

TRANSPARENCIA ALGORÍTMICA Y LA PROPIEDAD INTELECTUAL E INDUSTRIAL: TENSIONES Y SOLUCIONES*

MICHELLE AZUAJE PIRELA** Y DANIEL FINOL GONZÁLEZ***

RESUMEN

Este artículo analiza algunas de las tensiones que se generan entre las crecientes obligaciones de transparencia algorítmica surgidas en el marco de la cuarta revolución industrial y los derechos de propiedad intelectual e industrial, haciendo especial referencia a los secretos empresariales que puedan recaer sobre los algoritmos de inteligencia artificial utilizados para la toma de decisiones automatizadas y la realización de perfiles. En ese sentido, se aportan nuevos elementos para contribuir a la discusión sobre la problemática descrita y se proponen algunas soluciones que permitan resguardar de forma equilibrada tanto la transparencia como los derechos de propiedad intelectual e industrial, desde la perspectiva del Derecho chileno, haciendo puntuales referencias al derecho de la Unión Europea.

* En este artículo se presentan resultados parciales del proyecto de la Universidad Autónoma de Chile, Vicerrectoría de Investigación y Postgrado, DIUA150-2019 titulado: “Régimen jurídico aplicable a la protección del *Big Data* y los algoritmos en el Derecho chileno a la luz del Derecho comparado”, del cual la profesora Azuaje Pirela es investigadora responsable. Asimismo, fue redactado durante la estancia de investigación postdoctoral que realizó la mencionada profesora en los Departamentos de Derecho Civil y Derecho Administrativo de la Universidad de Alicante, con el apoyo del programa de estancias cortas postdoctorales de la Fundación Carolina, convocatoria 2019-2020. En ese sentido, los autores quieren agradecer al Dr. Rubén Martínez Gutiérrez, al Dr. Aurelio López-Tarruella y a la Dra. María Begoña Ribera Blanes, así como a la Universidad de Alicante, a la Fundación Carolina y a la Universidad Autónoma de Chile por el apoyo brindado para la realización de este trabajo.

** Doctora en Derecho, Universidad Autónoma de Chile. Profesora e Investigadora, Universidad Autónoma de Chile. Santiago de Chile (Chile). Correo-e: michelle.azuaje@uautonoma.cl. Fecha de recepción: 19 de marzo de 2020. Fecha de aceptación: 20 de julio de 2020. Para citar el artículo: AZUAJE PIRELA, MICHELLE y FINOL GONZÁLEZ, DANIEL. “Transparencia algorítmica y la propiedad intelectual e industrial: tensiones y soluciones” *Revista de la propiedad inmaterial* n.º 30, Universidad Externado de Colombia, julio 2020-diciembre 2020, pp. 111-146. doi: <https://doi.org/10.18601/16571959.n30.05>

*** Magíster en Computación Aplicada, Universidad del Zulia. Profesor del Minor en Inteligencia Artificial y Derecho, Universidad Autónoma de Chile. Santiago de Chile (Chile). Correo-e: daniel.finol@cloud.uautonoma.cl.

Palabras clave: Propiedad intelectual; Secretos empresariales; Transparencia algorítmica; Decisiones automatizadas; Inteligencia artificial.

ALGORITHMIC TRANSPARENCY AND INTELLECTUAL
PROPERTY: TENSIONS AND SOLUTIONS

ABSTRACT

This article analyzes some of the tensions between the algorithmic transparency obligations that arose in the framework of the fourth industrial revolution, and intellectual property rights, making special reference to the trade secrets that may apply to artificial intelligence algorithms used for automated decision making and profiling. In this sense, new elements are provided to contribute to the discussion on the problem described and some solutions are proposed that allow for the balanced safeguarding of both: transparency, and intellectual and industrial property rights, from the perspective of Chilean law, making specific references to the law of the European Union.

Keywords: Intellectual Property; Trade Secrets; Algorithmic Transparency; Automated Decisions; Artificial Intelligence.

INTRODUCCIÓN

En el mundo de las ciencias de la computación con el término Inteligencia Artificial (IA) se hace referencia, en general, a “la ciencia y la ingeniería para fabricar máquinas inteligentes, especialmente programas informáticos inteligentes”¹. Aunque no hay todavía una única definición sobre lo que es la IA, uno de los aspectos en los que existe acuerdo es que la idea de una máquina “inteligente” sugiere la existencia de un agente flexible que percibe su entorno y lleva a cabo acciones que maximicen sus posibilidades de éxito en algún objetivo o tarea. O que, de alguna manera, imita las funciones cognitivas de la mente humana, como por ejemplo: “percibir”, “razonar”, “aprender” y “resolver problemas”². Así, a través de la IA se busca que las máquinas o sistemas tengan una inteligencia similar a la humana. Incluso, su fin último es lograr ya no imitar a la mente humana, sino “ser una mente”³.

En ese sentido, se distingue entre la llamada IA débil y la IA fuerte. La primera consiste en construir programas que realicen tareas específicas sin necesidad de tener

1 MCCARTHY, J., *What is artificial intelligence?* [en línea] Disponible en: <http://www-formal.stanford.edu/jmc/whatisai/> [consultado el 19/02/2020].

2 RUSSELL, S.; NORVIG, P., *Artificial intelligence: a modern approach*. Upper Saddle River, N.J., Prentice Hall, 2010, p. 2.

3 SEARLE, J., “Minds, brains, and programs.” *Behavioral and Brain Sciences* 3 (3), 1980, 417-457. DOI: <https://doi.org/10.1017/S0140525X00005756>.

estados mentales; en tanto que la segunda (también conocida como Inteligencia Artificial General)⁴, implicaría que un sistema convenientemente diseñado no simula una mente, sino que “es una mente”, y, por consiguiente, debería ser capaz de tener una inteligencia igual o incluso superior a la humana⁵.

Ahora bien, a pesar de que en la actualidad la IA no ha alcanzado su máximo desarrollo⁶, es posible encontrar en la práctica algunos sistemas que realizan tareas específicas realmente sorprendentes y que ya generan las más diversas consecuencias sociales, que a su vez plantean nuevos conflictos jurídicos. Piénsese, por ejemplo, en los vehículos autónomos, los cuales cuentan con una red de señales electrónicas que tramitan sus decisiones. En ese sentido, como vehículos autónomos, son capaces de percibir el medio que les rodea y navegar en consecuencia⁷.

Entre la multiplicidad de alternativas que ofrece hoy en día la IA, también existen sistemas que, a través de *machine learning*⁸ (en español *aprendizaje automático*, que es una subdisciplina o área dentro de la disciplina de estudio, Inteligencia Artificial), hacen posible extraer valor, obtener patrones e inferir información a partir de grandes bases de datos, para convertirla en puntajes, clasificaciones, cálculos de riesgo u otros, que generan consecuencias muy importantes⁹. En particular, para estos sistemas de IA juega un papel fundamental el algoritmo. Este toma decisiones o sirve de instrumento para ello, y se utiliza también para crear perfiles o dirigir comportamientos e influir en determinados sucesos y resultados. Así que, en las últimas décadas, la IA, los datos y los algoritmos han adquirido un rol cada vez más protagónico y una complejidad creciente¹⁰.

4 Sin embargo, debe mencionarse que algunos autores consideran que no es lo mismo IA general que IA fuerte, aunque se trata de términos conectados. En ese sentido, toda IA fuerte será necesariamente general, pero puede haber IA generales, es decir multitarea, que no sean fuertes, que emulen la capacidad de exhibir inteligencia general similar a la humana, pero sin experimentar estados mentales. Sobre esto véase a LÓPEZ DE MÁNTARAS, R., “¿Hacia una nueva Ilustración? Una década trascendente. El futuro de la IA: hacia inteligencias artificiales realmente inteligentes”, [en línea], disponible en: <https://www.bbvaopenmind.com/articulos/el-futuro-de-la-ia-hacia-inteligencias-artificiales-realmente-inteligentes/> [consultado el 19/02/2020].

5 SEARLE, *Minds, brains, and programs*, cit.

6 Hasta ahora la IA es débil y específica, en el sentido de que todavía no existe tal cosa como sistemas que “sean una mente”, o que sean capaces de tener una inteligencia general como la de los seres humanos.

7 Con el término “vehículo autónomo” o “coche autónomo”, en sentido estricto, se hace referencia a un vehículo a motor equipado con un sistema de inteligencia artificial que permite conducirlo sin intervención humana, es decir, con delegación total en los sistemas del automóvil. En ese sentido, los coches autónomos son capaces de imitar las capacidades humanas de manejo, conducción y control. Como vehículo autónomo, puede percibir el medio que le rodea y navegar en consecuencia. BARRIO, M., “Consideraciones jurídicas acerca del coche autónomo”, *Actualidad Jurídica (Uría & Menéndez)* Núm. 52, 2019, pp. 101-108.

8 *Machine learning*, que se refiere en particular al estudio científico de algoritmos y modelos estadísticos que los sistemas computacionales usan para llevar a cabo una tarea específica de forma efectiva sin instrucciones explícitas, apoyándose en patrones e inferencias.

9 PASQUALE, F., *The Black Box Society: The Secret Algorithms That Control Money and Information*, Londres, Harvard University Press, 2015, p. 4.

10 ARELLANO TOLEDO, W., “El derecho a la transparencia algorítmica en *Big Data* e inteligencia artificial”, *Revista General de Derecho Administrativo*, 50, 2019, p. 3.

En efecto, la irrupción de la IA trajo consigo el incremento en el uso de algoritmos para la toma de decisiones automatizadas por parte de instituciones tanto públicas como privadas. En ese sentido, los algoritmos permiten, por ejemplo, a partir de criterios simples o múltiples, previamente asignados, aplicar modelos para determinar la o las alternativas que presenten la mejor puntuación con respecto a dichos criterios. De esta forma, el incremento en el uso de algoritmos de IA se debe, por una parte, a razones económicas (ellos son más eficientes, más rápidos y menos costosos que las personas a las que sustituyen o apoyan en la realización de algunas tareas) y, por otra parte, a razones de aparente objetividad. Así, se supone que los algoritmos al ser “mecánicos” no tienen los problemas de sesgo, subjetividad, emocionalidad y prejuicios característicos de los seres humanos.

Sin embargo, ciertos algoritmos han dado muestra de no ser tan objetivos como se esperaba, pues, en el caso de aprendizaje automático, el proceso de entrenamiento se basa en grandes bases de datos que pueden estar sesgadas, y dicho sesgo replicarse en la decisión tomada o propuesta por el algoritmo. Estas bases pueden estar sesgadas, bien sea por no ser una muestra aleatoria estadísticamente válida de la población de interés, o porque, en algunos casos, contienen el historial de decisiones anteriores tomadas por seres humanos, basadas en los factores que se reflejan en ellas¹¹. Sobre esto interesa destacar que, si el algoritmo contiene errores o sesgos y se utiliza para tomar decisiones puede generar discriminación, daños morales y patrimoniales, o afectar los derechos de las personas sometidas a la decisión. Por lo tanto, se requiere que el derecho como disciplina científica y la legislación, aporten soluciones, por eso la tendencia a nivel internacional es a exigir transparencia.

En este orden de ideas, frente al fenómeno de la IA y la masificación en el uso de datos (muchos de ellos de carácter personal) para crear nuevas formas de negocios y tomar decisiones automatizadas en la era digital, se ha hecho necesaria la creación o el reconocimiento de nuevos derechos y obligaciones. En ese sentido, a nivel internacional en lo relacionado con el uso de datos personales, se reconocen ahora el derecho a la protección de datos personales y, muy cercano a él, el derecho a la “transparencia algorítmica” (entre otros). Ellos implican, entre otras cosas, explicar a las personas cómo y para qué se usan sus datos por los algoritmos y cuáles son los pasos para la toma de las decisiones automatizadas¹². Pero tales derechos deben compatibilizarse con normas e instituciones tradicionales que sobreviven en las legislaciones y podrían dificultar su efectivo ejercicio, generan confusión y, por tanto, pueden obstaculizar la seguridad jurídica.

11 LAMBRECHT, A. & TUCKER, C., *Apparent Algorithmic Bias and Algorithmic Learning*, 2020, SSRN: <https://ssrn.com/abstract=3570076>.

12 COTINO HUESO, L. *Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales*. [en línea], *Dilemata*, 24, 2017, disponible en: <https://ssrn.com/abstract=3413277> [consultado el 28/02/2020]; Arellano, *El derecho a la transparencia algorítmica*, cit., p. 4.

