver Hartmann *et al.* (2022).

En esa línea, la agencia de administración de alimentos y medicamentos de EEUU supervisa los algoritmos de los dispositivos médicos, incluido un dispositivo que utiliza la IA para analizar las imágenes del ojo y detectar si los pacientes con diabetes pueden estar desarrollando una retinopatía diabética, que provoca la pérdida de visión (FEDERAL DRUG ADMINISTRATION, 2018).

<sup>56</sup> En el marco de esta figura, ver, por ejemplo: el art. 680 bis del Código Procesal Civil y Comercial de la nación argentina, el fallo de Corte Suprema de Justicia de la Nación argentina (CSJN) en autos “Camacho Acosta vs. Grafi Graf”, fallo: 320:1633, 1997; y el art. 300 § 3º del Código de Proceso Civil brasileiro.

<sup>57</sup> Este criterio de restricción mínima encuadra dentro de lo dispuesto por el artículo 1713 del CCCA.

<sup>58</sup> En ese sentido, con relación a la regulación de los *bots*, ver Lamo y Calo (2018).

<sup>59</sup> En el ámbito temporal del Derecho, observamos como la jurisprudencia juega con la función de prevención de daños: antes de que se produzca el daño (medidas preventivas), mientras se produce (orden de cese), después de que se produzca (daños temporales) y después de que se haya reconocido legalmente (*punitive damages*) (SINTEZ, 2009). En relación con las normas legales, también desde esta perspectiva temporal, ver, por ejemplo, el art. 1710 del CCCA.

afectar a aquellos que ya están en manos de los consumidores. Eso genera que la orden judicial sea más eficaz (LEMLEY y CASEY, 2019). Así, el juez, como un estratega, puede alinear la medida judicial con el fin de prevenir los daños hacia el futuro, como lo efectúa de modo habitual, y estrechar –a su vez– la dimensión temporal hacia el presente.

En cuanto a los requisitos para la procedencia de la acción preventiva por daños, que ubicamos dentro de la categoría función preventiva a), por ejemplo, el art. 1711 del CCCA expresa que ella “procede cuando una acción u omisión antijurídica hace previsible la producción de un daño, su continuación o agravamiento. No es exigible la concurrencia de ningún factor de atribución”. En relación con los daños causados por los RSA,<sup>60</sup> como vimos en el capítulo IV, en ciertos casos existe imprevisibilidad surgida del funcionamiento algorítmico de esos sistemas de IA basados en su aprendizaje automático a través de correlaciones. Ello trasluce la improcedencia de dicha acción preventiva en esos supuestos. Por consiguiente, se refuerza la necesidad de evitar con mayor anticipación el acaecimiento de los eventos dañosos. Por ello, pensamos que resulta apropiado el uso de la categoría b) en los supuestos de incertidumbre científica ante escenarios posibles de daños graves e irreversibles causados por los RSA. En esa línea, por ejemplo, el marco regulatorio europeo de la IA tiene al principio precautorio como uno de sus pilares.<sup>61</sup> La diferencia entre la prevención y la precaución radica en que en la primera, la peligrosidad de la cosa o actividad es conocida, y lo único que se ignora es si el daño va a producirse en un caso concreto; en cambio, en la segunda, la incertidumbre recae sobre la peligrosidad de la cosa ya que los conocimientos científicos son insuficientes para brindar una respuesta adecuada (ANDORNO, 2002). La precaución desafía la hegemonía del análisis coste-beneficio para dar lugar a una visión más amplia en el tiempo-espacio en aras del bien común de las generaciones presentes y futuras (ANDORNO, 2004). En ese sentido, coincidimos con Palmerini *et al.* (2016) en que la decisión regulatoria debe basarse en la ponderación de la perspectiva del impulso tecnológico, por un lado, y la seguridad,

<sup>60</sup> Los RSA podrían dañar a: los derechos individuales, los derechos de incidencia colectiva que recaen sobre derechos individuales homogéneos –ver CSJN, Halabi, Fallos: 332:111, 2009– y los derechos de incidencia colectiva que tienen por objeto bienes colectivos, por ejemplo el medio ambiente –como veremos en el párrafo final de este capítulo–.

<sup>61</sup> En ese sentido, ver Parlamento Europeo (2015/2103).

Por el contrario, sobre una perspectiva que considera que las medidas precautorias limitarán la innovación socavando el crecimiento económico, la ventaja competitiva y el progreso social, ver Castro y McLaughlin (2019). Ellos señalan como efectos negativos del principio precautorio en la IA: 1. desarrollo más lento y costoso de la IA, 2. disminución de la innovación, 3. IA de menor calidad, 4. menos adopción de la IA, 5. menor crecimiento económico, 6. merma de las opciones para los consumidores, 7. precios más altos, 8. experiencias inferiores para los consumidores, 9. menos impactos sociales positivos, y 10. disminución de la competitividad económica y de la seguridad nacional.

por otro, a la luz y conforme los valores de los Estados constitucionales –ver el último párrafo de este capítulo–. La función precautoria de la responsabilidad civil fue creada para proteger al medio ambiente. Ella surge de modo claro del principio 15 contenido en la Declaración de Río sobre el Medio Ambiente y el Desarrollo, de 1992.<sup>62</sup> Por otra parte, en relación con las características exigidas del daño para que se aplique la función precautoria, asertamos que grave e irreversible son palabras que padecen de textura abierta –ver Hart (1994)–, por ello, el centro algorítmico –en virtud de su equipo interdisciplinario y de la experiencia que adquirirá en el seguimiento de toda la evolución de los RSA– podría cumplir un rol importante en la determinación de esas características del perjuicio. La cuestión principal se centra, así, en relación con el nexo causal, de modo que se debería probar para su procedencia al menos un escenario de ocurrencia de un daño grave e irreversible de los RSA. A su vez, la dimensión colectiva de la protección de datos adquiere especial relevancia en el contexto de las ciudades inteligentes,<sup>63</sup> ya que, además de incidir en el derecho a la intimidad, aumenta el riesgo de sesgos discriminatorios en los sistemas de toma de decisiones algorítmicas, como lo señalamos en el párrafo previo, especialmente en las aplicaciones de policía predictiva y de reconocimiento facial contra minorías y grupos vulnerables. En este contexto, deben aplicarse los principios de transparencia y de precaución en materia de protección de datos personales para determinar la necesidad de una mayor prevención de los daños, exigiendo informes de impacto para proteger los datos o incluso prohibiendo el uso de determinadas tecnologías (BELLI y DONEDA, 2021, p. 68); medidas que serían analizadas por el centro algorítmico según el esquema propuesto en este trabajo. Asimismo, en algunos casos, la función precautoria de la responsabilidad civil ante los posibles daños causados por los RSA resulta aplicable a los sistemas de apoyo a la toma de decisiones clínicas (SADC), que son “sistemas de conocimiento activo que utilizan dos o más datos del paciente para generar consejos específicos para cada caso”

<sup>62</sup> Ver también: la Carta del medio ambiente de Francia, la ley 25.675 de Argentina, la ley 28.611 de Perú; la ley 7788/98 de Costa Rica; la ley 99 de Colombia.

Sobre un análisis de la función precautoria en la responsabilidad civil por daños al ambiente, ver Lorenzetti (2008).

<sup>63</sup> Una ciudad inteligente y sostenible es una ciudad innovadora que utiliza las tecnologías de información y comunicación y otros medios para mejorar la calidad de vida, la eficiencia del funcionamiento y los servicios urbanos y la competitividad, al tiempo que garantiza la satisfacción de las necesidades de las generaciones presentes y futuras en lo que respecta a los aspectos económicos, sociales y medioambientales (COMMITTED TO CONNECTING THE WORLD, 2021). En otras palabras, las ciudades inteligentes son aquellas que usan la data de modo coherente para la formación de sistemas digitales con un pensamiento a largo plazo que fomente el desarrollo sustentable: económico, social y ambiental.

Sobre el análisis de Barcelona y Lyon como ejemplos considerados exitosos de experimentos de gobernanza para las ciudades inteligentes, ver Belli y Doneda (2021).

(WYATT y SPIEGELHALTER, 1991). Los SADC, por ejemplo, proporcionan a los médicos: alertas o recordatorios, destacan las directrices durante la atención, ofrecen sugerencias de actuación e identifican la interacción entre medicamentos. Muchos de los principales riesgos del SADC parecen difíciles de reducir a los procedimientos habituales de evaluación de riesgos en base a que ellos difieren con relación al tipo de SADC y a su entorno de uso. La incertidumbre científica que rodea a los riesgos provenientes del uso de los SADC es en parte consecuencia de la complejidad en múltiples aspectos. Así, la función precautoria resulta aplicable a los SADC, pero solo en función de cada caso: por ejemplo, dependiendo del tipo de SADC (especialmente aquellos basados en datos), de la naturaleza de la decisión (por ejemplo, sobre salud pública o enfermedades transmisibles), del tipo de datos (verbigracia, datos biométricos), de la forma en que contribuyen a la toma de decisiones (por ejemplo, de modo automático)<sup>64</sup> y del lugar que ocupan los SADC en un entorno sanitario concreto (verbigracia, cuando están entrelazados con una gran variedad de procesos en un hospital). Por consiguiente, la función precautoria de la responsabilidad civil sería aplicable ya que los SADC, en el caso de RSA que se implementen a gran escala en el sistema sanitario, podrían acarrear daños graves e irreversibles, tanto a la salud individual como a la salud pública y a los derechos humanos<sup>65</sup> (SIKMA *et al.*, 2020).