En particular, la transparencia algorítmica implica precisamente otorgar transparencia a algo que, en muchas ocasiones, desde la perspectiva de la propiedad intelectual e industrial (PI) no la tiene o no podría tenerla. En ese sentido, la exigencia de transparencia (ahí donde ella exista) se traduce en una especie de derecho de acceso al algoritmo que, por ejemplo, la justicia italiana ha entendido como un derecho a “descifrar la lógica” de este, y puede conllevar la obligación de proporcionar no solamente las instrucciones relativas al funcionamiento del algoritmo y el proceso para la toma de decisiones, sino también la de proporcionar el lenguaje informático resultante, esto es, el código fuente¹³. Esto plantea o puede plantear un conflicto con la propiedad intelectual e industrial sobre todo porque revelar el código fuente implica revelar el algoritmo, el cual frecuentemente es resguardado como secreto empresarial o información no divulgada. Por lo tanto, en muchas ocasiones los algoritmos se mantienen en un plano de confidencialidad que, siempre que se cumplan las condiciones de ley, también está protegida por el Derecho¹⁴.

En este orden de ideas, la convivencia entre los sistemas tradicionales de propiedad intelectual y las nuevas exigencias de transparencia en el uso de sistemas de IA para la toma de decisiones puede generar importantes tensiones: ¿se puede explicar cómo funciona un algoritmo sin revelar el secreto empresarial que lo protege? O bien, ¿puede una empresa tecnológica excusarse de explicar cómo funciona un algoritmo o cómo se tomó una decisión automatizada porque este está amparado por un secreto empresarial? En ese sentido, algunos de los nuevos desafíos del derecho frente a la IA obligan a resolver: ¿cómo cumplir con la transparencia algorítmica y al mismo tiempo mantener protegida información privilegiada y sensible para las empresas?, ¿cómo hacer compatibles dos regímenes que parecen ser tan antagónicos?, ¿es importante distinguir si se trata de una institución pública o privada?, ¿es o debe ser la transparencia algorítmica un nuevo límite a la PI? O ¿es la PI un límite a la transparencia algorítmica?

Este artículo tiene como propósito aportar más elementos que puedan contribuir a esta discusión, así como esbozar algunas soluciones a la problemática descrita, desde la perspectiva del Derecho chileno, haciendo puntuales referencias al Derecho de la Unión Europea.

13 Sobre este particular, la justicia italiana ya se ha pronunciado en términos de exigir a administraciones públicas que utilizan algoritmos para la toma de decisiones que proporcionen no solamente todas las instrucciones relativas al funcionamiento del algoritmo, asegurando la comprensibilidad del funcionamiento del software incluso para el ciudadano común, sino también el lenguaje informático resultante (código fuente) del sistema algorítmico. CARLONI, E., “IA, algoritmos y Administración pública en Italia”, [en línea], *Revista de Internet, Derecho y Política*, 30, 2020, disponible en: https://www.researchgate.net/publication/339633312_IA_algoritmos_y_Administracion_publica_en_Italia [consultado el 28/05/2020].

14 PÉREZ SANZ, C., “Aspectos legales del Big Data”, en *Índice: Revista de Estadística y Sociedad*, 68, 2016, pp. 18-21.

I. EL ALGORITMO Y SU RELEVANCIA PÚBLICO-PRIVADA

Actualmente no existe unanimidad en cuanto a la definición técnica y formal de algoritmo; ella es aún objeto de investigación. No obstante, en términos generales, es descrito como una secuencia finita y determinista de pasos mecánicos precisos que producen la solución a un problema¹⁵. Los algoritmos no pueden considerarse equivalentes o sinónimos de los programas de computación, puesto que no necesariamente están expresados en secuencias de instrucciones en lenguaje de programación o de máquina, ya que en general un algoritmo es independiente de su forma de expresión¹⁶; el programa es la implementación del algoritmo.

En el contexto de la IA moderna, que es el foco de interés del presente trabajo, puede decirse que el algoritmo constituye una secuencia de operaciones lógicas que se traducen en instrucciones al computador para que actúe sobre los datos incorporados y adopte decisiones automáticamente. Los resultados que se obtengan se basan en entradas de datos y parámetros inferidos de una muestra independiente de datos¹⁷.

Hoy en día, las empresas tecnológicas ofrecen una gran variedad de servicios que utilizan grandes volúmenes de datos (*big data* o macrodatos) y aplican algoritmos para facilitar o llevar a cabo diversas tareas tanto en el ámbito público como en el privado. Por lo tanto, estos se encuentran presentes en la vida cotidiana y se utilizan como base para, por ejemplo, calcular tipos de intereses de préstamos¹⁸, evaluar y contratar trabajadores, predecir niveles de criminalidad y reincidencia¹⁹, proponer soluciones a decisiones administrativas²⁰, e incluso para crear “obras de arte”²¹.

15 MOSCHOVAKIS, Y., “What is an algorithm?”, en ENGQUIST, B., & SCHMID, W. (Eds.) *Mathematics Unlimited — 2001 and beyond, Part II*, Springer, 2001, pp. 919-936; BUSS, S., ALEXANDER, S., PILLAY, A., & SHORE, R., “The Prospects for Mathematical Logic in the Twenty-First Century”, *The Bulletin of Symbolic Logic*, 7, 2, 2001, pp. 169-196; BLASS, A., & GUREVICH, Y., “Algorithms: A Quest for Absolute Definitions”, *Bulletin of the European Association for Theoretical Computer Science*, 81, 2003, pp. 195-225; GUREVICH, Y., “What is an Algorithm? (Revised)”, en A. Olszewski et al. (Eds.) *Church’s Thesis: Logic, Mind and Nature*, Copernicus Center Press, 2014, pp. 1-15.

16 PÉREZ, *Aspectos legales*, cit., p. 21.

17 DOMINGOS, P., *The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World*, New York, Basic Books, 2015, p. 1.

18 OTERO GONZÁLEZ, L. & DURÁN SANTOMIL, P., “Fintech, blockchain y big data”, en García Novoa, César y Santiago Iglesias, Diana (Dir.), *4ª Revolución industrial: impacto de la automatización y la Inteligencia artificial en la Sociedad y la economía digital*, Pamplona, Thomson Reuters Aranzadi, 2018, pp. 81-113.

19 ANGWIN, J.; LARSON, J.; MATTU, S. & KIRCHNER, L., “Machine Bias. There’s software used across the country to predict future criminals. And it’s biased against blacks” [en línea], disponible en: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> [consultado el 10/01/2020].

20 DE LA SIERRA, S., “Inteligencia artificial y justicia administrativa: una aproximación desde la teoría del control de la administración pública”, *Revista General de Derecho Administrativo*, 53, 2020, pp. 1-19.

21 NAVAS NAVARRO, S., “Obras generadas por algoritmos. En torno a su posible protección jurídica”, *Revista de Derecho Civil*, vol. V, núm. 2018, pp. 273-291; NAVAS NAVARRO, S., “Creación Original e Inteligencia Artificial” en Navas Navarro, Susana (Dir.), *Nuevos desafíos para el Derecho de Autor. Robótica, Inteligencia Artificial, Tecnología*, Madrid, Reus,

Entre las ventajas que se predicán del uso de los algoritmos destacan su fiabilidad y precisión, ya que apoyan o efectúan la toma de decisiones pertinente sin dudas ni ambigüedades. Por eso su uso y valor económico van en incremento. Piénsese que, por medio del uso de algoritmos, han sido posibles cosas tan inimaginables como la producción de la primera imagen de un agujero negro, la predicción de ataques al corazón o la detección de riesgos de cáncer de mama.

En efecto, en un estudio de la Universidad de Chile en el que se detectó discriminación de género en el mercado de créditos de consumo, para corregirla se recomendó, entre otras cosas, la automatización del proceso de evaluación mediante el uso de algoritmos, para limitar la influencia de los ejecutivos de cuenta en la decisión final²². También en relación con el sobreendeudamiento se ha explorado el uso de las herramientas del *Big Data*, *fintech* y el apoyo de *roboadvisors*²³ para elaborar perfiles y tomar medidas que ayuden a evitar el endeudamiento excesivo o aliviarlo una vez constatado²⁴. En estos y otros casos los algoritmos se utilizarían para garantizar la objetividad de proceso esperándose que actúen mejor que los seres humanos. En efecto, algunas investigaciones afirman que los algoritmos bien diseñados deberían poder corregir y evitar sesgos cognitivos de muchos tipos²⁵.

Sin embargo, existen también estudios en contrario, de acuerdo con las cuales la presumible objetividad de los algoritmos no es tal²⁶. Y, aunque puede alegarse

2019, pp. 27-45; RÍOS RUIZ, W., “Los sistemas de inteligencia artificial y la propiedad intelectual de las obras creadas, producidas o generadas mediante ordenador”, *Revista la propiedad inmaterial*, n.º 3, 2001, pp. 5-13.

22 MONTOYA, A.; PARRADO, E.; SOLIS, A.; UNDURRAGA, R., “Documento de Trabajo n.º 03/20: Discriminación de género en el mercado de créditos de consumo” [en línea], disponible en: https://www.sbf.cl/sbifweb3/internet/archivos/publicacion_12587.pdf [consultado el 26/02/2020].

23 *Fintech “Financial Technology”* se refiere a aquellas actividades financieras que utilizan nuevas tecnologías para mejorar la eficiencia en los servicios financieros. Los *roboadvisors*, por su parte, son un tipo de asesores que a través del uso de modelos automatizados y algoritmos proporcionan un servicio de gestión de carteras basado en la web en los que prácticamente no intervienen personas. Se caracterizan por ser económicos y porque los algoritmos en los que se basan permiten prestar servicios personalizados. OTERO & DURÁN, *Fintech, blockchain y big data*, cit., p. 82.

24 Según GOLDENBERG, J., “Herramientas del Big Data y del *fintech* para prevenir y aliviar el sobreendeudamiento del consumidor: una propuesta”, *Revista chilena de derecho y tecnología* [en línea], vol.8, n.º 2, 2019, pp. 5-32, disponible en: <http://dx.doi.org/10.5354/0719-2584.2019.54051> [consultado el 19/02/2020]; como parte relevante de la industria del *fintech*, se han ido generando plataformas de *roboadvisors* basadas en los perfiles de riesgo, antecedentes y metas de los clientes. Su significado genérico es la entrega del consejo financiero por medio de una plataforma digital y su operatividad se basa en: i) la recolección de datos de manera voluntaria entregados por parte de los clientes -incluyendo toda suerte de datos personales, incluso sensibles-, justificables bajo los parámetros de la “autogestión de la privacidad”; y ii) en la información obtenida por medio de las respuestas a las múltiples preguntas dispuestas por la plataforma, los que son utilizados por los algoritmos de la entidad financiera para generar el consejo de endeudamiento o inversión adecuado.

25 SUNSTEIN, C., “Algorithms, Correcting Biases”, [en línea], *Forthcoming, Social Research*, 2018, SSRN: <https://ssrn.com/abstract=3300171> [consultado el 26/02/2020]; COWGILL, B., “Bias and Productivity in Humans and Machines”, 2019, SSRN: <https://ssrn.com/abstract=3584916> [consultado el 28/02/2020].

26 LAMBRECHT & TUCKER, *Apparent Algorithmic Bias and Algorithmic Learning*, cit.

que estos, en el peor de los casos, solo estarían reproduciendo los sesgos de los humanos, dada la escalabilidad y masividad con que pueden aplicarse, es posible que pequeños sesgos tengan consecuencias masivas al aplicarse a gran escala.

Así que esa aludida cotidianidad del uso de los algoritmos que por mucho tiempo pasó “inadvertida” y generó ingentes beneficios económicos, hoy en día es más conocida y cuestionada en ciertos ámbitos. Y es que si los algoritmos afectan la vida de las personas en diversos niveles –a veces sin saberlo–, y a través de ellos se tratan datos personales para tomar decisiones o realizar inferencias, cabría preguntarse: ¿cómo funcionan?, ¿cómo saber que no cometen errores?, ¿cómo saber que no están sesgados o son discriminatorios? La inherente falta de transparencia, la opacidad en el diseño y la falta de explicabilidad de los algoritmos son grandes desafíos que deben enfrentar los ordenamientos jurídicos ante la irrupción de la IA²⁷. Sobre esto se volverá más adelante.

II. PROTECCIÓN JURÍDICA DE LOS ALGORITMOS

POR EL SISTEMA DE PROPIEDAD INTELECTUAL E INDUSTRIAL

A grandes rasgos, la propiedad intelectual es el área del Derecho que regula la creación, uso y explotación del trabajo que es resultado de procesos creativos o mentales. La acepción restringida del término “propiedad intelectual” se refiere específicamente al “derecho de autor”. De este se desprende un conjunto de prerrogativas o facultades morales y patrimoniales que nacen por el solo acto de la creación de la obra, en favor de los autores de “obras de la inteligencia” en los dominios literarios, artísticos y científicos, cualquiera que sea su forma de expresión.

En los países de tradición latina, además de la expresión derecho de autor, se utilizan las expresiones propiedad literaria y artística y propiedad intelectual como especie de sinónimos²⁸. En ese contexto, la propiedad intelectual (en oposición a la propiedad industrial) se relaciona con la protección de las creaciones del espíritu en las que queda plasmada la personalidad del autor, tratándose de creaciones únicas y no producidas industrialmente o en serie.

En su acepción amplia (que es la que se utiliza en el marco de los instrumentos internacionales administrados por la Organización Mundial de la Propiedad Intelectual, OMPI), la propiedad intelectual se relaciona con las creaciones de la mente que incluyen invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizados en el comercio. De ahí que en ese contexto se divide en dos

27 MITTELSTADT, B.; ALLO, P.; TADDEO, M.; WACHTER, S. & FLORIDI, L., *The Ethics of Algorithms: Mapping the Debate*. [en línea], *Big Data & Society*. 3(2), 2016, disponible en: 10.1177/2053951716679679 [consultado el 26/02/2020]; WACHTER, S.; MITTELSTADT, B. & FLORIDI, L., “Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation”, *International Data Privacy Law*, 2017, SSRN: <https://ssrn.com/abstract=2903469>.

28 LIPSZYC, D., *Derecho de Autor y Derechos Conexos*, Buenos Aires, Unesco, 2002, p. 19. En el ordenamiento jurídico chileno “propiedad intelectual” se entiende como derecho de autor y su contenido está regulado por la Ley 17.336, “de propiedad intelectual”.

categorías: la propiedad industrial, que abarca fundamentalmente las patentes de invención, las marcas, los diseños industriales y las indicaciones geográficas; y el derecho de autor, que comprende las obras literarias, las películas, la música, las obras artísticas y los diseños arquitectónicos, los programas de computación, entre otros.

Tales derechos y, particularmente el derecho de autor, gozan de protección constitucional²⁹, lo que, en el caso de este último, deviene de un régimen jurídico especial, para cuyo nacimiento es necesario que exista un autor, una obra, y que ella sea original. Quedando esta última protegida frente a actos tales como la publicación, reproducción y comunicación pública no autorizadas (salvo excepciones)³⁰. Adicionalmente, es posible hallar otros derechos distintos al derecho de autor, pero relacionados con él, que se confieren en torno a otras formas de creatividad humana, como es el caso de los derechos afines, conexos o de los llamados derechos *sui generis* que han venido reconociéndose de la mano del desarrollo tecnológico.

En este orden de ideas, desde la perspectiva de los derechos intelectuales es importante distinguir entre el programa de computación y el algoritmo en sí mismo. Ello porque, tanto en Chile como en otros países que comparten su tradición jurídica, el programa computacional está protegido por el sistema de derecho de autor conforme al artículo 3° 16) de la Ley 17.336, de propiedad intelectual³¹, pero, en el caso del algoritmo, el panorama es un poco diferente, pues no existe una protección específica.

Y es que, así como resulta complejo aportar una definición de algoritmo, también lo es determinar una eventual autoría o titularidad de derechos intelectuales sobre el mismo. Por ejemplo, porque si bien normalmente son personas (computistas, matemáticos, ingenieros, etc.) quienes lo crean, algunos algoritmos pueden ser diseñados automáticamente por una computadora. También porque en ocasiones se duda acerca de si esos algoritmos son “descubiertos” o implican alguna actividad creativa o inventiva de su creador, pudiendo existir o no originalidad o novedad en ellos, para ser considerados obras o invenciones dignas de proteger, según sea el caso³².

29 Así lo establece la Constitución Política chilena en su artículo 19, n.º 25.

30 Las legislaciones sobre derecho de autor contienen un capítulo dedicado a los “límites y excepciones”, que consiste en un catálogo de usos de obras protegidas que podrán hacer terceros sin que se requiera de la autorización del autor o titular del derecho. En ese sentido, el derecho de autor tiene los límites propios de los derechos subjetivos, los que derivan de la colisión con otros derechos y otros “genéricos” resultantes de la necesidad de su ejercicio conforme a la buena fe y la prohibición del abuso del derecho mismo. ROGEL VIDE, C. & SERRANO GÓMEZ, E., *Manual de Derecho de Autor*. Madrid, Reus, 2008, p. 55.

31 Conforme a esta norma, quedan especialmente protegidos con arreglo a la presente ley (entre otros), los programas computacionales, “cualquiera sea el modo o forma de expresión, como programa fuente o programa objeto, e incluso la documentación preparatoria, su descripción técnica y manuales de uso”.

32 AZUAJE, M. & FINOL, D., “Big Data, algoritmos y propiedad intelectual”, *Anuario de propiedad intelectual*, N.º. 2016, 2017, p. 262.

En relación con este particular, se han planteado recientemente algunas discusiones. Así, sobre la hipótesis de que “puede haber situaciones en las que un software o un algoritmo deben ser considerados los inventores”, algunos representantes del proyecto AIP (The Artificial Inventor Project)³³ solicitaron patentes para dos inventos³⁴, en las que, en lugar de identificar a un inventor humano en los formularios, se indicó que el inventor era Dabus AI, un sistema de inteligencia artificial de Stephen Thaler, CEO de una compañía llamada Imagination Engines. En la solicitud se indicó a Dabus AI como quien ideó las innovaciones después de recibir datos generales sobre muchos temas porque, aunque Stephen Thaler creó a Dabus, él aducía no tener conocimientos ni ser capaz de desarrollar por sí mismo la luz de advertencia y el recipiente de alimentos a los que se contraen las solicitudes de patentes. Por eso en opinión del equipo de AIP, Dabus es el legítimo inventor y así se indicó en las solicitudes. Sin embargo, tanto la oficina de patentes del Reino Unido como la de Europa consideraron que, aunque las invenciones en sí mismas podrían ser dignas de patentes, las solicitudes debían rechazarse porque el “inventor” no era un ser humano³⁵.

El problema en este caso se orientó hacia la falta de personalidad jurídica del agente señalado como inventor (lo que deriva del hecho de que quien se señala como inventor no es un ser humano), pero también se ha cuestionado si incluso existiendo aquella, puede entenderse técnicamente que una IA es realmente capaz de “inventar algo” sin asistencia humana cuando, como se señalaba al inicio, con la tecnología actual todavía no existe una IA fuerte y general³⁶. Así que se trata de una tecnología que, a pesar de su gran sofisticación y enorme complejidad, no deja de pertenecer a alguien y, por lo tanto, está subordinada a la titularidad y manejo de personas que tendrían que ser jurídicamente determinadas, y esa falta de determinación es uno de los grandes problemas jurídicos actuales.

En todo caso, en relación con el sistema para proteger al algoritmo propiamente tal, si este fuese “obra”, estaría protegido por el derecho de autor desde el momento mismo de su creación (dado su carácter declarativo), y si fuese “invención”, podría ser patentado siguiendo el procedimiento de ley para ello (en virtud de su carácter constitutivo). Sin embargo, dado que los algoritmos constituyen un conjunto de operaciones que se pretende realizar para conseguir un resultado concreto o resolver un problema, son entidades abstractas. Esto conlleva la dificultad de protegerlos

33 Página web: <https://artificialinventor.com/>.

34 La identificada “EP 18 275 163” y la “EP 18 275 174”.

35 La Intellectual Property Office rechazó asimismo la solicitud en diciembre de 2019; la decisión está disponible en: <https://www.ipo.gov.uk/p-challenge-decision-results/o74119.pdf>. Por su parte, las decisiones de la EPO están disponibles en: <https://register.epo.org/application?documentId=E4B63SD62191498&number=EP18275163&lng=en&npl=false>; y en: <https://register.epo.org/application?documentId=E4B63OBI2076498&number=EP18275174&lng=en&npl=false>.

36 CHEN, A., “Inteligencia Artificial: El caso de la IA que intentó patentar dos inventos en su nombre”, *MIT Technology Review*, [en línea] disponible en: <https://www.technologyreview.es/s/11776/el-caso-de-la-ia-que-intento-patentar-dos-inventos-en-su-nombre>[consultado el 19/08/2020].

per se como elementos independientes, porque no pueden considerarse “propiedad intelectual” (por no calificar como obras) y porque se les considera fuera de las materias patentables, ya que en muchos casos se les equipara a los “métodos matemáticos”.

Dado que el derecho de autor protege la forma de expresión de las obras intelectuales y no las ideas en sí mismas, al pertenecer al mismo mundo abstracto que estas no son protegidos por este régimen (a menos que se considere a los algoritmos como parte del software que los implementa, siendo que este último —el software—, sí está protegido por este derecho, y, por tanto, por derechos de no divulgación y al inédito). Así que, aunque los algoritmos son más precisos, definidos y específicos que una “mera idea”, no se protegen de forma independiente por este sistema. Tampoco serían patentables (o, para poder serlo, tendrían que reunir una serie de requisitos, que normalmente no reúnen) y no estar excluidos por la legislación de propiedad industrial respectiva.

En este orden de ideas, en Chile, ni la Ley 17.336 de propiedad intelectual ni la Ley 19.039 de propiedad industrial hacen mención del término *algoritmo*. Pero dado que, en el caso del derecho de autor, se protege la forma de expresión y no la “idea”, un algoritmo estaría protegido solo cuando no recoja “meras ideas” o principios generales sino en la medida en que revista el carácter de originalidad necesario para considerarse una “obra”.

En cuanto a su patentabilidad, la Ley 19.039, en su artículo 37 letra a) dispone que no se considera invención y quedarán excluidos de la protección por patente: “los descubrimientos, las teorías científicas y los métodos matemáticos”. Término con el que generalmente se les asocia. Con todo, algunas oficinas de patentes en el mundo han admitido el registro de algoritmos presentados de forma conjunta con un elemento físico³⁷. En esos casos, la información relativa a la patente que haya sido registrada por el órgano respectivo será de acceso público.

Así pues, ante la falta de precisión, ambigüedades legislativas, y ante la dificultad del patentamiento de los algoritmos o frente a la imposibilidad de su protección por el derecho de autor, estos no disponen de un régimen jurídico específico o propio. En atención a ello y también por razones económicas y comerciales, en la actualidad a los algoritmos se les resguarda normalmente como secretos empresariales. Por lo que no resulta extraño que se les mantenga en un plano de confidencialidad³⁸.

A. ALGORITMOS Y SECRETOS EMPRESARIALES

Los secretos empresariales se relacionan con cualquier información, relativa a cualquier ámbito de la empresa, incluido el tecnológico, científico, industrial,

³⁷ GUADAMUZ GONZÁLEZ, A., “Patentabilidad del software: nuevas cuestiones jurídicas.” *Revista de la OMPI*, 6, 2008, [en línea] disponible en: http://www.wipo.int/wipo_magazine/es/2008/06/ [consultado el 19/02/2020].

³⁸ PÉREZ, *Aspectos legales*, cit., p. 21.

comercial, organizativo o financiero, que reúna tres condiciones fundamentales: a) que sea secreta, en el sentido de no ser generalmente conocida ni de fácil acceso para los círculos en que normalmente se utilizaría; b) que tenga valor empresarial como consecuencia de su carácter secreto, y c) que se hayan adoptado medidas razonables por parte de su titular para que permanezca secreto³⁹.

En ese sentido, no se adquiere de un registro válidamente efectuado, sino el mantenimiento en secreto, pero, aunque no se requiere título de protección, no es suficiente con que el titular de la información aduzca que ella es secreta o confidencial, sino que es necesario que efectivamente lo sea y que su revelación produzca perjuicios económicos o merme las ventajas competitivas de su titular. Así que una de las principales diferencias entre los secretos empresariales y las patentes está precisamente en que mientras los primeros son confidenciales, las segundas son de acceso público, pues nacen de un proceso de registro público.

En efecto, en el caso de las patentes, el inventor consigue protección solo si hace público su conocimiento técnico. Pero a pesar de esa publicidad la invención queda protegida, dado que durante cierto tiempo es “gravada” con la exclusividad, no pudiendo ser utilizada en forma libre por terceros⁴⁰. Aunque los secretos empresariales y la información no divulgada gozan de protección constitucional y de algunas ventajas, tradicionalmente ha sido uno de los regímenes más débiles y difusos del sistema de PI (incluso hay quienes niegan que pertenezca a él)⁴¹ y esto contrasta con el creciente valor económico y las infinitas posibilidades de aplicación de los algoritmos y los nuevos modelos de negocios en la era digital.

La protección jurídica de los secretos empresariales se cuestiona, entre otras razones, porque a diferencia del derecho de autor y las patentes, no se tiene protección frente a la copia, no posee limitación temporal (lo que puede ser a su vez una ventaja), y, además, porque la utilización no autorizada de dicha información por personas distintas del titular del secreto empresarial se considera práctica desleal y violación de este. Además, el derecho conferido por ellos se caracteriza por su vulnerabilidad, en la medida en que su divulgación generalizada y pérdida de control conduce inevitablemente a la pérdida del derecho⁴².