Por otra parte, resaltamos la importancia de la adopción de otras medidas técnicas idóneas (*ex ante*) con el fin de disminuir la probabilidad de causación de daños por fuera del sistema de las funciones preventiva y precautoria de la responsabilidad civil, en el caso, por ejemplo: de RSA de riesgo inaceptable y de alto riesgo. De aquí que la Propuesta de ley sobre IA de la UE gradúa la sanción entre la prohibición para los RSA de riesgo inaceptable y para los RSA de alto riesgo dispone que: deben aplicarse requisitos en lo que respecta a la calidad de los conjuntos de datos usados, la documentación técnica y el mantenimiento de registros, la transparencia y el suministro de información a los usuarios, la supervisión humana y la solidez, la precisión y la ciberseguridad. Asimismo, destacamos las siguientes medidas *ex ante* con relación a cualquier clase de RSA para prevenir los daños causados por ellos. 1. La certificación y el control adecuado del funcionamiento de los RSA, que también serán realizados por el centro algorítmico; ello garantizará la trazabilidad de los resultados. Así, por ejemplo, el *White paper On Artificial Intelligence – An European approach to excellence and*

<sup>64</sup> Ver Mazur (2019).

<sup>65</sup> Gran parte de los riesgos más graves de los SADC están relacionados con la violación de los derechos humanos, como: la autonomía, la igualdad de acceso a la asistencia sanitaria y la privacidad. El Tribunal Europeo de Derechos Humanos ha reconocido el principio de precaución en relación con los derechos humanos. EHRM. 27 januari 2009, ECLI:EC:ECHR:2009:0127JUD006702101 (Tatar/Roemenië).

*trust*, del 19.02.2020 propone para los RSA de bajo riesgo un régimen de etiquetado voluntario, con la opción de vincularse a requisitos legales o similares especialmente creados en este ámbito. Esto sería una condición para recibir un sello de calidad para los RSA, confirmando que una determinada empresa cumpliría con ciertas normas objetivas (CANTARINI, 2021). En esa línea, la Comisión Nacional de Protección de Datos de Luxemburgo (CNPD) adoptó, el 13 de mayo de 2022, el primer mecanismo de certificación a nivel nacional e internacional en el marco del RGPD. En particular, la CNPD destacó que ahora las empresas, las autoridades públicas, las asociaciones y otras organizaciones establecidas en Luxemburgo tienen la posibilidad de demostrar que sus actividades de tratamiento de datos cumplen con el RGPD.<sup>66</sup> 2. Por otra parte, el artículo 63 del RGPD otorga al interesado el derecho a conocer y recibir comunicaciones sobre la lógica que subyace a cualquier tratamiento de datos en relación con la toma de decisiones automatizada.<sup>67</sup> Ese artículo del RGPD se integra al artículo 22 del RGPD, que regula la toma de decisiones automatizadas, así como al considerando 71 del RGPD, que recoge la explicación como una de las garantías en caso de tales decisiones. Esto otorga potencialmente al interesado el derecho a una explicación de la tecnología. En consecuencia, ello podría aumentar: el conocimiento de los riesgos de daños causados por los RSA y –de ese modo– la disminución de esos perjuicios; por ejemplo, para prevenir la discriminación. Como vimos en la nota 31, el RGPD no prevé el derecho a la explicación para todas las decisiones algorítmicas, sino solo para las que tienen un efecto legal o significativo. Para todas las demás decisiones algorítmicas, el interesado puede ejercer otros derechos previstos en el RGPD, como el derecho a la información o el derecho de acceso. El régimen jurídico de la UE limita el derecho a la explicación únicamente a las decisiones basadas en datos personales; por tanto, las decisiones basadas exclusivamente en datos no personales quedan en una laguna normativa. Sin embargo, en determinadas circunstancias, las decisiones basadas en datos no personales también pueden producir un efecto jurídico o similar significativo sobre el interesado; por consiguiente, requerirían igualmente una explicación (BRKAN y BONNET, 2020), como es el caso de la práctica de Uber mencionada en el capítulo IV. Asimismo, la comprensión de las razones que subyacen a una decisión algorítmica también puede verse obstaculizada por los límites jurídicos, por ejemplo: los secretos comerciales u otra información confidencial (BRKAN y BONNET, 2020). Los siguientes son algunos de los más conocidos secretos

<sup>66</sup> Ver <https://www.dataguidance.com/news/luxembourg-cnpd-adopts-first-ever-gdpr-certification>.

<sup>67</sup> Sobre las leyes nacionales aprobadas en los Estados miembros de la UE que han aplicado el RGPD en el ámbito de la toma de decisiones automatizada (prohibición, excepciones, salvaguardias), ver Malgieri (2019).

comerciales: el sistema de recomendación de Amazon, el algoritmo de difusión de publicaciones de Instagram o los algoritmos de búsqueda de Google –sobre estos últimos, ver Noto La Diega (2018)–.<sup>68</sup> 3. A su vez, la información adecuada de los riesgos de causación de daños del RSA entre los sujetos pasibles de ser responsables civilmente también aminoran la producción de esos perjuicios. Por ejemplo, en una decisión reciente relacionada con un RSA quirúrgico, *Taylor v. Intuitive Surgical*, 389 P.3d 517 (2017), la Suprema Corte de Washington decidió sobre la responsabilidad del cirujano –es decir, el operador– o del fabricante por el uso del RSA y sobre la obligación de información del fabricante. El tribunal sostuvo que los fabricantes de dispositivos médicos tienen el deber de informar a los hospitales y a los operadores de los sistemas de los riesgos del RSA quirúrgico.

4. Asimismo, podría resultar un medio para la prevención de los daños la creación de un Registro abierto de IA análogo al creado en Amsterdam y en Helsinki, que sirven para que la ciudadanía pueda proporcionar sus comentarios sobre los servicios ofrecidos mediante esta tecnología o participar en investigaciones. El objetivo de estos registros es garantizar que la IA empleada en los servicios públicos funcione en cumplimiento con los principios de responsabilidad, transparencia y seguridad, hacia un desarrollo digital abierto y compartido. De aquí que un aspecto valioso del funcionamiento de dicho Registro consiste en concientizar sobre el uso normal, común y de utilidad de los RSA<sup>69</sup> en entornos urbanos y en la automatización de las ciudades, y mostrar como nuestro mundo depende cada vez más de las soluciones digitales (FLORIDI, 2020). Esto constituirá un aporte para la prevención de los daños en virtud de un uso más seguro y eficiente de los RSA por parte de los ciudadanos. El registro de Helsinki permite el intercambio de opiniones, sugerencias y la posibilidad de participar en investigaciones a través del uso de *chatbots*.<sup>70</sup> A su vez, el registro de Amsterdam,

<sup>68</sup> Un código fuente es una implementación particular de un algoritmo en un lenguaje de programación concreto (verbigracia: Python, Java, etc.), mientras que un algoritmo es un procedimiento definible y fiable para resolver un problema, ver Chabert ed. (1999); a su vez, el software son las instrucciones que indican a un ordenador lo que debe hacer; el software comprende todo el conjunto de programas, procedimientos y rutinas asociados al funcionamiento de un sistema informático (BRITANNICA). Por consiguiente, un software y un código fuente pueden ser objeto de derechos de autor, pero no un algoritmo que no es más que una idea abstracta que sustenta el programa informático y el código fuente. Sin embargo, los algoritmos pueden encuadrar en la definición de secretos comerciales –aquellos que tienen valor comercial en virtud de su carácter secreto y son mantenidos en ese estado por medidas razonables del titular de la información, como los conocimientos técnicos no divulgados y la información comercial (ver Directiva, UE 2016/943)– como lo demuestra su reconocimiento jurisprudencial (BRKAN y BONNET, 2020).

<sup>69</sup> Ver capítulo IV.