En consecuencia, sus titulares dejan sometido el conocimiento de los secretos a obligaciones de confidencialidad, a la toma de las medidas contractuales para garantizarla, y otras necesarias para mantener el secreto. En ese contexto, en caso

39 Artículo 39 del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio ADPIC.

40 SCHMITZ VACCARO, C., “Propiedad intelectual, dominio público y equilibrio de intereses”, *Revista Chilena de Derecho*, vol. 36 n.º 2, 2010, pp. 343-367.

41 Véase entre otros a: SCHMITZ VACCARO, C., “Secretos empresariales en Chile: medidas de protección”, *Revista Internacional Foro de Derecho Mercantil*, 37, 2012, pp. 13-41; y PEÑA TORRES, M., “Protección constitucional del secreto industrial”, *Revista Chilena de Derecho*, 28, 2, 2001, pp. 413-424.

42 LISSÉN ARBELOA, J. & GUILLÉN MONJE, P., “Características, alcance de la protección conferida e implicaciones para las empresas en la nueva Ley de Secretos Empresariales”, *Diario La Ley*, 2019, pp. 1-7.

de acceso, apropiación o difusión no autorizada, se debe recurrir a las acciones civiles y penales normalmente dispersas en el ordenamiento jurídico (en leyes de propiedad industrial, de libre competencia y en códigos penales). Pero su mayor garantía la han ofrecido los contratos, pues la infracción de normas contractuales podría devenir en indemnizaciones de perjuicios. Asimismo, a diferencia de las otras modalidades de propiedad industrial no están constreñidos por el principio de territorialidad⁴³.

En Chile, los secretos empresariales se protegen sobre la base del artículo 19 n.º 25 de la Constitución Política. Ahí se garantiza “la propiedad industrial sobre las patentes de invención, marcas comerciales, modelos, procesos tecnológicos u otras creaciones análogas, por el tiempo que establezca la ley”. De esta forma, aunque no se mencionan de manera expresa, históricamente se ha entendido que, al emplear la expresión “otras creaciones análogas”, se da cabida a la protección de los secretos empresariales. También al *know how* y los conocimientos técnicos no patentables que tengan el carácter de reservados cuando se menciona a los “procesos tecnológicos”, ya que estos se refieren a todos los métodos o procedimientos planificados y que se mantienen en reserva, con los cuales es posible producir un invento o un modelo industrial⁴⁴.

Asimismo, pueden encontrarse algunas normas aplicables a los secretos empresariales en el D.L. n.º 211^[45]. Pero es en los artículos 86 al 91 de la Ley 19.039 donde se desarrolla específicamente su régimen jurídico. Sin embargo, este adolece de algunas deficiencias. Entre ellas destaca, en primer lugar, que el artículo 86 contiene una definición restringida de secreto que no se ajusta a los estándares internacionales (artículo 39 ADPIC suscrito por Chile), pues entiende por tales “todo conocimiento sobre productos o procedimientos industriales, cuyo mantenimiento en reserva proporciona a su poseedor una mejora, avance o ventaja competitiva”⁴⁶, lo que comprende únicamente a los secretos industriales. En segundo lugar, no se prevé (salvo excepción en materia sanitaria) un régimen de limitaciones y excepciones para que ciertas autoridades o sujetos, bajo ciertos presupuestos puedan acceder lícitamente al secreto.

Piénsese que, aunque es legítimo que el titular del secreto pueda mantener reserva de él y esta reserva goza de protección jurídica, como cualquier otro derecho, este tendría que admitir algunos límites y excepciones⁴⁷. Así, en el Derecho español, recientemente entró en vigor la Ley 1/2019, de Secretos Empresariales (LSE) que contiene una regulación transversal del secreto empresarial que fortalece

43 PÉREZ, *Aspectos legales*, cit., p. 21.

44 PEÑA, *Protección constitucional del secreto industrial*, cit., p. 419.

45 Decreto Ley n.º 211 (07/03/2005) Que fija el texto refundido, coordinado y sistematizado del decreto ley n.º 211, de 1973.

46 SCHMITZ, *Secretos empresariales*, cit.

47 Sin perjuicio de esto, en materia de derecho de autor la Ley 17.336 sí reconoce un catálogo de límites y excepciones a través de las cuales se garantizan ciertos usos y accesos a obras protegidas por este régimen. Pero tales límites tienen una naturaleza jurídica distinta a la que aquí se propone.

las garantías y aborda diversos aspectos imponiendo nuevas obligaciones. A través de ella se transpone la Directiva (UE) 2016/943^[48], dando un paso más en la defensa legal de la innovación en España. La ley precisa el ámbito de protección conferido por el secreto empresarial, los actos de infracción, los mecanismos procesales a hacer valer por el titular frente a los infractores, pero también sus excepciones y límites⁴⁹.

De especial interés resulta el artículo 2, relativo a la “Obtención, utilización y revelación lícitas de secretos empresariales”. En él se considerará lícita la obtención de la información constitutiva del secreto empresarial en los casos y términos en los que el Derecho europeo o español lo exija o permita. También se establece que no procederán las acciones y medidas previstas en ella cuando se dirijan contra actos de obtención, utilización o revelación de un secreto empresarial que hayan tenido lugar con la finalidad de descubrir, en defensa del interés general, alguna falta, irregularidad o actividad ilegal que guarden relación directa con dicho secreto empresarial; o bien con el fin de proteger un interés legítimo reconocido por el Derecho europeo o español.

En particular, no podrá invocarse la protección dispensada por la ley de secretos empresariales para obstaculizar la aplicación de la normativa que exija a los titulares de ellos divulgar información o comunicarla a las autoridades administrativas o judiciales en el ejercicio de sus funciones, ni para impedir la aplicación de la normativa que prevea la revelación por las autoridades públicas europeas o españolas, en virtud de las obligaciones o prerrogativas que les hayan sido conferidas por el Derecho europeo o español, de la información presentada por las empresas que obre en poder de dichas autoridades.

Conforme a esta experiencia, se observa que no es tan extraño que los secretos empresariales –aunque protegidos– pueden admitir ciertos límites y excepciones, y debería ser así especialmente cuando se trate de proteger mediante esta vía una herramienta que toma decisiones con un alto grado de injerencia en la vida de las personas (por ejemplo, pacientes, compradores en línea o asegurados). Pero al mismo tiempo es cierto que el secreto empresarial puede servir como límite a la transparencia y a ciertas actuaciones administrativas⁵⁰.

48 Relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales), contra su obtención, utilización y revelación ilícitas.

49 LISSÉN & GUILLÉN, *Características, alcance de la protección*, cit., pp. 1-7; MOLINA HERNÁNDEZ, C., “La protección de secretos empresariales,” en CAMPUZANO, A.; PALOMAR OLMEDA, A.; SAN JUAN y MUÑOZ, E. y MOLINA HERNÁNDEZ, C., *La protección de secretos empresariales*, Valencia: Tirant Lo Blanch, 2019, pp. 39-48; Fuentes MASSAGUER, J., “De nuevo sobre la protección jurídica de los secretos empresariales (a propósito de la ley 1/2019, de 20 de febrero, de secretos empresariales)”, *Revista “Actualidad Jurídica Uría Menéndez”*, 51, 2019, pp. 46-70.

50 ESTEVE PARDO, M., “El secreto profesional y la propiedad intelectual e industrial,” en INAP, *Los límites al derecho de acceso a la información pública*, Madrid, Instituto Nacional de Administración Pública, 2017, pp. 175-183.

III. PRINCIPALES PROBLEMAS ÉTICO-JURÍDICOS DE LOS ALGORITMOS: ALGUNAS TENSIONES ENTRE LA TRANSPARENCIA ALGORÍTMICA Y LA PROPIEDAD INTELECTUAL E INDUSTRIAL

A) PRINCIPALES PROBLEMAS ÉTICO-JURÍDICOS DEL USO DE ALGORITMOS DE IA

A pesar de la objetividad que se ha mencionado parece ser característica de los algoritmos, algunos de ellos han dado muestra de no ser tan objetivos como se esperaba⁵¹. A este respecto, se puede argumentar que no es necesario que los algoritmos de IA (o las bases a partir de las cuales realizan sus inferencias) sean 100% objetivos y libres de sesgos, sino que es suficiente con que sean más objetivos que los humanos a los que reemplazan o apoyan en la realización de algunas tareas. Sin embargo, un contraargumento para su uso es que los seres humanos, a pesar de no ser 100% objetivos, son capaces de ofrecer una explicación razonada de las decisiones que toman, la cual no siempre pueden dar los algoritmos, especialmente los de caja negra.

La característica fundamental de estos últimos es que ni siquiera sus creadores pueden ver cómo están tomando dichas decisiones⁵². Una de las técnicas de aprendizaje automático es el *deep learning* (aprendizaje profundo) que utiliza “redes neuronales”⁵³. A través de *deep learning*, la máquina actuará como si fuera una red neuronal, es decir, imitando al cerebro. Esto implica que de la misma forma que ocurre con él, con la tecnología más avanzada que se usa en la actualidad, nadie sabe exactamente el “razonamiento” detrás de un resultado particular. Para saberlo se requiere más investigación y más recursos que permitan comprender estos modelos y ello va más allá de un problema de transparencia o de propiedad intelectual, trasladándose a un plano más técnico⁵⁴. Sin embargo, este tipo de algoritmos ha venido usándose casi de forma imperceptible.

Ahora bien, desde la perspectiva ético-jurídica, una de las mayores preocupaciones que rodean los usos actuales de los algoritmos de IA (no solamente los de caja negra) se centra tanto en sus efectos frente a ciertos derechos fundamentales, como en la eventual falta de justicia en la toma de decisiones algorítmicas automatizadas. Entendiendo por tales, aquellas tomadas por medios tecnológicos sin

51 MYERS WEST, S.; WHITTAKER, M.; CRAWFORD, K., “Discriminating systems: Gender, Race, and Power in AI” [en línea], disponible en: <https://ainowinstitute.org/discriminating-systems.pdf> [consultado el 04/03/2020].

52 ARELLANO, *El derecho a la transparencia algorítmica*, cit., 3; Cotino, *Big data*, cit. 136; Mittelstadt *et al.*, cit. *The Ethics of Algorithms*.

53 NAVAS NAVARRO, S., “Derecho e inteligencia artificial desde el diseño”, en NAVAS NAVARRO, SUSANA (COORD.), *Inteligencia artificial: tecnología, derecho*, Valencia, Tirant Lo Blanch, 2017, p. 52.

54 Access Now, *Human Rights in the age of artificial intelligence*. [en línea], disponible en: <https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf> [consultado el 10/01/2020]; ROGEL VIDE, C., “Robots y personas” en ROGEL VIDE, C. (Ed.), *Los robots y el Derecho* Madrid, Reus, 2018, p. 9.

intervención humana⁵⁵. Esta preocupación se funda por una parte en que la eventual presencia de sesgos o errores en los sistemas puede afectar derechos fundamentales, tales como el derecho a la igualdad y no discriminación; y, por otra parte, en la posibilidad de que se vulneren derechos como los de privacidad y protección de datos personales, entre otros⁵⁶.

Piénsese que, en febrero de 2020, la Corte del Distrito de La Haya prohibió el uso del algoritmo SyRI (*System Risk Indication*), utilizado por el gobierno de Países Bajos para determinar qué ciudadanos son supuestamente más proclives a defraudar al Estado. SyRI es un sistema de indicación de riesgos que comparaba bases de datos de pensiones, seguros, tipo de casa, impuestos, multas, integración, deudas, ingresos o subsidios de empleo para determinar quiénes son probables defraudadores. En su sentencia, la Corte consideró que aunque es lícito utilizar este tipo de instrumentos (si existe un interés público que lo justifique y si se toman las medidas adecuadas para garantizar la mínima injerencia necesaria en el derecho a la privacidad), la implementación de SyRI no ofrece garantías suficientes como para considerar que este sistema en concreto respetaba el necesario juicio de proporcionalidad que debe superar toda injerencia en la privacidad de acuerdo con el artículo 8 del Convenio Europeo de Derechos Humanos (CEDH)⁵⁷.

Otro caso llamativo ocurrió en torno al sistema informático COMPAS comercializado por la compañía Northpointe. Esta herramienta de IA utilizada por tribunales estadounidenses evalúa la probabilidad de reincidencia de un convicto (la que condiciona el otorgamiento de la libertad condicional). El algoritmo, luego de revisar 137 parámetros distintos del sujeto, determina sus posibilidades de reincidir en el futuro. Aunque el modelo no utiliza la raza del sujeto en su evaluación, sí considera otros criterios sesgados, como su código postal de residencia que conllevan a resultados racistas. Su objetividad estuvo en entredicho cuando se descubrió que tenía un sesgo racista que le hacía equivocarse especialmente en contra de personas de raza negra⁵⁸.

55 Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, 2017, Grupo de Trabajo sobre Protección de Datos del Artículo 29, p. 8.

56 MALIK, M., "Can algorithms themselves be biased?" [en línea], disponible en: <https://medium.com/berkman-klein-center/can-algorithms-themselves-be-biased-cffecbf2302c> [consultado el 19/02/2020]; Access Now, *Human Rights*, cit.; O'Neil (2016); MAYER-SCHÖNBERGER, V. & CUKIER, K., *The Dictatorship of Data*. [en línea] *MIT Technology Review*, disponible en: <https://www.technologyreview.com/s/514591/the-dictatorship-of-data/> [consultado el 19/02/2020].

57 FERRER, I., "Países Bajos veta un algoritmo acusado de estigmatizar a los más desfavorecidos" [en línea], disponible en: https://elpais.com/tecnologia/2020/02/12/actualidad/1581512850_757564.html [consultado el 19/02/2020]. Un análisis sobre este caso puede verse en el trabajo de LAZCOZ MORATINOS, G., & CASTILLO PARRILLA, J., "Valoración algorítmica ante los derechos humanos y el Reglamento General de Protección de Datos: el caso SyRI." *Revista Chilena de Derecho y Tecnología*, 9(1), 2020, pp. 207-225. doi:10.5354/0719-2584.2020.56843.

58 ANGWIN *et al.*, *Machine Bias*, cit.

En otro orden de ideas, desde la perspectiva privada, preocupan aquellas empresas que basan su modelo de negocios en la realización de perfiles de sus usuarios (*profiling*). Ello supone un tratamiento automatizado de datos personales que consiste en utilizarlos para evaluar aspectos de la persona, analizar o predecir sus intereses, comportamientos y otros atributos⁵⁹. El perfilamiento puede ser parte de un proceso automatizado de toma de decisiones, pero puede incluso inducir comportamientos. Por lo tanto, podría resultar lesivo de varios derechos fundamentales, así que se requiere del ordenamiento jurídico medidas preventivas y correctivas.

Los casos descritos, aunque con sus particularidades, plantean problemas globales y transversales que preocupan a los juristas a nivel mundial y Chile no es la excepción⁶⁰. En particular, estas situaciones dejan de manifiesto la importancia de definir cuál es la perspectiva que corresponde asumir frente a las consecuencias del uso de algoritmos de IA tanto en el ámbito público como en el privado: ¿autorregulación, heterorregulación o corregulación?⁶¹. Tomar una u otra vía requiere de diversos análisis. En todo caso, con carácter general, la ética de la IA busca proteger valores esenciales, como la dignidad, la libertad, la democracia, la igualdad, la autonomía de las personas y la justicia frente a los razonamientos mecánicos⁶². Pero a pesar del gran componente ético del debate, no debe perderse de vista que las soluciones debería aportarlas el Derecho, por lo que es urgente la regulación normativa de la IA, la cual deberá atender, entre muchas otras, a las consideraciones aquí señaladas⁶³.

B) TENSIONES ENTRE LA TRANSPARENCIA ALGORÍTMICA Y LA PROPIEDAD INTELECTUAL E INDUSTRIAL

Frente al aumento en la toma de decisiones automatizadas y el surgimiento de problemas y dilemas éticos como los señalados en el epígrafe anterior, la transparencia y explicabilidad de los algoritmos se imponen a nivel mundial como alternativas para promover la confianza y garantizar particularmente la privacidad y protección de datos personales. Sin embargo, desde la perspectiva de la propiedad intelectual e industrial una “IA transparente” puede plantear más de un problema si no se fijan expresamente ciertos criterios y se repiensen algunos aspectos contenidos en los sistemas tradicionales todavía vigentes.

59 Artículo 4 número 4 del Reglamento (UE) 2016/679, General sobre la Protección de Datos.

60 Téngase en cuenta, además, que el uso sistemas sesgados puede resultar contrario a la Ley 20.609, que establece medidas contra la discriminación.

61 HAGEMANN R. y LECLERC J., *Inteligencia artificial: un equilibrio entre la regulación y la autorregulación*. [en línea], disponible en: <https://www.ibm.com/blogs/policy/latin-america/2020/01/22/inteligencia-artificial-un-equilibrio-entre-la-regulacion-y-la-autorregulacion/> [consultado el 04/03/2020].

62 Agencia Española de Protección de Datos, “Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción” [en línea], disponible en <https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf> [consultado el 28/02/2020].

63 ROGEL, *Robots y personas*, cit. p. 23.

Para entender con precisión las tensiones que se generan entre la PI y la transparencia, piénsese, por ejemplo, en un programa informático que contiene un algoritmo de IA utilizado para realizar el proceso de selección universitaria, que decide quiénes ingresan o no a una determinada institución. Los estudiantes sometidos a él deben proporcionar información y datos de carácter personal y se someterán a una decisión que afectará su proyección profesional. De esta forma, estarían interesados en saber que están siendo sometidos a dicha evaluación, también si el programa tiene problemas de seguridad, si está bien desarrollado, cómo funciona, qué criterios se supone que aplica (y si efectivamente el programa los aplica), qué procedimientos se tienen en cuenta para realizar tal selección y si realmente estos son justos; todo lo cual puede requerir algo más que una simple explicación.

En ese caso, un problema con la PI se planteará si, por ejemplo, para dar transparencia al funcionamiento del algoritmo, se solicita acceso al código fuente y una copia del programa. En primer lugar, porque como se ha dicho, de acuerdo con la ley de propiedad intelectual, en diversos ordenamientos ocurrirá que los programas computacionales son considerados obras originales, cualquiera que sea el modo o forma de expresión, y esto incluye el programa fuente o programa objeto (e incluso la documentación preparatoria, su descripción técnica y manuales de uso). Así que, en principio, incluso si el programa está en poder de la Administración Pública, bajo la vigencia de tales normas dicho acceso tendría que ser denegado si el titular del derecho intelectual no consiente en ello por estar protegido por el sistema de derecho de autor (a menos que exista una limitación o excepción expresa en la ley). En segundo lugar, porque revelar el código fuente implica revelar el algoritmo que, se ha dicho, normalmente es secreto y su divulgación puede generar pérdidas económicas a su titular, así como la pérdida de su derecho.

A este respecto, no existe en la legislación de propiedad intelectual chilena una norma que resuelva una situación como la planteada o que contenga una excepción que facilite el acceso a algún órgano de la Administración Pública en casos determinados. Adicionalmente, aunque en Chile se discute un proyecto de ley que perfecciona tres cuerpos legales en materia de propiedad industrial⁶⁴ (incluyendo precisamente a la Ley 19.039, al Código Procesal Penal y la Ley 20.254, que crea el Instituto Nacional de Propiedad Industrial), en lo que se refiere a los secretos empresariales se proponen ajustes a la definición, pero no se contempla tampoco la posibilidad de incluir un régimen de limitaciones y excepciones o normas relativas al acceso de la Administración Pública. La competencia excepcional expresa para acceder al secreto resultaría conveniente, pues en ocasiones es necesario ponderar si deben prevalecer los derechos e intereses económicos que el secreto empresarial protege, o los relacionados con el acceso a la información que se requiere, ya que, como se ha visto, puede ocurrir que se haga abuso del derecho mismo o que con el secreto se vulneren algunos derechos fundamentales⁶⁵.

64 Boletín 12135.

65 ELSAYED-ALI. S., *Artificial intelligence: how it impacts human rights and what we*

Como puede verse, el complejo fenómeno de la IA va haciendo cada vez más necesario fijar algunos nuevos criterios en diversas áreas del Derecho y también en el Derecho de propiedad intelectual e industrial. De hecho, esta necesidad ya fue advertida por la Organización Mundial de la Propiedad Intelectual (OMPI), la cual llamó a sus Estados miembros y a terceras partes interesadas a debatir en relación con el impacto de la IA sobre la propiedad intelectual y a formular colectivamente preguntas que coadyuven en la generación de nuevas políticas en el área, encontrándose entre otros temas de análisis, los relativos a la propiedad intelectual sobre los algoritmos y los secretos empresariales⁶⁶.

IV. ALGUNAS SOLUCIONES

A) TENDENCIAS EN LA UNIÓN EUROPEA: LA SOLUCIÓN EN EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

Descrito el panorama anterior se ha podido observar que, con el uso de sistemas de IA, es posible que se capten, traten y almacenen datos personales para la toma de ciertas decisiones automatizadas y otras muy diversas aplicaciones. En ese sentido, en el área específica de la protección de datos personales la tendencia es que las empresas tecnológicas deban cumplir con ciertos estándares, derivados de nuevas categorías de derechos.

Así, en la Unión Europea se ha desarrollado un cuerpo de documentos, resoluciones, declaraciones, reglamentos y directivas encaminadas a la protección de los datos personales desde una perspectiva de derechos fundamentales, que se espera que vaya trasladándose a las legislaciones de los Estados miembros, aunque en ciertos casos sus efectos puedan extenderse incluso fuera de la Unión. Entre los mencionados documentos destacan: la Resolución del Parlamento Europeo, de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (Resolución sobre macrodatos), y el Reglamento (UE) 2016/679, General sobre la Protección de Datos, GDPR, por sus siglas en inglés.

En el marco de ellos, se propugna “la responsabilidad y la transparencia algorítmica”⁶⁷. Y, en virtud del GDPR, se proponen los más elevados estándares de

should do about it. [en línea], disponible en: <https://medium.com/@sherifea/the-impact-of-artificial-intelligence-on-human-rights-problems-and-solutions-fd52d1ac2158> [consultado el 04/03/2020]; Ureña, R., “Autoridad algorítmica: ¿cómo empezar a pensar la protección de los derechos humanos en la era del “big data”?”, *Latin American Law Review*, 2, 2019, 99-124. doi.org/10.29263/lar02.2019.05.

⁶⁶ Organización Mundial de la Propiedad Intelectual (OMPI), *Draft Issues Paper on Intellectual Property Policy and Artificial Intelligence*. [en línea], disponible en: https://www.wipo.int/meetings/en/doc_details.jsp?doc_id=470053 [consultado el 18/05/2020]; Por Chile véase: Organización Mundial de la Propiedad Intelectual (OMPI), “Public Consultation on AI and IP Policy - Submissions. Query: Chile”, [en línea], disponible en: https://www.wipo.int/about-ip/en/artificial_intelligence/submissions- [consultado el 18/05/2020].

⁶⁷ Parlamento Europeo, Resolución de 14 de marzo de 2017, sobre las implicacio-

protección de datos personales desde la fase de diseño que deben cumplir tanto instituciones públicas como privadas⁶⁸. En ese contexto, los procesos de aprendizaje automático deben hacerse confiables⁶⁹ y transparentes si involucran tratamiento de datos personales. A partir de los mencionados instrumentos es que se plantea que está por nacer (o ha nacido) un nuevo “derecho a la transparencia algorítmico”⁷⁰. Derecho que consistiría en explicar a las personas cómo se usan sus datos por los algoritmos, y cuáles son los pasos para la toma de las decisiones automatizadas.

En relación con ello, la Resolución sobre macrodatos insta a que las autoridades de protección de datos evalúen de manera específica la necesidad, no solo de transparencia algorítmica, sino también de transparencia en relación con posibles sesgos en los datos de capacitación (macrodatos) utilizados por los algoritmos de IA para hacer inferencias. Asimismo, recomienda que las empresas realicen evaluaciones periódicas sobre la representatividad de los conjuntos de datos, que consideren si los conjuntos de datos se ven afectados por elementos sesgados, y que desarrollen estrategias para superarlos; y pone de relieve la necesidad de examinar la exactitud e importancia de las predicciones basadas en el análisis de los datos teniendo presente las preocupaciones éticas y la equidad⁷¹.

Por su parte, el GDPR, para hacer frente a algunos de los dilemas éticos previamente mencionados, establece el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado (salvo excepciones). Y, asimismo, en su artículo 22 se dispone que “todo interesado tendrá 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”. Esta oposición no se aplicará si a) el tratamiento es necesario para la celebración o ejecución de un contrato, b) el tratamiento se encuentra autorizado por el Derecho de la Unión o de los Estados miembros y c) si se basa en el consentimiento explícito del interesado.

nes de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI)), considerando N; considerando general 1 y 21.

68 MARTÍNEZ MARTÍNEZ, R., “Designing artificial intelligence. Challenges and strategies for achieving regulatory compliance”, en *Revista Catalana de Dret Públic*, 58, 2019, 64-81. <https://doi.org/10.2436/rcdp.i58.2019.3317>.