<sup>70</sup> Los casos de uso de IA como parte de los servicios urbanos de Helsinki son: el *chatbot* de estacionamiento, el servicio de recomendación de libros, el sistema inteligente de gestión de materiales, el *chatbot* de clínica de maternidad y el *chatbot* de búsqueda de apartamentos de alquiler, ver <https://ai.hel.fi/en/ai-register/>.

usa RSA como parte de sus servicios urbanos sobre: control de estacionamiento automatizado, problemas de denuncia en el espacio público y riesgo de alquiler ilegal de viviendas para vacaciones.<sup>71</sup> Estos registros no están completamente optimizados; no obstante, ambos están en plena expansión. Ambos registros son fruto de una asociación privada y pública ya que el proyecto se ejecuta con la empresa finlandesa Saidot. 5. Por otra parte, según Infantino sería sensato complementar las funciones de la responsabilidad civil con directrices de *soft law*, códigos de conducta, estándares, mejores prácticas y declaraciones de impacto humano destinadas a orientar *ex ante* la conducta de los diseñadores, promotores, propietarios y usuarios de los RSA, para prevenir que se produzcan daños (2019).<sup>72</sup> 6. Asimismo, resulta oportuno destacar un ejemplo de como la integración de herramientas tecnológicas puede resultar adecuado para la prevención de los daños causados por la robótica. La robótica de enjambres estudia la optimización de los caminos computacionales para que los RSA puedan intercambiar información entre sí y actuar en conjunto, conforme un objetivo común para el que fueron programados. Por ejemplo, uno de los mayores experimentos en robótica de enjambres se realizó en el Instituto Wyss de Ingeniería de Inspección Biológica de la Universidad Harvard y fue publicado en el año 2014.<sup>73</sup> Los enjambres artificiales de RSA pueden usarse en misiones de búsqueda y rescate, en la construcción, en la recuperación del medio ambiente y en las aplicaciones médicas, etc. Por ejemplo, las Fuerzas de Defensa de Israel usaron enjambres de drones contra los grupos Hamas y Jihad Islámica durante la operación sobre la Franja de Gaza de mayo de 2021. Esta se considera una de las primeras misiones de ese tipo en el mundo.<sup>74</sup> El logro del consenso es una capacidad crucial para los enjambres de RSA, por ejemplo, para la selección de rutas, la agregación espacial o la detección colectiva. Ahora bien, la presencia de RSA que funcionan mal (RSA bizantinos) puede hacer imposible lograr el consenso utilizando los protocolos de consenso clásicos. En una investigación reciente, científicos demostraron como un enjambre de RSA puede lograr el consenso a través de contratos inteligentes basados en *blockchain* que sirven como *metacontroladores*, incluso en presencia de RSA bizantinos. Así, por ejemplo, la tecnología de cadena de bloques puede evitar que los ataques sibilinos –falsifican un gran número de identidades– perturben el comportamiento del enjambre, introduciendo la escasez en sistemas descentralizados: así, un RSA que quiera ejercer influencia debe pagar por ello

<sup>71</sup> Ver <https://algoritmeregister.amsterdam.nl/en/ai-register/>.

<sup>72</sup> Ver Montagnani y Cavallo (2021).

<sup>73</sup> Ver Rubenstein *et al.* (2014).

<sup>74</sup> Ver <https://www.israeleconomico.com/defensa/fuerzas-de-defensa-de-israel-usaron-enjambres-de-drones-contra-hamas-en-gaza/>.

gastando un recurso escaso (*criptotokens*) (STROBEL *et al.*, 2020). 7. Finalmente, la teoría de juegos<sup>75</sup> puede facilitar la cooperación<sup>76</sup> humano-robot, como un paso necesario para la evolución del Derecho en la era digital. Li *et al.* (2019) publicaron una investigación reciente que desarrolló un controlador de robot interactivo capaz de entender la estrategia de control del usuario humano y reaccionar de forma óptima a sus movimientos. A su vez, ellos demostraron que la combinación de un observador con un controlador de teoría de juegos diferencial puede inducir una interacción estable entre los dos socios, identificar con precisión la ley de control del otro y permitirles realizar con éxito la tarea con el mínimo esfuerzo. Por consiguiente, el uso de la teoría de juegos opera como una herramienta auxiliar para que la toma de decisión del RSA sea compatible con los intereses de los sujetos con los que interacciona disminuyendo el riesgo de daños. Así, dicha investigación demostró de modo indirecto que la teoría de juegos es útil para la prevención de los daños. Asimismo, ese estudio constituye un avance en la solución al problema de la alineación, es decir, de cómo alinear los objetivos o valores de los humanos con los resultados de lo que hará la IA.<sup>77</sup> Esto se relaciona con la estructura de la estrategia, que consiste en la alineación de los medios y los fines;<sup>78</sup> de ese modo, el aspecto trascendente del problema de control radica en el modo de diseño estratégico del sistema para que este funcione respetando la decisión humana.<sup>79</sup>

En relación con la prevención c), como vimos, ella funcionaría para los daños previsibles causados por los RSA aunque ella quedaría condicionada por la contratación del seguro obligatorio mencionado en el capítulo IV. Por último, en lo tocante a la prevención d), la vigencia de los *punitive damages*—cuya característica más destacada es que tienen por finalidad no la reparación del daño causado a la víctima, sino el castigo al autor de un comportamiento particularmente grave, y la consiguiente prevención, a fin de evitar que se reitere el comportamiento indeseado (FELDTHUSEN, 1990)—, que no sean pasibles de póliza de cobertura, operarían como un contrapeso de los condicionantes mencionados con el objetivo de disuadir a los empresarios a la adopción de medidas preventivas que disminuyan el riesgo de daños causados por los RSA en un marco de tutela de los terceros.

<sup>75</sup> Ver: Neumann y Morgenstern (1953), Paenza (2007) y Mascitti (2012).

<sup>76</sup> Ver capítulo 1.

<sup>77</sup> En ese sentido, Mantelero dice que las cuestiones relativas a la nueva era de las máquinas involucran al papel del diseñador y de los usuarios, que pueden configurar —de modo: aislado o conjunto— los valores incorporados a la máquina y transmitidos a través de la tecnología (2022, p. 102).

<sup>78</sup> Ver Lewis Gaddis (2019).

<sup>79</sup> Ver Russell (2019).

En definitiva, los cuatro modos de prevención descriptos –a), b), c) y d)– consisten en tácticas dentro de la estrategia de garantía de protección de los derechos humanos –que son el fundamento del Derecho de los Estados constitucionales– que se ven reflejados en el subsistema de la responsabilidad civil a raíz de la constitucionalización del Derecho civil –el artículo 1 del CCCA es un ejemplo de ello–.<sup>80</sup> La idea de garantizar los derechos de los ciudadanos ha jugado un rol incontestable dentro del Derecho de la responsabilidad civil que constituye ciertamente una de sus funciones (TUNC, 1981).<sup>81</sup> Los derechos humanos consisten –a su vez– junto al *rule of law* y a la democracia, los pilares de la política<sup>82</sup> cuyo fin es la consecución del bien común,<sup>83</sup> que asimismo constituye un elemento del principio supremo de justicia –valor absoluto del Derecho– junto a: la libertad, la igualdad, la fraternidad, la dignidad y el medio ambiente. Por ello, el principio supremo de justicia es aquel que exige adjudicar a cada individuo la (a) esfera de libertad necesaria para su personalización teniendo en cuenta: la (b) igualdad de ellos –garantizándola por medio de acciones afirmativas y/o de abstenciones–, (c) la dignidad de todos los individuos y (d) la fraternidad en un marco de (e) protección ambiental para construir el (f) bien común (MASCITTI, 2022a).<sup>84</sup> El principio supremo de justicia nos permite iluminar las notas actuales y necesarias del valor justicia en los casos difíciles en el Derecho de los Estados constitucionales mediante la ponderación de los valores que surgen de dicho principio. Coincidimos con Sen en cuanto a que “los debates sobre la justicia, si van a ocuparse de asuntos prácticos, no pueden ser sino sobre comparaciones” (2012).<sup>85</sup> El enfoque interaccionista de la razón<sup>86</sup> predice que las personas deberían de ser hábiles evaluando las razones de los demás, rechazando las débiles y cambiando de opinión cuando las razones son suficientemente buenas (MERCIER y SPERBER, 2017, p. 273). Por ello, la valoración de la justicia se fue produciendo en los casos concretos; fortalecida por la dialéctica del proceso,

<sup>80</sup> El fenómeno de positivización de los derechos humanos en el Derecho internacional, como reaseguro de sus positivizaciones nacionales, es lo que hizo perder buena parte del sentido práctico al clásico debate entre iusnaturalismo y iuspositivismo. CSJN, Fallos: 328:2056 (14/06/2005).

<sup>81</sup> En ese sentido, Alpa dice que “las normas del Código concernientes a la responsabilidad civil, interpretadas e integradas en un sistema racional de indemnización, operan como una ‘función de garantía’, es decir, en resguardo del individuo de la acción de terceros, de las lesiones que devienen del ejercicio de las actividades de otro” (1986).

<sup>82</sup> Ver Waldron (2008).