69 En efecto, la Comisión Europea trabaja en la definición de una Inteligencia Artificial confiable, y establece que ella ha de cumplir con siete requisitos clave: acción y supervisión humanas, solidez técnica y seguridad, gestión de la privacidad y los datos, transparencia, diversidad, no discriminación y equidad, bienestar social y ambiental y rendición de cuentas. Comisión europea, “Directrices éticas para una IA fiable. Grupo de expertos de alto nivel sobre inteligencia artificial” [en línea], disponible en: <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top> [consultado el 27/02/2020]; Comisión europea, “White paper on Artificial Intelligence - A European approach to excellence and trust” [en línea], disponible en: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf [consultado el 28/02/2020].

70 COTINO, *Big data*, cit. p. 142; Arellano, *El derecho a la transparencia algorítmica*, cit., p. 4.

71 Parlamento Europeo, *Resolución sobre macrodatos*, cit. cons. general 21.

En todo caso, el responsable del tratamiento está obligado en los casos a) y c) a adoptar las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado. Esto incluye el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

Igualmente, en el considerando 71 se establece que el titular tiene derecho “a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión”. Esto implica, por ejemplo, que cuando a una persona se le niega el acceso a una universidad o institución educativa porque así lo ha decidido o recomendado un algoritmo, esa persona debe tener derecho a que se le explique cuáles han sido las variables que han hecho que se tome esa decisión. Sin embargo, en lo que interesa a esta investigación, no queda claro cuál es el alcance de dicha explicación si ella conllevase la revelación de un secreto empresarial, lo cual podría ser resuelto por las respectivas legislaciones nacionales.

En otro orden de ideas, también conforme al GDPR es imperativo no confiar únicamente en las manifestaciones de los fabricantes y distribuidores para garantizar la transparencia del algoritmo o sistema de IA, sino que obligatoriamente se establecen mecanismos basados en terceros confiables para determinar los niveles necesarios de calidad y confiabilidad. Estos mecanismos se materializan ya sea dando acceso a las autoridades de control a los aspectos internos de los sistemas de IA, o bien estableciendo mecanismos de certificación por terceros independientes.

De esta forma, en el marco del GDPR se propone el desarrollo y aplicación de esquemas de certificación que establezcan marcos de referencia (para fabricantes, responsables, autoridades y usuarios) a través de los cuales se acredite por un tercero independiente qué tanto el sistema de IA cumple con el principio de transparencia. En ese sentido, en el artículo 42 del GDPR se contempla la posibilidad de desarrollar mecanismos de certificación específicos en materia de protección de datos y de sellos y marcas de protección de datos como herramientas para demostrar su cumplimiento. Tal y como explica el Considerando 100, los mecanismos de certificación sirven igualmente para aumentar la transparencia en los tratamientos de datos de carácter personal⁷².

En ese sentido, esta alternativa que, en definitiva, propone la adopción de un sistema sustentado en la autorregulación o corregulación, y requeriría la adecuación a unos requisitos técnicos concretos⁷³, tiene como gran ventaja que permitiría el resguardo de derechos a la protección de datos personales sin que ello implique necesariamente la divulgación del secreto empresarial protegido, situación que

72 Agencia Española de Protección de Datos, *Adecuación al RGPD*, cit., p. 34.

73 VIGURI CORDERO, J., “La implementación de nuevos esquemas de certificación en la UE como garantía de protección de los derechos fundamentales de consumidores y usuarios (especial referencia a la protección de datos personales)”, *Revista CESCO de Derecho de Consumo*, n.º 19, 2016, pp. 28-40, [en línea], disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=5807262> [consultado el 10/01/2020].

ocurriría muy excepcionalmente, pues el sistema habría sido previamente certificado para poder utilizarse.

Sin embargo, debe destacarse que este régimen solo se aplicará en relación con la protección de datos personales (lo que lleva a concluir lógicamente que habrá situaciones que queden fuera de su amparo) y que este a su vez se ha sostenido sobre un modelo de consentimiento que algunos afirman que está quebrado y no es sostenible frente a la complejidad del contexto tecnológico de la IA⁷⁴.

En efecto, en lo que se contrae a esta investigación, aunque el GDPR ofrece un elevado estándar en materia de protección de datos personales, y a pesar de que su aplicación pretende “acompañar” a los datos personales si se exportan al extranjero⁷⁵, puede ocurrir que otros derechos fundamentales que entren en conflicto con un sistema de IA protegido por un secreto empresarial u otros derechos de PI queden fuera de su marco y no encuentren solución en la legislación actual si no se articulan medidas adicionales en las legislaciones nacionales dentro y fuera de la Unión Europea⁷⁶.

Por eso, en el Derecho anglosajón (en el que también se busca prevenir que las máquinas y, principalmente, los sistemas de aprendizaje automático tengan la capacidad de discriminar o violar los Derechos Humanos⁷⁷), se han propuesto otras alternativas, como realizar auditorías por terceros independientes a los algoritmos⁷⁸ y, algunas más tecnológicas, como el uso de herramientas de software para detectar y/o mitigar los sesgos en los algoritmos. Es decir, usar algoritmos que “auditen” a otros algoritmos⁷⁹.

74 RUBINSTEIN, I., “Big Data: The End of Privacy or a New Beginning?”, en *International Data Privacy Law, NYU School of Law, Public Law Research Paper*, 2013, 12-56. SSRN; Solove, D., “Autogestión de la privacidad y el dilema del consentimiento”, *Revista Chilena de Derecho y Tecnología*, 2(2), 2013, 11-47. doi:10.5354/0719-2584.2013.30308.

75 Como se desprende del contenido del Capítulo v del GDPR, cuando los datos personales se transfieren fuera de la Unión Europea, la protección ofrecida por él acompañará a los datos y solo puede tener lugar con arreglo a ciertas condiciones ahí previstas. Esto quiere decir que si los datos se exportan al extranjero, la empresa debe garantizar que se cumpla una de las siguientes condiciones: a) La protección de datos del país no miembro de la Unión Europea se considera adecuada; b) La empresa toma las medidas necesarias para proporcionar las oportunas salvaguardias, como la inclusión de cláusulas específicas en el contrato celebrado con el importador no europeo de los datos personales, o c) La empresa se basa en motivos específicos para la transferencia (excepciones), como el consentimiento del interesado. Al respecto véase a: USTARÁN, E. & GARCÍA, P., “Transferencias internacionales de datos”, en Rallo Lombarte, A. (Dir.), *Tratado de Protección de Datos*. Tirant lo Blanch, 2019, pp. 459-490.

76 COTINO, *Big data*, cit., p. 146.

77 Por ejemplo véase la Declaración de Toronto, “The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems” [en línea], disponible en: <https://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems/> [consultado el 28/02/2020].

78 GUSZCZA, J.; RAHWAN, I.; BIBLE, W.; CEBRIAN, M. & KATYAL, V., “Why We Need to Audit Algorithms”, [en línea], *Harvard Business Review*, 2018, disponible en: <https://hbr.org/2018/11/why-we-need-to-audit-algorithms> [consultado el 04/03/2020].

79 LOMAS, N., “IBM launches cloud tool to detect AI bias and explain automated decisions” [en línea], disponible en: <https://techcrunch.com/2018/09/19/ibm-launches-cloud-tool-to-detect-ai-bias-and-explain-automated-decisions/> [consultado el 19/02/2020]; Chowdhury, R. & Mulani, N., “Auditing Algorithms for Bias”, [en línea], disponible

B) PERSPECTIVAS PARA CHILE

En Chile, a pesar de la existencia de la alguna vez pionera (hoy muy cuestionada) Ley sobre Protección de la Vida Privada (Ley 19.628), no es sino desde el 16 de junio de 2018, que la protección de los datos personales tiene indudable rango constitucional, en virtud de la publicación de la Ley n.º 21.096 que lo consagra como un derecho autónomo, hoy establecido en el artículo 19 n.º 4 de la Constitución Política. En ese sentido, la Ley 19.628 establece el marco jurídico aplicable a la protección de datos personales desde el año 1999, lo que significa que este nació mucho tiempo antes del reconocimiento constitucional del mencionado derecho y en una época en la que no existían muchos de los dilemas que hoy plantea el uso de sistemas y algoritmos de IA.

En efecto, debido a una serie de carencias e insuficiencias que desde hace algunos años se atribuyen a la mencionada ley, está en discusión el Proyecto de Ley que Regula la Protección y el Tratamiento de los Datos Personales y crea la Agencia de Protección de Datos Personales⁸⁰, que entre otras cosas busca modificar sustancialmente los desaciertos de la Ley 19.628 para estar al nivel de los estándares internacionales en materia de protección de datos personales. Los aludidos problemas pueden sintetizarse en: la falta de un órgano administrativo fiscalizador, la inexistencia de un procedimiento de reclamo idóneo, la ausencia de infracciones y sanciones efectivas, así como la inexistente regulación para la transferencia internacional de datos, entre otros⁸¹; asuntos que de alguna manera sí están resueltos en el GDPR.

en: <https://hbr.org/2018/10/auditing-algorithms-for-bias> [consultado el 28/02/2020]; Clarke, L., "IBM's AI toolkit will help developers fight bias in AI", [en línea] disponible en: <https://www.techworld.com/developers/how-ibms-ai-toolkit-will-help-developers-fight-bias-in-ai-3686831/> [consultado el 28/02/2020].

80 Boletines 11.144 y 11.092, refundido.

81 Sobre las reiteradas críticas que se han venido realizando desde su entrada en vigor pueden consultarse los trabajos de: VERGARA, M., "Chile: Comentarios preliminares al proyecto de ley que regula la protección y tratamiento de datos personales y crea la Agencia de Protección de Datos Personales", en *Revista Chilena de Derecho y Tecnología*, 6(2), 2017, pp. 135-152. doi:10.5354/0719-2584.2017.45822; VIOLIER, P., "El Estado de la Protección de Datos Personales en Chile. Derechos Digitales" [en línea], disponible en: <https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf> [consultado el 15/01/2020]; De la Maza, I. y Momberg, R., "Términos y condiciones: acerca del supuesto carácter contractual de las autorizaciones para el tratamiento de datos personales en sitios web", en *Revista Chilena de Derecho y Tecnología*, 6(2), 2017, pp. 25-55. doi:10.5354/0719-2584.2017.46226; ÁLVAREZ VALENZUELA, D., "Acceso a la información pública y protección de datos personales. ¿Puede el consejo para la transparencia ser la autoridad de control en materia de protección de datos?", en *Revista de Derecho Universidad Católica del Norte*, Año 23, n.º 1, 2016, pp. 51-79; VELASCO, P. & VIOLIER, P., "Información financiera y discriminación laboral en Chile: un caso de estudio sobre Big Data. *Derechos Digitales*" [en línea], disponible en: <https://www.derechosdigitales.org/wp-content/uploads/big-data-informe.pdf> [consultado el 26/02/2020]; MATUS, J., "Derecho de acceso a la información pública y protección de datos personales", *Revista Chilena de Derecho y Tecnología*, 2(1), 2013, 197-228. doi:10.5354/0719-2584.2013.26959; CERDA SILVA, A., "Legislación sobre protección de las personas frente al tratamiento de datos personales." *Centro de Estudios en Derecho Informático*, Universidad de Chile, 2012.

Adicionalmente, y en lo que se relaciona con esta investigación, debe señalarse que la Ley 19.628 no contiene disposiciones que regulen la creación de perfiles y la toma de decisiones automatizadas, o que se refiera expresamente a la transparencia algorítmica. Además, a falta de institucionalidad o de una entidad administrativa, autoridad u órgano responsable de la protección de datos personales, tampoco existe una competencia para tener acceso a secretos empresariales cuando estos estén asociados al uso de algoritmos que afecten derechos fundamentales.

La única mención cercana a una regulación sobre decisiones automatizadas es la contenida en el artículo 2 literal o) de acuerdo con el cual se entenderá por tratamiento de datos cualquier operación o complejo de operaciones o procedimientos técnicos “*de carácter automatizado o no*, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma” (destacado fuera del original).

Por eso no existe claridad, por ejemplo, en cuanto al estándar de protección que corresponde a los datos que arroje un perfil. Ni en cuanto a los derechos o mecanismos de impugnación que podrían tener las personas objeto de toma de decisiones automatizadas ¿Cómo se toman estas decisiones?, ¿deben explicarse?, ¿qué tipo de explicación sería válida y suficiente?, ¿quiénes estarían legitimados para exigirla? Tampoco queda claro ¿qué obligaciones adicionales deben cumplir quienes realicen toma de decisiones automatizadas?, ¿en qué casos podrían eximirse de ellas? Si la explicación no fuera suficiente, ¿cómo?, ¿cuándo?, ¿por qué y en qué medida se puede acceder a algoritmos protegidos por secretos empresariales u otras formas de PI?⁸². ¿La respuesta sería distinta si el algoritmo lo usa un ente público?, ¿son suficientes el derecho a desarrollar cualquier actividad económica, la autonomía de la voluntad y la disponibilidad de un derecho, para fundamentar la falta de transparencia en el uso de un algoritmo en el ámbito privado?, ¿es la transparencia un límite al secreto empresarial o el secreto empresarial un límite a la transparencia?

A este respecto, el Proyecto de Ley que Regula la Protección y el Tratamiento de los Datos Personales y crea la Agencia de Protección de Datos Personales, además de contener una definición de la creación de perfiles (artículo 2º letra w), establece en su artículo 8 bis, el que vendría a ser un derecho a oponerse a valoraciones personales automatizadas y elaboración de perfiles (salvo excepciones). La redacción de ambas normas se encuentra inspirada casi íntegramente en el GDPR. No obstante, todavía no es Derecho positivo en Chile y es probable que cuando lo sea, también resulte insuficiente si no se articula con la legislación de PI, a través del establecimiento de nuevos límites y excepciones hasta ahora no contemplados en dicho régimen jurídico especial.

82 COTINO, *Big data*, cit., p. 142.

Estos límites y excepciones podrían dar respuesta a la pregunta sobre cuándo, quién y en qué medida podría acceder a algoritmos protegidos por secretos empresariales u otras formas de PI. Además, podrían facilitar el cumplimiento del régimen relativo a la transferencia de datos fuera de la Unión Europea contenido en el Capítulo V del GDPR, en la medida en que todos los países que ofrecen productos y servicios a los ciudadanos de la Unión Europea deben cumplir con sus postulados; por ende, Chile también debe observar estas normas pese a no ser miembro de la Unión.

Lo anterior es particularmente importante porque, aunque conforme a la Ley 20.285, sobre acceso a la información pública, los organismos públicos tienen el deber de recibir solicitudes de información y entregar esta, podrán abstenerse de aquello cuando exista un motivo de secreto o reserva. En ese sentido, conforme al artículo 21 n.º 2, se podrá denegar total o parcialmente el acceso a la información “cuando su publicidad, comunicación o conocimiento afecte los derechos de las personas, particularmente tratándose de su seguridad, su salud, la esfera de su vida privada o derechos de carácter comercial o económico”. En este último supuesto se incluyen los secretos empresariales (en los casos en que efectivamente lo sean) y por tanto su revelación afecte a su titular. Recuérdese además que, como se señaló, sobre la base de lo dispuesto en su artículo 19 n.º 25, la Constitución Política protege también a los secretos empresariales. En todo caso es destacable lo paradójico que resulta que precisamente la norma que exceptúa el acceso por la existencia de derechos de carácter comercial o económico es la que busca proteger también la vida privada.

Ahora bien, de acuerdo con la jurisprudencia del Consejo para la Transparencia para denegar el acceso en virtud de la citada norma, se requiere determinar la afectación a los bienes jurídicos protegidos por las causales de reserva o secreto de la información. Para ello, en primer lugar, es necesario no solo que la información de que se trate concierna a las materias sobre las que estos versan, sino que además su publicidad debe dañarlos o afectarlos negativamente en alguna magnitud y con alguna especificidad que debe determinarse, daño que no cabe presumir, sino que debe acreditarse por los órganos administrativos o terceros, que tiene alguna probabilidad de ocurrir, empleándose el denominado “test de daño”⁸³.

Esto implica que, en Chile, en el ámbito público, conforme a la legislación vigente, la protección de los secretos empresariales opera como un límite a la transparencia y no a la inversa, como es tendencia a nivel mundial. Y esto resulta preocupante porque, como se ha visto en el contexto de la complejidad del fenómeno IA, en algunas ocasiones se podrían vulnerar otros derechos que también gozan de rango constitucional, como el derecho a la igualdad y no discriminación,

83 Consejo para la Transparencia, 14 de octubre de 2011, Decisión amparo Rol C428-11; Consejo para la Transparencia, 17 de noviembre de 2017, Decisión amparo Rol C2727-17.

la privacidad y el derecho a la protección de datos personales, por solo mencionar algunos.

En todo caso, los derechos de PI son derechos subjetivos que, aunque reconocidos y protegidos por la Constitución, deben tener límites frente a determinadas situaciones, como cualquier otro en una sociedad democrática. Dichos límites deben implicar que el legislador evite que a través de los privilegios reconocidos se abuse del derecho en perjuicio de terceros. Es por lo que, en mérito de circunstancias debidamente fundadas y justificadas, como puede ser precisamente la colisión con otros derechos constitucionalmente protegidos, tanto en el sistema de derecho de autor como en el sistema de patentes se admiten ciertos límites y excepciones. La dificultad de instaurarlos en relación con los secretos empresariales estará en garantizar que la Administración Pública o los terceros autorizados por ley mantengan la reserva de la información a la que acceden para no disminuir las ventajas competitivas en aquellos sistemas que en definitiva resulten justos y legales.

CONCLUSIONES

En el uso de los sistemas de IA juega un papel fundamental el algoritmo. Este toma decisiones o sirve de instrumento para ello, y se utiliza también para crear perfiles o dirigir comportamientos e influir en determinados sucesos y resultados. La posible presencia de sesgos y otros tipos de errores en el uso de algoritmos de IA se ha convertido en una preocupación que requiere que el Derecho como disciplina científica y la legislación aporten soluciones, por eso la tendencia a nivel internacional es a exigir transparencia. Aunque el alcance de este término todavía no es muy preciso, ella se traduce en explicar a las personas cómo funcionan los algoritmos y cuáles son los pasos para la toma de las decisiones automatizadas.

En lo que se refiere a la propiedad intelectual e industrial, la existencia de regímenes anteriores a los desarrollos actuales puede hacer difícil que la transparencia se garantice en algunos casos. En particular, cuando se estime necesario develar secretos empresariales para garantizar la protección de otros derechos. De manera que, para lograr una IA y algoritmos transparentes, debe contarse con mecanismos jurídicos adicionales, y un sistema articulado que, además de disminuir la litigiosidad y facilitar el cumplimiento de compromisos internacionales, permita fundamentar qué se entiende como una explicación suficiente pero también cómo, cuándo, por qué y en qué medida se podría acceder excepcionalmente a algoritmos protegidos por secretos empresariales u otras formas de PI (o bien, cómo suplir la falta de dicho acceso). Y, asimismo, cómo han de diseñarse los sistemas de IA en adelante de acuerdo con los nuevos estándares de la cuarta revolución industrial para que puedan ser utilizados de forma justa y legal sin afectar derechos fundamentales. Delimitando las fronteras de lo público y lo privado si es que esto fuera necesario.

En ese contexto resultan de interés los avances que se han planteado en el Derecho europeo por los elevados estándares que ofrece específicamente en materia

de protección de datos personales, cuyos alcances, aunque territoriales y acotados, podrían extenderse a otras situaciones que van más allá de este marco. En él se han reconocido nuevos derechos asociados al entorno digital, y en particular, el derecho a la transparencia algorítmica que, vinculado con la protección de datos personales, subyace a diversos instrumentos de la Unión Europea. Sin embargo, dado que su contenido y alcance apenas comienzan a dibujarse, los desafíos son múltiples, transversales y globales, así que queda mucho por hacer.

En Chile, a pesar de los avances y de que se acercan algunas soluciones si se aprueba el Proyecto de Ley que Regula la Protección y el Tratamiento de los Datos Personales y crea la Agencia de Protección de Datos Personales, lo cierto es que el marco jurídico actual no ofrece respuestas a las nuevas problemáticas y tensiones planteadas por la IA. De hecho, a pesar de que muchas empresas chilenas mantienen relaciones comerciales como miembros de la Unión Europea, no puede afirmarse que exista en el Derecho positivo chileno un “derecho a la transparencia algorítmica”. Aunque, como se analizó, la realidad la hace cada vez más necesaria. En efecto, si bien el proyecto establece el que vendría a ser un derecho a oponerse a valoraciones personales automatizadas y elaboración de perfiles, es cuestionable que dicha norma por sí sola sea suficiente cuando se generen conflictos con derechos de PI, sobre todo si se tiene en cuenta que en la legislación vigente sobreviven normas conforme a las cuales los secretos empresariales son más bien un límite a la transparencia y no existe una “excepción a la excepción”.

Así que, frente a las preguntas sobre si ¿se puede explicar cómo funciona un algoritmo sin revelar el secreto empresarial que lo protege? O si ¿puede una empresa tecnológica excusarse de explicar cómo funciona un algoritmo o cómo se tomó una decisión automatizada porque este está amparado por un secreto empresarial? En el caso de Chile, conforme a la legislación vigente (especialmente de acuerdo con el artículo 21 n.º 2 de la Ley 20.285), la información y explicación que se suministre no podría implicar revelar el código fuente u objeto (como se ha resuelto en Italia) en la medida en que ello implique a su vez revelar algoritmos protegidos por secretos empresariales siempre que se cumplan las condiciones previamente estudiadas.

En ese sentido, aunque es cierto que los desarrolladores de sistemas de inteligencia artificial pueden –y en algunos casos deben– tomar medidas tecnológicas que hagan posible inferir la forma en la que toman sus decisiones o realizan sus tareas sin que sea necesario revelar el algoritmo si ello no es deseable, no deben descartarse otras posibles soluciones.

Por eso deben examinarse en paralelo otras categorías tradicionales y su adecuación a las nuevas tendencias para establecer nuevos criterios que permitan la protección de los derechos de los individuos, sin que ello implique desincentivar el desarrollo tecnológico ni la innovación o la inversión privada en IA. En ese marco se inserta la revisión a la normativa tradicional de los privilegios y monopolios derivados de los derechos de PI cuando estos entran en pugna con otros derechos fundamentales.

En ese orden de ideas, desde la perspectiva de la PI una de las razones por las cuales los algoritmos son secretos es que no cuentan con un sistema de protección que dé respuesta a sus particularidades; esto implica que aun con sus históricas debilidades el régimen de los secretos empresariales se vislumbra como una de las mejores alternativas para protegerlos. Sin embargo, hay otras medidas que pueden tomarse para hacer compatibles dos regímenes que parecen ser totalmente antagónicos.

En primer lugar, si lo confidencial es contrario a lo transparente, conviene, por una parte, analizar la posibilidad de incluir en los sistemas normativos vigentes algunas disposiciones que flexibilicen la protección de los algoritmos *per se* a través de un régimen especial por el que estos puedan ser públicos, explicables y protegibles frente a la copia, sin que con ello pierdan su valor económico (por ejemplo, facilitando su patentabilidad o un sistema *sui generis* para ellos).

En segundo lugar, conviene fortalecer el régimen especial relativo a los secretos empresariales no solo para incluir un catálogo de límites y excepciones adecuadas a la cuarta revolución industrial, sino también para dotar al sistema de una regulación integral y sistemática que mejore la seguridad jurídica y ofrezca una protección legal adecuada a todos los operadores del mercado.

Y, en tercer lugar, estas u otras medidas pueden complementarse con la adopción de sistemas de certificación por terceros imparciales que, aunque nacidas en el marco de protección de datos personales, lucen como una alternativa exportable a los sistemas de IA en general. En ese sentido, los mecanismos de certificación pueden materializarse dando acceso a determinadas autoridades de control (por ejemplo, autoridades nacionales de protección de datos personales) a los aspectos internos de los sistemas de IA, o bien, estableciendo mecanismos de certificación por terceros independientes, ambos sujetos a estrictas normas de confidencialidad y al cumplimiento de las respectivas normas técnicas.

Además, los sistemas de certificación podrían ser obligatorios o voluntarios. En efecto, un criterio para determinar su obligatoriedad o no, puede fundamentarse en el carácter público o privado de la entidad que pretende hacer uso del sistema de IA, recomendándose siempre la obligatoriedad en el caso de la Administración Pública con pleno sometimiento a principios de derecho administrativo. En todo caso, ya sea que estos mecanismos se implementen en el ámbito público o privado, servirían para garantizar la fiabilidad de los sistemas y la no divulgación de los secretos que protegen a los algoritmos, al tiempo que facilitarían el cumplimiento de las obligaciones internacionales derivadas de la transferencia de datos conforme al GDPR.

Las alternativas aquí esbozadas deberán enfrentarse a una serie de requerimientos y condiciones a las que estos investigadores harán referencia en obra separada. Sin embargo, cabe destacar que los mayores obstáculos para su implementación en el caso de Chile están, por una parte, en la inexistente institucionalidad en materia de protección de datos personales para la resolución de conflictos específicos de

esa naturaleza; y, por otra parte, en la conocida lentitud que conlleva cualquier reforma legislativa.