<sup>83</sup> Ver Bobbio (2003, p. 242).

<sup>84</sup> Los elementos del principio supremo de justicia están contenidos en los principios de la declaración de Asilomar sobre IA, así, por ejemplo: libertad (13), igualdad (14 y 15), dignidad (11), la fraternidad reflejada por la cooperación (4 y 5) medio ambiente (14, 17, 20, 21) y bien común (23). Ver <https://futureoflife.org/ai-principles/>.

<sup>85</sup> Ver Mascitti (2022b).

<sup>86</sup> Ver capítulo I.

donde se intercambian ideas que luego son analizadas por los jueces previo a su toma de decisión racional. Así, el estratega deberá balancear esos elementos del principio supremo de justicia para la selección de alguno de ellos como medio para *dar a cada uno lo suyo* en los casos difíciles donde deba dirimirse sobre la procedencia del ejercicio de la función de la prevención de daños causados por los RSA. Precisamente, la función de prevención de daños protege todos los elementos del principio supremo de justicia. Veamos. Los daños a prevenir causados por los RSA podrían afectar a: i. la libertad, que –precisamente– constituye el fundamento de la función de prevención de daños, es decir ella deriva de la tutela de la esfera de la libertad de la persona que se ve reflejada en el principio *alterum non laedere*, o sea, se trata de no dañar pero también de evitar que los daños se produzcan;<sup>87</sup> ii. la igualdad ya que ella significa la contracara de la discriminación –como vimos en el desarrollo de la prevención de daños a)–; iii. la fraternidad como hermandad (que refuerza a la solidaridad, principio en que se sustenta el sistema de responsabilidad civil moderno),<sup>88</sup> también a través de los sesgos algorítmicos; iv. la dignidad (por ejemplo a través del uso de la neurotecnología que podría afectar a los siguientes neuroderechos: el derecho a la intimidad mental; el derecho a la agencia; y el derecho a la identidad; ello podría ser clasificado como un riesgo inaceptable, como vimos en el capítulo II), que calificamos como el valor no derrotable<sup>89</sup> en la ponderación de principios constitucionales en el caso concreto; v. el medio ambiente (cuya protección preventiva destacan la mayoría de los Derechos de los Estados constitucionales –ver por ej. arts.: 41 de la Constitución nacional argentina, 45 de la Constitución nacional española y 80 de la Constitución nacional colombiana–)<sup>90</sup> a través de un RSA que tome decisiones basado en un algoritmo que refleje una asignación de valuación de principios que lo vulnere de modo ilegítimo procurando una obtención desmedida de utilidad; y vi. el bien común, cuya tutela preventiva debe constituir una de las finalidades principales de la investigación y del desarrollo de los RSA. En ese sentido, Bostrom afirma que el problema político en la investigación de la IA se refiere al desafío de cómo lograr una situación en la que los individuos o

<sup>87</sup> Una sentencia del Consejo Constitucional francés del 22-10-1982 declaró: “Tiene carácter constitucional el art. 1382 del Código Civil (similar a nuestro art. 1109, Cód. Civ.) porque no teniendo nadie el derecho de dañar a otro, el que lo hace tiene obligación de reparar”.

<sup>88</sup> Por ello, la aparición del seguro, de la seguridad social y de los regímenes de garantía estatal, indican la evolución de la responsabilidad civil a otra forma de reparación colectiva o de socialización de los daños (MESSINA de ESTRELLA GUTIÉRREZ, 2015).

<sup>89</sup> Ver Gomá Lanzón (2019).

<sup>90</sup> En la UE, el proyecto AI4Cities, financiado por el programa de investigación e innovación Horizonte 2020 de la UE, vincula a seis ciudades y regiones europeas que buscan soluciones de IA en materia de movilidad y energía para acelerar la neutralidad del carbono. El enfoque puede ser arriesgado, si no conduce a la cooperación, porque hay retos sistémicos y globales (FLORIDI, 2020). Ver <https://ai4cities.eu/>.

las instituciones facultados por dicha IA la usen de modo que promueva el bien común (2017).

## VI Conclusión

El ser humano es un *homo prospectus* por su capacidad de imaginar el futuro. Si la construcción de la cultura es la forma humana de resolver los problemas biológicos básicos de la supervivencia y la reproducción, entonces la prospección benefició a los humanos al fortalecer la cultura. La existencia real del futuro se basa en los entendimientos compartidos del grupo social; en cierto sentido, el futuro es un producto de la imaginación y el acuerdo colectivos; la cooperación puede impulsar marcos temporales aun más largos (BAUMEISTER, 2016). Precisamente, el Derecho –que es un objeto cultural– no se habría inventado sin la idea de futuro;<sup>91</sup> por tanto, el Derecho es prospectivo. En cambio, las decisiones algorítmicas suelen *codificar* el pasado, capturando soluciones y predicciones en esquemas procedentes de acontecimientos históricos y de valores que han dirigido la programación del algoritmo en que se apoya el proceso decisorio (BATTELLI, 2021); esto significa que los algoritmos –pilares de los RSA– *congelan* el futuro (HILDEBRANDT, 2020b). Asimismo, en la medida de lo posible, el Derecho debe promover la cooperación. Dentro del subsistema de la responsabilidad civil, el Derecho debe ampliar el horizonte temporal de su accionar fijando sanciones como incentivos a la cooperación, cuyo resultado sea una mayor prevención de los daños previsibles acaecidos en la complejidad de la era digital. Sin embargo, la función preventiva de la responsabilidad civil es insuficiente en virtud de la imprevisibilidad generada por el funcionamiento de los RSA basado en las correlaciones mencionadas. Ello requiere la actuación con mayor anticipación del Derecho con el objetivo de mantener la paz social, la armonía y la solidaridad. A tal efecto, en el capítulo V, propusimos: la adopción de la función precautoria y la vigencia de medidas *ex ante* en los casos de los RSA de riesgo inaceptable (prohibición) y de alto riesgo (mantenimiento de: registros, supervisión humana y solidez, transparencia y suministro de información a los usuarios, precisión y ciberseguridad) y en los supuestos de toda clase de RSA (certificación, información sobre la lógica de las decisiones automatizadas, comunicación entre los posibles responsables por daños causados por uso de los RSA, Registro abierto de IA, códigos de conducta, integración de tecnologías, diseño algorítmico para la cooperación hombre-máquina) y la creación de un centro algorítmico de carácter

---

<sup>91</sup> Ver Mascitti (2020a).

público-privado. En consecuencia, a modo de respuesta a la pregunta formulada en la introducción, afirmamos que el sistema actual de responsabilidad civil de los Estados constitucionales resulta insuficiente para la prevención de los daños causados por los RSA. Por consiguiente, pensamos que las ideas vertidas en el trabajo pueden resultar adecuadas para una mejor prevención de los daños causados por los RSA, dentro de un marco de fertilización cruzada de diversas disciplinas científicas. Ello, podría servir como base para la elaboración de una normativa impactante, es decir, que goce de la capacidad de cambiar el resto de la realidad<sup>92</sup> y sea afín al principio supremo de justicia,<sup>93</sup> fortaleciendo –de ese modo– la construcción de un Derecho humanista.

### The preventive function of damage caused by robotics and autonomous systems

**Abstract:** It is a contribution to the progress of Tort law in this digital era through the development of the preventive function of damage caused by robotics and autonomous systems (RAS). A detailed analysis of their functioning – with the help of the interdisciplinary approach – makes it possible to reduce the foreseeable occurrence of damage. However, the precautionary function and various ex-ante measures – not contained in this preventive function – are necessary to reduce the risk of damage caused by RASs due to the unpredictability of their actions in some cases. Therefore, the determination of the preventive function becomes an essential issue for: the understanding of contemporary legal developments and the progress of tort law, recognising the factual complexity of the digital era and the various values at stake that require an effective protection of users by encouraging the appropriate development of technological innovation.

**Keywords:** Progress. Tort law. Preventive function. Precaution. Digital era. AI. Robotics and autonomous systems. Interdisciplinary approach.

**Summary:** I Introduction – II Robotics and autonomous systems (RAS) as elements of the complexity of the digital era – III RAS as risky products – IV The interdisciplinary contribution to the construction of the preventive function of damage caused by RAS – V The plot of the Civil liability functions as a support for the damage prevention – VI Conclusion – References

### A função preventiva dos danos causados pela robótica e sistemas autónomos

**Resumo:** É uma contribuição para o progresso do Direito da responsabilidade civil nesta era digital através do desenvolvimento da função preventiva dos danos causados pela robótica e sistemas autónomos (RSA). Uma análise detalhada do seu funcionamento – com a ajuda da abordagem interdisciplinar – torna possível reduzir a ocorrência previsível de danos. Contudo, a função preventiva e várias medidas *ex-ante* – não contidas nesta função preventiva – são necessárias para reduzir o risco de danos causados pelos RSA devido à imprevisibilidade das suas acções em alguns casos. Portanto, a determinação da função preventiva torna-se uma questão essencial para: a compreensão da evolução jurídica contemporânea e o progresso do Direito da responsabilidade civil, reconhecendo a complexidade factual da era digital e os vários valores em jogo que exigem uma protecção eficaz dos usuários, promovendo o desenvolvimento adequado da inovação tecnológica.

<sup>92</sup> Ver Mascitti (2020b).

<sup>93</sup> La reparación, aunque sea su intención, nunca es tan justa que vuelva las cosas a su estado anterior (MOSSET ITURRASPE, 2008).

**Palavras-chave:** Progresso. Direito da responsabilidade civil. Função preventiva. Precaução. Era digital. IA. Robótica e sistemas autônomos. Abordagem interdisciplinar.

**Sumário:** I Introdução – II RSA como elementos da complexidade da era digital – III RSA como produtos de risco – IV A contribuição interdisciplinar para a construção da função de prevenção dos danos causados pelo RSA – V A trama das funções da responsabilidade civil como base para a prevenção de danos – VI Conclusão – Referências

## Referencias

ACCIARI, Hugo. Funciones del Derecho de daños y de prevención. Buenos Aires: *Revista La Ley*, 2013.

ALPA, Guido. La responsabilité civile en Italie: problèmes et perspectives. *Revue Internationale de Droit Comparé*. Año 39. Nro. 4, 1986.

ALPA, Guido. *Trattato di diritto civile*. T. IV. Milano: Giuffré, 1999.

ANDORNO, Roberto. El principio de precaución: un nuevo standard jurídico para la era tecnológica. Buenos Aires: *La Ley*, 2002.

ANDORNO, Roberto. The Precautionary Principle: A New Legal Standard for a Technological Age. *Journal of International Biotechnology Law* 1(1):11-19, 2004. DOI: 10.1515/jibl.2004.1.1.11.

BARFIELD, Woodrow. *Liability for autonomous and artificially intelligent robots*. 2018. Disponible en: <https://www.degruyter.com/downloadpdf/j/pjbr.2018.9.issue-1/pjbr-2018-0018/pjbr-2018-0018.pdf>. Acceso en: 8 de febrero 2022.

BARRIO ANDRÉS, Moisés. *Robótica, inteligencia artificial y Derecho*. 2018. Disponible en: <http://www.realinstitutoelcano.org/wps/wcm/connect/b7a72224-1d79-4649-8c51-bc0419e40cd4/ARI103-2018-BarrioAndres-Robotica-inteligencia-artificialderecho.pdf?MOD=AJPERES&CACHEID=b7a7224-1d79-4649-8c51-bc0419e40cd4>. Acceso en: 8 de febrero 2022.

BARROS VALE, Sebastião; ZANFIR-FORTUNA, Gabriela. Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities. *Future of Privacy forum*, 2022.

BATTELLI, Ettore. La decisión robótica: algoritmos, interpretación y justicia predictiva. *Revista de Derecho Privado*, N° 40, 2021. DOI: 10.18601/01234366.n40.03.

BAUMEISTER, Roy. Collective Prospection: The Social Construction of the Future. En: SELIGMAN, Martin E.; RAILTON, Peter; BAUMEISTER, Roy F.; SRIPADA, Chandra. *Homo prospectus*. Oxford University Press, 2016.

BELLI, Luca; DONEDA, Danilo. Governança de dados nas “cidades inteligentes”: ensinamentos aprendidos das práticas brasileiras e europeias, en *Smart Cities no Brasil: regulação, tecnologia e direitos*/André Ramiro... [et al.]; organizado por Jess Reia, Luca Belli. Belo Horizonte, MG: Casa do Direito, 2021.

BERTOLINI, Andrea. The legal issues of robotics. *Robohub*, 2017. Disponible en: <http://robohub.org/the-legal-issues-of-robotics/>. Acceso en: 8 de febrero 2022.

BERTOLINI, Andrea; EPISCOPO, Francesca. Robots and AI as Legal Subjects? Disentangling the Ontological and Functional Perspective. *Front. Robot. AI*, 2022. Disponible en: <https://doi.org/10.3389/robt.2022.842213>.

BRKAN, Maja; BONNET, Grégory. Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: Of Black Boxes, White Boxes and Fata Morganas. *European Journal of Risk Regulation*, 11(1), 2020. DOI: 10.1017/err.2020.10.

- BOBBIO, Norberto. *Teoría General de la Política*. Madrid: Trotta, 2003.
- BOSTROM, Nick. Strategic implications of openness in AI development. *Global policy* 5, 2017.
- BROWNSWORD, Roger. *Rethinking Law, Regulation, and Technology*. Edward Elgar Publishing, 2022.
- BRYNJOLFSSON, Erik; ROCK, Daniel; SYVERSON, Chad. Artificial intelligence and the modern productivity paradox: a clash of expectations and statistics. *National Bureau for Economic Research*, 2007.
- CALABRESI, Guido. Does the Fault System Optimally Control Primary Accident Costs? *Law and Contemporary Problems* 33, 1968.
- CALABRESI, Guido. A Broader View of the Cathedral: The Significance of the Liability Rule, Correcting a Misapprehension. *Law and Contemporary Problems*, 1-13, 2014.
- CALABRESI, Guido; MELAMED, Douglas. Property rules, liability rules, and inalienability: one view of the cathedral. *Harvard Law Review* 85, 1972.
- CANTARINI, Paola. Artificial intelligence: regulatory challenges and Riskification. *Revista Jurídica Unicuritiba*. Curitiba. V. 05. Nro. 67, 2021.
- CASTRO, Daniel; MCLAUGHLIN, Michael. Ten Ways the Precautionary Principle Undermines Progress in Artificial Intelligence. *ITIF*, 2019. Disponible en: <https://itif.org/publications/2019/02/04/ten-ways-precautionary-principle-undermines-progress-artificial-intelligence>. Acceso en: 18 de abril de 2022.
- CNIL, *Decisión nº MED 2021-134*, 2021a.
- CNIL, *Facial recognition: the CNIL orders CLEARVIEW AI to stop reusing photographs available on the Internet*, 2021b. Disponible en: <https://www.cnil.fr/en/facial-recognition-cnil-orders-clearview-ai-stop-reusing-photographs-available-internet>. Acceso en: 18 de abril de 2022.
- CHABERT, Jean L. (ed.). *A History of Algorithms. From the Pebble to the Microchip*. Springer, 1999.
- CHALMERS, David J. The singularity: A philosophical analysis. *Journal of Consciousness Studies* 17 (9-10), 2010.
- CHARISI, Vasiliki; COMPANO, Ramon; DUCH BROWN, Nestor; GOMEZ GUTIERREZ, Emilia; KLENERT, David; LUTZ Michael; MARSCHINSKI, Robert; TORRECILLA SALINAS, Carlos. What future for european robotics? A science for policy perspective, *JRC Virtual Conference*, 2021. Disponible en: <https://publications.jrc.ec.europa.eu/repository/bitstream/JRC125343/what-future-for-european-robotics.pdf>. Acceso en: 18 de abril de 2022.
- CHOI, Jin-A; LIM, Kiho. Identifying machine learning techniques for classification of target advertising. *ICT Express*, 6(3), 2020.
- CHURCHLAND, Patricia S. The Brains Behind Morality. *Cerebrum*, October, 2017.
- COMMITTED TO CONNECTING THE WORLD. *Focus Group on Smart Sustainable Cities*. Disponible en: <https://www.itu.int/en/ITU-T/focusgroups/ssc/Pages/default.aspx>. Acceso en: 30 abr. 2021.
- CONSEJO CONSTITUCIONAL DE FRANCIA, sentencia del 22-10-1982.
- CORNEJO PLAZA, María I. Neuroderechos y Neurotecnologías en Chile: prioridades legislativas. *El mostrador*, 2021. Recuperado el 21 de agosto de 2021. Disponible en: <https://www.elmostrador.cl/noticias/opinion/columnas/2021/07/26/neuroderechos-y-neurotecnologias-en-chile-prioridades-legislativas/>. Acceso en: 18 de abril de 2022.
- CORNEJO PLAZA, María I. Problema. Perspectiva neurocientífica de la agencia: ¿es problemática para el derecho? *Anuario de Filosofía y Teoría del Derecho* 16, México: UNAM, 2022.
- CORTE SUPREMA DE JUSTICIA DE LA NACIÓN ARGENTINA. Camacho Acosta vs. Grafi Graf. Fallo: 320:1633, 1997.

CORTE SUPREMA DE JUSTICIA DE LA NACIÓN ARGENTINA. Fallo: 328:2056, 2005.

CORTE SUPREMA DE JUSTICIA DE LA NACIÓN ARGENTINA. Halabi, Fallo: 332:111, 2009.

DANAHER, John. Robots, law and the retribution-gap. *Ethics and Information Technology*, 18(4), 2016.

DE ÁNGEL YÁGUEZ, Ricardo. *Algunas previsiones sobre el futuro de la responsabilidad civil* (con especial atención a la reparación del daño). Madrid: Cuadernos Civitas, 1995.

DICCIONARIO DE MATEMÁTICAS. *Superprof*. Disponible en: <https://www.superprof.es/diccionario/matematicas/calculo/variable-dependiente.html#:~:text=Qu%C3%A9%20significa%20variable%20dependiente%20en%20Matem%C3%A1ticas&text=Una%20variable%20dependiente%20es%20aquella,representa%20en%20el%20eje%20ordenadas>. Acceso en: 8 de febrero 2022.

DICKSON, Kelly; HINDS, Kate; BURCHETT, Helen; BRUNTON, Ginny; STANSFELD, Claire; THOMAS, James. No-fault compensation schemes: a rapid realist review. EPPI-Centre, *Social Science Research Unit*. UCL Institute of Education. London: University College London, 2016.

DÍEZ-PICAZO, Luis. *Derecho de daños*. Madrid: Civitas, 1999.

DWORKIN, Ronald. *Taking Rights Seriously*. Harvard University Press, 1977.

DWORKIN, Ronald. *Law's Empire*. Cambridge: The Belknap press of Harvard University Press, 1986.

ELMAN, Jeremy; CASTILLA, Abel. *Artificial intelligence and the law*, 2017. Disponible en: <https://techcrunch.com/2017/01/28/artificial-intelligence-and-the-law/>. Acceso en: 8 de febrero 2022.

EUROPEAN DATA PROTECTION BOARD (2022). *Guidelines 3/2022 on Dark patterns in social media platform interfaces*: How to recognise and avoid them. Available at: [https://edpb.europa.eu/our-worktools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media\\_en](https://edpb.europa.eu/our-worktools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en). Acceso en: 18 de abril de 2022.

FEDERAL DRUG ADMINISTRATION. FDA Permits Marketing of Artificial Intelligence-Based Device to Detect Certain Diabetes-Related Eye Problems. *News release*, 2018. Disponible en: <https://www.fda.gov/newsevents/newsroom/pressannouncements/ucm604357.htm>. Acceso en: 18 de abril de 2022.

FELDMAN BARRETT, Lisa. *How Emotions Are Made: The Secret Life of the Brain*. Mariner Books, 2017.

FELDTUSEN, Bruce. Recent developments in the Canadian law of punitive damages. *Rev. Can. De Droit de Commerce*. Vol. 16. Nro. 3, 1990.

FINNIS, John. *Natural law and natural rights*. Oxford: Clarendon Press, 1980.

FLORIDI, Luciano. Artificial Intelligence as a Public Service: Learning from Amsterdam and Helsinki. *Philos. Technol.* 33, 541–546, 2020. <https://doi.org/10.1007/s13347-020-00434-3>

FLORIDI Luciano; SANDERS Jeff W. On the morality of artificial agents. *Minds and Machines*, 2004.

FOSSA, Fabio. Artificial Moral Agents: Moral Mentors or Sensible Tools? *Ethics Inf. Technol.* 20, 2018. DOI: 10.1007/s10676-018-9451-y.

GALLI, Francesca. Law Enforcement and Data-Driven Predictions at the National and EU Level: A Challenge to the Presumption of Innocence and Reasonable Suspicion? in *Constitutional Challenges in the Algorithmic Society*. Edited by Hans-W. Micklitz, Oreste Pollicino, Amnon Reichman, Andrea Simoncini, Giovanni Sartor and Giovanni De Gregorio, Cambridge University Press, 2021, DOI: <https://doi.org/10.1017/9781108914857.003>.

GARRIDO CORDOBERA, Lidia M. R. La Responsabilidad por riesgo de desarrollo en materia de productos de consumo. En: *Responsabilidad Civil*. Ed. Rubinzal Culzoni, 2007.

GPDP. *Ordinanza ingiunzione nei confronti di Clearview AI – 2022* [9751362].

- GOETHALS, Sofie; MARTENS, David; EVGENIOU, Theodoros. The non-linear nature of the cost of comprehensibility. *J Big Data* 9, 30, 2022. <https://doi.org/10.1186/s40537-022-00579-2>.
- GOMÁ LANZÓN, Javier. *Dignidad*. Barcelona: Galaxia Gutenberg, [S.L.], 2019.
- GUASTINI, Riccardo. *Estudios de teoría constitucional*. 2ª ed. UNAM. México: Instituto de Investigaciones Jurídicas-Fontamara, 2003.
- GUERRA, Alice; PARISI, Francesco; PI, Daniel. Liability for robots II: An economic analysis. *Journal of Institutional Economics*, 2021. DOI: 10.1017/S1744137421000837.
- HART, Herbert L. A. *The concept of law*. 2ª edition. Oxford: Clarendon Press, 1994.
- HARTMANN, Ivar A.; FRANQUEIRA, Bruna D.; IUNES, Julia; ABBAS, Lorena; CURZI, Yasmin; VILLA, Beatriz; ABREU, Fernanda; DIAS, Renan. Regulação de Inteligência Artificial No Brasil. *FGV Direito Rio*, 2020. Available at: <https://hdl.handle.net/10438/30078>. Acceso en: 26 de enero de 2022.
- HILDEBRANDT, Mireille. *Smart Technologies and the End(s) of Law*. Novel Entanglements of Law and Technology. Cheltenham: Edward Elgar Publishing Limited, 2015.
- HILDEBRANDT, Mireille. *Law for Computer Scientists and Other Folk*. Kindle edition, 2020a.
- HILDEBRANDT, Mireille. Code-driven Law: Freezing the Future and Scaling the Past in *Critical Perspectives on Law and Artificial Intelligence*. Markou, Deakin, Hart Publishers, 2020b.
- HILDEBRANDT, Mireille. The Issue of Proxies and Choice Architectures. Why EU law matters for recommender systems. *SocArXiv*, 2021. DOI: 10.31235/osf.io/45x67.
- HIMMA, Kenneth E. Artificial agency, Consciousness, and the Criteria for Moral agency: what Properties Must an Artificial Agent Have to Be a Moral Agent? *Ethics Inf. Technol.* 11, 2009. DOI: 10.1007/s10676-008-9167-5.
- HODSON, Hal. DeepMind and Google: the battle to control artificial intelligence. *The economist*, 2019.
- HOWELL, Bronwyn; KAVANAGH, Judy; MARRIOTT, Lisa. No-fault public liability insurance: evidence from New Zealand. *Agenda* 9(2):135-149, 2002.
- INFANTINO, Marta. La responsabilità per danni algoritmici: propsetive europeo-continentali. *Responsabilità civile e previdenza* 1762, 2019.
- JOLLS, Christine; SUSTEIN, Cass; THALER, Richard. A Behavioral Approach to Law and Economics. Chicago: *Faculty Scholarship Series*, 1998.
- KAHNEMAN, Daniel. *Thinking, fast and slow*. Farrar, Straus and Giroux, 2011.
- KURZWEIL, Raymond. *The singularity is near*. New York: Penguin Books, 2005.
- LAMO, Madeline; CALO, Ryan. Regulating Bot Speech. *UCLA Law Review*, 2018.
- LEMLEY, Mark A.; CASEY, Bryan. Remedies for Robots. *Stanford Law and Economics*, 2019. Disponible en: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3223621](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3223621). Acceso en: 8 de febrero 2022.
- LEWIS GADDIS, John. *Grandes estrategias*. Trad. por Miguel Marqués Muñoz. Barcelona: Taurus. Kindle edition, 2019.
- LI, Zihao. Affinity-based algorithmic pricing: A dilemma for EU data protection law. *Computer Law & Security Review*, Volume 46, 2022. <https://doi.org/10.1016/j.clsr.2022.105705>.
- LI, Yanan; CARBONI, Gerolamo; GONZALEZ, Franck; CAMPOLO, Domenico; BURDET, Etienne. Differential game theory for versatile physical interaction. *Nature Machine Intelligence* 1 (01 2019), 2019. <https://doi.org/10.1038/s42256-018-0010-3>.

LIAO, Yu-ping; WHITE, Michelle J. No-Fault for Motor Vehicles: An Economic Analysis. 4 *AM. L. & ECON. Rev.* 258, 2002.

LORENZETTI, Ricardo L. *Teoría del Derecho ambiental*. México: Porrúa, 2008.

LUPIÁÑEZ-VILLANUEVA, Francisco; BOLUDA, Alba; BOGLIACINO, Francesco; LIVA, Giovanni; LECHARDOY, Lucie; RODRÍGUEZ DE LAS HERAS BALLELL, Teresa. *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation*. European Commission. Final Report, 2022.

MAGRANI, Eduardo. New perspectives on ethics and the laws of artificial intelligence. *Internet Policy Rev* 8(3):1-19, 2019.

MALGIERI, Gianclaudio. Automated decision-making in the EU Member States: The right to explanation and other 'suitable safeguards' in the national legislations. *Computer Law & Security Review*, Volume 35, Issue 5, 2019. <https://doi.org/10.1016/j.clsr.2019.05.002>.

MANTELERO, Alessandro. Beyond Data Human Rights, Ethical and Social Impact Assessment in *AI. Information Technology and Law Series*. Volume 36. Springer, 2022. Disponible en: <https://link.springer.com/content/pdf/10.1007/978-94-6265-531-7.pdf>. Acceso en: 9 de junio de 2022.

MANTELERO, Alessandro; ESPOSITO, Maria S. An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems. *Computer Law & Security Review*. Volume 41, 2021, <https://doi.org/10.1016/j.clsr.2021.105561>.

MAQUEO RAMÍREZ, María S. La responsabilidad civil extracontractual desde la perspectiva del análisis económico del derecho y la economía del comportamiento. *Revista IUS*, vol. 14, núm. 46, 2020.

MARCHISIO, Emiliano. In support of "no-fault" civil liability rules for artificial intelligence, *SN Soc Sci*, 2021. <https://doi.org/10.1007/s43545-020-00043-z>.

MARKOU, Christopher; DEAKIN, Simon. Ex Machina Lex: Exploring the Limits of Legal Computability. In: Simon Deakin and Christopher Markou (eds). *Is Law Computable? Critical Perspectives on Law + Artificial Intelligence*. Cambridge: Hart Publishing, 2020.

MARMOR, Andrei. *The Rule of Law and its Limits*. USC Public Policy Research, Los Angeles: University of Southern California Law School Los Angeles, 2016.

MASCITTI, Matías. Aportes para la integración de la matemática en el mundo jurídico. *Revista persona*, 2012. Disponible en: <http://www.ijeditores.com.ar/articulos.php?idarticulo=61499&print=1>. Acceso en: 18 de abril de 2022.

MASCITTI, Matías. Aporte trialista para el análisis jurídico de la economía. *Revista Temas Socio Jurídicos*. Vol. 36. Nro. 71. 2016b. DOI: <https://doi.org/10.29375/01208578.2640>.

MASCITTI, Matías. El azar como límite en el Derecho privado patrimonial. *Rivista JUS CIVILE*. Maggio-giugno. Torino: G. Giappichelli Editore, 2019. Disponible en: [http://www.juscivile.it/contributi/2019/02\\_Mascitti.pdf](http://www.juscivile.it/contributi/2019/02_Mascitti.pdf). Acceso en: 18 de abril de 2022.

MASCITTI, Matías. La función conjetural del Derecho reforzada por los algoritmos en la era de big data. *IUS ET SCIENTIA*. Universidad de Sevilla. 6 (2). 2020a. DOI: <https://doi.org/10.12795/IETSCIENTIA.2020.102.11>.

MASCITTI, Matías. Las interrelaciones entre el Derecho y la Genética desde la perspectiva integracionista de la Teoría trialista del mundo jurídico. *Revista Pensar en Derecho*. Nro. 17. UBA. 2020b. Disponible en: <http://www.derecho.uba.ar/publicaciones/pensar-en-derecho/revistas/17/las-interrelaciones-entre-el-derecho-y-la-genetica-desde-la-perspectiva-integracionista-de-la-teoria-trialista-del-mundo-juridico.pdf>. Acceso en: 18 de abril de 2022.

MASCITTI, Matías. El derecho del trabajo como un medio para atenuar el impacto de la vigilancia del trabajador, su manipulación y su discriminación en el ámbito laboral de la sociedad de la transparencia. *IUS ET SCIENTIA*, Universidad de Sevilla. 7(1), 2021a, <https://doi.org/10.12795/IETSCIENTIA.2021.i01.11>.

MASCITTI, Matías. La insuficiencia de la causalidad como presupuesto de la responsabilidad civil en los daños producidos por la robótica y los sistemas autónomos. *Revista de Derecho Privado*. Universidad del Externado. Bogotá. 42, 2021b. DOI: <https://doi.org/10.18601/01234366.42.09>Anónimo.

MASCITTI, Matías. El Trialismo como un medio para promover la justicia dentro de la complejidad de la era digital. *Revista Anales de la cátedra Francisco Suárez*, Granada, 2022a. DOI: <https://doi.org/10.30827/acfs.v56i.18498>.

MASCITTI, Matías. El rango constitucional de los neuroderechos como una exigencia de justicia. *Revista Cuestiones constitucionales* Nro. 46. México: UNAM, 2022b. DOI: <https://doi.org/10.22201/ij.24484881e.2022.46.17051>.

MAYER SCHONBERGER, Viktor; CUKIER, Kenneth. *Big Data: A Revolution That Will Transform How We Live*. Kindle edition, 2013.

MAZUR, Joanna. Automated decision-Making and the precautionary principle in EU law. *Baltic Journal of European Studies Tallinn University of Technology* Vol. 9, No. 4 (29), 2019.

MERCIER, Hugo; SPERBER, Dan. *The Enigma of Reason*. Harvard University Press, 2017.

MESSINA DE ESTRELLA GUTIÉRREZ, Graciela N. La función social del Derecho de daños. Rosario: *Investigación y Docencia* Nro. 51, 2015.

MINDA, Gary. Los movimientos del Derecho y la Economía y de los estudios jurídicos críticos en el Derecho norteamericano. En *Derecho y Economía*. Ministerio de Economía y Hacienda. Madrid: Instituto de Estudios Fiscales, 1991.

MONTAGNANI, Maria L.; CAVALLO, Mirta. Liability and Emerging Digital Technologies: An EU Perspective. *Notre Dame Journal of International & Comparative Law*. Vol. 11: Iss. 2, Article 4, 2021. Disponible en: <https://scholarship.law.nd.edu/ndjicl/vol11/iss2/4>. Acceso en: 8 de febrero 2022.

MORENO, Valeria. La prevención en el Derecho de daños. Buenos Aires: *Revista El Derecho*, 2017.

MOSSET ITURASPE, Jorge. Prevención versus reparación. Daño a la persona. Derecho a la no discriminación. Daño por discriminación. *Revista de Derecho de Daños*. Prevención del Daño, 2008.

NAUDÉ, Wim; DIMITRI, Nicola. The race for an artificial general intelligence: implications for public policy. *AI & society*. 35:367–379, 2020.

NEUMANN, John V.; MORGENSTERN, Oskar. *Theory of Games and Economic Behavior*. Princeton: Princeton University Press, 1953.

NINO, Carlos S. La Constitución como convención. *Revista del Centro de Estudios Constitucionales* (6), 1990.

NOTO LA DIEGA, Guido. Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information. *JIPITEC* 3, 2018.

NYHOLM, Sven. Attributing Agency to Automated Systems: Reflections on Human–Robot Collaborations and Responsibility-Loci. *Sci Eng Ethics* 24, 2018. <https://doi.org/10.1007/s11948-017-9943-x>.

O'NEIL, Cathy. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Kindle edition, 2016.

PAENZA, Adrián. *Matemática... ¿Estás ahí?* Episodio 3, 14. 1ª ed. Buenos Aires: Siglo XXI Editores Argentina, 2007.

- PALMERINI, Erica; BERTOLINI, Andrea. Liability and risk management in robotics. En: Schulze R, Staudenmayer D (eds). *Digital revolution: challenges for contract law in practice*. Baden-Baden: Nomos, 2016.
- PALMERINI, Erica; BERTOLINI, Andrea; BATTAGLIA, Fiorella; KOOPS, Bert J.; CARNEVALE, Antoni; SALVINI, Pericle. *RoboLaw: Towards a European framework for robotics regulation, Robotics and Autonomous Systems*, 2016. <http://dx.doi.org/10.1016/j.robot.2016.08.026>.
- PAPO, Laura E.; GONZÁLEZ, Liliana N. Tutela anticipada. *Revista de derecho laboral y seguridad social*. Fascículo Nº 18. Lexis Nexis, 2006.
- PARLAMENTO EUROPEO. *Resolución 2015/2103*, Reglas de Derecho Civil sobre Robotica. Disponible en: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//EN>. Acceso en: 18 de abril de 2022.
- PARLAMENTO EUROPEO. *Resolución 2020/2014*, con recomendaciones a la Comisión sobre un régimen de responsabilidad civil en el ámbito de la IA.
- PELLEGATTA, Stefano. Autonomous driving and civil liability: the Italian perspective. *Rivista di Diritto dell'Economia, dei Trasporti e dell'Ambiente*, 2019.
- PÉREZ BERMEJO, Juan M. *Coherencia y sistema jurídico*. Madrid: Marcial Pons, 2006.
- PESSOA, Luiz. On the relationship between emotion and cognition. *Nature Reviews Neuroscience* 9, 2008. DOI: 10.1038/nrn2317.
- PEYRANO, Jorge W. Régimen de las medidas autosatisfactivas. Nuevas Propuestas. Buenos Aires: *Revista La Ley*, 1998a.
- RACHUM-TWAI, Omri. Whose robot is it anyway?: liability for artificialintelligence-based robots. *University of Illinois Law Review*, 2020.
- RAHMAN, Farhan. COMPAS Case Study: Fairness of a Machine Learning Model, *Towards Data Science*, 2020. Disponible en: <https://towardsdatascience.com/compas-case-study-fairness-of-a-machine-learning-model-f0f804108751>. Acceso en: 18 de abril de 2022.
- RAWLS, John. *A Theory of justice*. Cambridge Massachusetts: Harvard University Press, 1999.
- REALE, Miguel. *Estudos de filosofia e ciencia do direito*. São Paulo: Saraiva, 1978.
- ROYSTER, David C. *Foundations of Real Analysis*. Charlotte: University of North Carolina, 2008.
- RUBENSTEIN, Michael; AHLER, Christian; HOFF, Nick; CABRERA, Adrian; NAGPAL, Radhika. Kilobot: A low cost robot with scalable operations designed for collective behaviors. *Robotics and Autonomous Systems*. Volume 62. Issue 7. 2014, <https://doi.org/10.1016/j.robot.2013.08.006>.
- RUSSELL, Stuart. *Human compatible. Artificial intelligence and the problem of control*. Nueva York: Viking, 2019.
- SALVADOR CODERCH, Pablo. Punitive damages. *Revista Indret*, 2019.
- SEN, Amartya. *La idea de la justicia*. Madrid: Penguin Random House Grupo Editorial. Kindle edition, 2012.
- SINTEZ, Cyril. *Preventive Sanction in the Law of civil responsibility*. A contribution to the theory of construction and effectuation of legal norms, 2009. Disponible en: <https://core.ac.uk/download/pdf/55645942.pdf>. Acceso en: 8 de febrero 2022.
- SLOVIC, Paul; FINUCANE, Melissa L.; PETERS, Ellen; MACGREGOR, Donald. Risk as analysis and risk as feelings: Algunas reflexiones sobre el afecto, la razón, el riesgo y la racionalidad. *Risk Analysis*, 24, 2004.
- SOBRINO, Waldo A. El Deber de Prevención (art. 1710 del Código Civil y Comercial) y su aplicación a los seguros. *Sistema argentino de información jurídica*, 2017.

- STALLA, Sophie; THUERMER, Gefion; WALKER, Johanna; CARMICHAEL, Laura. Data protection by design: Building the foundations of trustworthy data sharing. *Data & Policy* 1, 2020. DOI: 10.1017/dap.2020.1.
- STONOGA, Andreza C. *Tutela inibitória ambiental: a prevenção do ilícito*. Curitiba: Juruá, 2003.
- STROBEL, Volker; CASTELLÓ FERRER, Eduardo; DORIGO, Marco. Blockchain Technology Secures Robot Swarms: A Comparison of Consensus Protocols and Their Resilience to Byzantine Robots. *Front. Robot. AI* 7:54, 2020. DOI: 10.3389/frobt.2020.00054.
- SULER, John R. *Psychology of the Digital Age: Humans Become Electric*. Cambridge University Press, 2015.
- SUPREMA CORTE DE WASHINGTON. Taylor v. Intuitive Surgical, 389 P.3d 517, 2017.
- SURDEN, Harry; WILLIAMS, Mary A. *Technological Opacity, Predictability, and SelfDriving Cars*, 2016. Disponible en: <https://scholar.law.colorado.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1024&context=articles>. Acceso en: 8 de febrero 2022.
- TALEB, Nassim N. *The Black Swan: The Impact of the Highly Improbable*. London: Allen Lane, 2007.
- THALER, Richard H. Economía del comportamiento: pasado, presente y futuro. *Revista de Economía Institucional* 20(38):9, 2018. DOI: 10.18601/01245996.v20n38.02.
- Theories of Tort Law. Stanford Enciclopedia of Philosophy, 2003. Disponible en: <http://plato.stanford.edu/entries/tort-theories/>. Acceso en: 8 de febrero 2022.
- TOMASELLO, Michael. *A Natural History of Human Morality*. Cambridge, Massachusetts: Harvard University press. Kindle edition, 2016.
- Tort as debt market: agency costs, strategic debt, and borrowing against the future. *Harvard Law Review*. Vol. 115. No. 8. Cambridge, Massachusetts, 2002.
- TRAJTENBERG, Manuel. Artificial Intelligence as the Next GPT: A Political-Economy Perspective. En: Agrawal A, Gans J, Goldfarb A (ed.). *The economics of artificial intelligence: an agenda*. Chicago: University of Chicago press, 2019.
- TUNC, André. *La responsabilité civile*. París: Études Juridiques Comparatives, 1981.
- VAN DE GEVEL, Ad J. W.; NOUSSAIR, Charles N. The nexus between artificial intelligence and economics. *Springer Briefs in economics*. Berlin: Springer, 2013.
- VON BERTALANFFY, Ludwig. *Teoría general de los sistemas*. Fundamentos, desarrollo, aplicaciones. Trad. por Juan Almela, México: Fondo de cultura económica. 7ª reimp., 1989.
- WALDRON, Jeremy. The Concept and the Rule of Law. *Georgia Law Review*, 2008.
- WALLIS, Katharine. New Zealand's 2005 'no-fault' compensation reforms and medical professional accountability for harm. *N Z Med J* 126(1371), 2013.
- White paper On Artificial Intelligence - An European approach to excellence and trust, 2020. Disponible en: [https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020\\_en.pdf](https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf). Acceso en: 8 de febrero 2022.
- WIGMORE, Ivy. Black box AI. *WhatsIs.com*, 2019. Disponible en: <https://www.techtarget.com/whatis/definition/black-box-AI#:~:text=A%20black%20box%2C%20in%20a,features%20to%20produce%20an%20output>. Acceso en: 18 de abril de 2022.
- WYATT, Jeremy; SPIEGELHALTER, David. Field trials of medical decision-aids: potential problems and solutions. In: Clayton, P., ed. *Proceedings of 15th Symposium on Computer Applications in Medical Care*. New York: McGraw Hill, 1991.
- YUSTE, Rafael; GENSER, Jared; HERRMANN, Stephanie. It's Time for Neuro-Rights. New Human Rights for the Age of Neurotechnology, Horizons. *Journal of International Relations and Sustainable Development*. 2021.

ZAGREBELSKY, Gustavo. *Derecho dúctil. Ley, derechos, justicia*. Madrid: Trotta, 2011.

SIKMA, Tijs; EDELENBOSCH, Rosanne; VERHOEF, Petra. The use of AI in healthcare: A focus on clinical decision support systems. *RECIPES*, 2020. Disponible en: [https://recipes-project.eu/sites/default/files/2020-11/D2\\_3\\_AI\\_In\\_Healthcare%28CDSS%29\\_HarvardStyle.pdf](https://recipes-project.eu/sites/default/files/2020-11/D2_3_AI_In_Healthcare%28CDSS%29_HarvardStyle.pdf). Acceso en: 18 de junio de 2022.

[http://www.law.harvard.edu/library/collections/special/online-collections/common\\_law/Lecture01.php](http://www.law.harvard.edu/library/collections/special/online-collections/common_law/Lecture01.php). Acceso en 8 de febrero 2022.

[https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020\\_en.pdf](https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf). Acceso en 8 de febrero 2022.

<https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html>. Acceso en: 8 de febrero 2022.

<https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf>. Acceso en: 8 de febrero 2022.

<https://ai.hel.fi/en/ai-register/>. Acceso en: 8 de febrero 2022.

<https://algorithmeregister.amsterdam.nl/en/ai-register/>. Acceso en: 8 de febrero 2022.

<https://www.britannica.com/technology/software>. Acceso en: 2 de junio 2022.

<https://ai4cities.eu/>. Acceso en: 8 de febrero 2022.

<https://www.dataguidance.com/news/luxembourg-cnspd-adopts-first-ever-gdpr-certification>. Acceso en: 10 de junio de 2022.

<https://www.israeleconomico.com/defensa/fuerzas-de-defensa-de-israel-usaron-enjambres-de-drones-contra-hamas-en-gaza/>. Acceso en: 10 de junio de 2022.

<https://futureoflife.org/ai-principles/>. Acceso en: 10 de junio de 2022.

---

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

MASCITTI, Matías. La función preventiva de los daños causados por la robótica y los sistemas autónomos. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 16, p. 15-54, out. 2022. Número especial.

---

Recebido em: 22.03.2022

Pareceres: 07.06.2022, 06.10.2022

Aprovado em: 06.10.2022