Mientras tanto, en caso de conflicto de derechos de PI con otros derechos fundamentales que hagan necesario invocar la transparencia algorítmica, la reserva tendrá que ser justificada, probada y fundamentada para que pueda ser mantenida, debiéndose ponderar en cada caso si prevalecen los derechos e intereses protegidos por el secreto empresarial u otros derechos de PI, o los derechos e intereses de quienes requieren que este sea divulgado, labor que corresponderá a los ya muy colapsados tribunales de justicia.

REFERENCIAS

- Access Now, *Human Rights in the age of artificial intelligence*. [en línea], disponible en: <https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf> [consultado el 10 de enero de 2020].
- Agencia Española de Protección de Datos, *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*. [en línea], disponible en <https://www.aepd.es/sites/default/files/2020-02/adequacion-rgpd-ia.pdf> [consultado el 28/02/2020].
- ÁLVAREZ VALENZUELA, D., “Acceso a la información pública y protección de datos personales. ¿Puede el consejo para la transparencia ser la autoridad de control en materia de protección de datos?”, en *Revista de Derecho Universidad Católica del Norte*, Año 23, n.º 1, 2016, pp. 51-79.
- ANGWIN, J.; LARSON, J.; MATTU, S. & KIRCHNER, L., “Machine Bias. There’s software used across the country to predict future criminals. And it’s biased against blacks” [en línea], disponible en: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> [consultado el 10/01/2020].
- ARELLANO TOLEDO, W., “El derecho a la transparencia algorítmica en *Big Data* e inteligencia artificial”, en *Revista General de Derecho Administrativo*, 50, 2019.
- AZUAJE, M. y FINOL, D., “Big Data, algoritmos y propiedad intelectual”, en *Anuario de propiedad intelectual*, n.º. 2016, 2017, pp. 257-275.
- BARRIO, M., “Consideraciones jurídicas acerca del coche autónomo”, en *Actualidad Jurídica (Uría & Menéndez)* Núm. 52, 2019, pp. 101-108.
- BLASS, A., & GUREVICH, Y., “Algorithms: A Quest for Absolute Definitions”, *Bulletin of the European Association for Theoretical Computer Science*, 81, 2003, pp. 195-225.
- BUSS, S.; ALEXANDER, S.; PILLAY, A. & SHORE, R., “The Prospects for Mathematical Logic in the Twenty-First Century”, en *The Bulletin of Symbolic Logic*, 7, 2, 2001, pp. 169-196.
- CARLONI, E., “IA, algoritmos y Administración pública en Italia”, en *Revista de Internet, Derecho y Política*, 30, 2020, [en línea], disponible en: <https://www>.

- researchgate.net/publication/339633312_IA_algoritmos_y_Administracion_publica_en_Italia [consultado el 28/05/2020].
- CERDA SILVA, A., *Legislación sobre protección de las personas frente al tratamiento de datos personales*, Centro de Estudios en Derecho Informático, Universidad de Chile, 2012.
- CHEN, A., “Inteligencia Artificial: El caso de la IA que intentó patentar dos inventos en su nombre”, en *MIT Technology Review*, [en línea] disponible en: <https://www.technologyreview.es/s/11776/el-caso-de-la-ia-que-intento-patentar-dos-inventos-en-su-nombre> [consultado el 19/08/2020].
- CHOWDHURY, R. & MULANI, N., “Auditing Algorithms for Bias”, [en línea] disponible en: <https://hbr.org/2018/10/auditing-algorithms-for-bias> [consultado el 28/02/2020].
- CLARKE, L., “IBM’s AI toolkit will help developers fight bias in AI”, [en línea], disponible en: <https://www.techworld.com/developers/how-ibms-ai-toolkit-will-help-developers-fight-bias-in-ai-3686831/> [consultado el 28/02/2020].
- Comisión europea, “Directrices éticas para una IA fiable. Grupo de expertos de alto nivel sobre inteligencia artificial” [en línea], disponible en: <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top> [consultado el 27/02/2020].
- Comisión europea, “White paper On Artificial Intelligence - A European approach to excellence and trust” [en línea], disponible en: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf [consultado el 28/02/2020].
- COTINO HUESO, L. “Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales”, *Dilemata*, 24, 2017, [en línea], disponible en: <https://ssrn.com/abstract=3413277> [consultado el 28/02/2020].
- COWGILL, B., “Bias and Productivity in Humans and Machines”, 2019, SSRN: <https://ssrn.com/abstract=3584916> [consultado el 28/02/2020].
- Declaración de Toronto, “The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems” [en línea], disponible en: <https://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems/> [consultado el 28/02/2020].
- DE LA SIERRA, S., “Inteligencia artificial y justicia administrativa: una aproximación desde la teoría del control de la administración pública”, en *Revista General de Derecho Administrativo*, 53, 2020, pp. 1-19.
- DE LA MAZA, I. y MOMBORG, R., “Términos y condiciones: acerca del supuesto carácter contractual de las autorizaciones para el tratamiento de datos personales en sitios web”, en *Revista Chilena de Derecho y Tecnología*, 6(2), 2017, pp. 25-55. DOI:10.5354/0719-2584.2017.46226.

- DOMINGOS, P., *The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World*, New York, Basic Books, 2015.
- ELSAVED-ALI, S., “Artificial intelligence: how it impacts human rights and what we should do about it” [en línea], disponible en: <https://medium.com/@sherifea/the-impact-of-artificial-intelligence-on-human-rights-problems-and-solutions-fd52d1ac2158> [consultado el 04/03/2020].
- ESTEVE PARDO, M., “El secreto profesional y la propiedad intelectual e industrial,” en INAP, *Los límites al derecho de acceso a la información pública*, Madrid, Instituto Nacional de Administración Pública, 2017, pp. 175-183.
- FERRER, I., “Países Bajos veta un algoritmo acusado de estigmatizar a los más desfavorecidos” [en línea], disponible en: https://elpais.com/tecnologia/2020/02/12/actualidad/1581512850_757564.html [consultado el 19/02/2020].
- FUENTES MASSAGUER, J., “De nuevo sobre la protección jurídica de los secretos empresariales (a propósito de la ley 1/2019, de 20 de febrero, de secretos empresariales)”, en *Revista “Actualidad Jurídica Uría Menéndez”*, 51, 2019, pp. 46-70.
- GOLDENBERG, J., “Herramientas del Big Data y del fintech para prevenir y aliviar el sobreendeudamiento del consumidor: una propuesta”, en *Revista chilena de derecho y tecnología* [en línea], vol.8, n.2, 2019, 5-32, disponible en: <http://dx.doi.org/10.5354/0719-2584.2019.54051> [consultado el 19/02/2020].
- GUADAMUZ GONZÁLEZ, A., “Patentabilidad del software: nuevas cuestiones jurídicas”, en *Revista de la OMPI*, 6, 2008, [en línea] disponible en: http://www.wipo.int/wipo_magazine/es/2008/06/ [consultado el 19/02/2020].
- GUREVICH, Y., “What is an Algorithm? (Revised),” en A. Olszewski *et al.* (Eds.) *Church’s Thesis: Logic, Mind and Nature*, Copernicus Center Press, 2014, pp. 1-15.
- GUSZCZA, J.; RAHWAN, I.; BIBLE, W.; CEBRIAN, M. & KATYAL, V., “Why We Need to Audit Algorithms”, en *Harvard Business Review*, 2018, [en línea], disponible en: <https://hbr.org/2018/11/why-we-need-to-audit-algorithms> [consultado el 04/03/2020].
- HAGEMANN R. y LECLERC J., “Inteligencia artificial: un equilibrio entre la regulación y la autorregulación” [en línea], disponible en: <https://www.ibm.com/blogs/policy/latin-america/2020/01/22/inteligencia-artificial-un-equilibrio-entre-la-regulacion-y-la-autorregulacion/> [consultado el 04/03/2020].
- LAMBRECHT, A. & TUCKER, C., “Apparent Algorithmic Bias and Algorithmic Learning”, 2020, SSRN: <https://ssrn.com/abstract=3570076>.
- LAZCOZ MORATINOS, G. y CASTILLO PARRILLA, J., “Valoración algorítmica ante los derechos humanos y el Reglamento General de Protección de Datos: el caso SyRI”, en *Revista Chilena de Derecho y Tecnología*, 9(1), 2020, pp. 207-225. doi:10.5354/0719-2584.2020.56843.
- LISSÉN ARBELOA, J. y GUILLÉN MONJE, P., “Características, alcance de la protección conferida e implicaciones para las empresas en la nueva Ley de Secretos Empresariales”, en *Diario La Ley*, ISSN 1989-6913, 9372, 2019, pp. 1-7.

- LIPSZYC, D., *Derecho de Autor y Derechos Conexos*, Buenos Aires, Unesco, 2002.
- LOMAS, N., “IBM launches cloud tool to detect AI bias and explain automated decisions” [en línea], disponible en: <https://techcrunch.com/2018/09/19/ibm-launches-cloud-tool-to-detect-ai-bias-and-explain-automated-decisions/> [consultado el 19/02/2020].
- LÓPEZ DE MÁNTARAS, R., “¿Hacia una nueva Ilustración? Una década trascendente. El futuro de la IA: hacia inteligencias artificiales realmente inteligentes”, [en línea], disponible en: <https://www.bbvaopenmind.com/articulos/el-futuro-de-la-ia-hacia-inteligencias-artificiales-realmente-inteligentes/> [consultado el 19/02/2020].
- MCCARTHY, J., “What is artificial intelligence?”, [en línea] disponible en: <http://www-formal.stanford.edu/jmc/whatisai/> [consultado el 19/02/2020].
- MALIK, M., “Can algorithms themselves be biased?” [en línea], disponible en: <https://medium.com/berkman-klein-center/can-algorithms-themselves-be-biased-cffecbf2302c> [consultado el 19/02/2020].
- MARTÍNEZ MARTÍNEZ, R., “Designing artificial intelligence. Challenges and strategies for achieving regulatory compliance”, en *Revista Catalana de Dret Públic*, 58, 2019, pp. 64-81. <https://doi.org/10.2436/rcdp.i58.2019.3317>.
- MATUS, J., “Derecho de acceso a la información pública y protección de datos personales”, en *Revista Chilena de Derecho y Tecnología*, 2(1), 2013, pp. 197-228. DOI:10.5354/0719-2584.2013.26959.
- MAYER-SCHÖNBERGER, V., & CUKIER, K., “The Dictatorship of Data”, en *MIT Technology Review*, [en línea] disponible en: <https://www.technologyreview.com/s/1514591/the-dictatorship-of-data/> [consultado el 19/02/2020].
- MITTELSTADT, B.; ALLO, P.; TADDEO, M.; WACHTER, S. & FLORIDI, L., “The Ethics of Algorithms: Mapping the Debate”, *Big Data & Society*. 3(2), 2016, [en línea], disponible en: 10.1177/2053951716679679 [consultado el 26/02/2020].
- MOLINA HERNÁNDEZ, C., “La protección de secretos empresariales”, en Campuzano, A., Palomar Olmeda, A., San Juan y Muñoz, E.; Molina Hernández, C., *La protección de secretos empresariales*, Valencia: Tirant Lo Blanch, 2019, pp. 39-48.
- MONTOYA, A.; PARRADO, E.; SOLÍS, A.; UNDURRAGA, R., *Documento de Trabajo n.º 03/20: Discriminación de género en el mercado de créditos de consumo*. [en línea], disponible en https://www.sbif.cl/sbifweb3/internet/archivos/publicacion_12587.pdf [consultado el 26/02/2020].
- MOSCHOVAKIS, Y., “What is an algorithm?”, en Engquist, B., & Schmid, W. (Eds.) *Mathematics Unlimited — 2001 and beyond, Part II*, Springer, 2001, pp. 919-936.
- MYERS WEST, S.; WHITTAKER, M.; CRAWFORD, K., “Discriminating systems: Gender, Race, and Power in AI” <https://ainowinstitute.org/discriminatingystems.pdf> [consultado el 04/03/2020].

- NAVAS NAVARRO, S., “Derecho e inteligencia artificial desde el diseño”, en Navas Navarro, Susana (coord.), *Inteligencia artificial: tecnología, derecho*, Valencia, Tirant Lo Blanch, 2017, pp. 23-72.
- NAVAS NAVARRO, S., “Obras generadas por algoritmos. En torno a su posible protección jurídica”, en *Revista de Derecho Civil*, vol. v, núm. 2018, pp. 273-291.
- NAVAS NAVARRO, S., “Creación Original e Inteligencia Artificial” en NAVAS NAVARRO, SUSANA (Dir.), *Nuevos desafíos para el Derecho de Autor. Robótica, Inteligencia Artificial, Tecnología*, Madrid, Reus, 2019, pp. 27-45.
- O’NEIL, C., *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, New York, Crown, 2016.
- Organización Mundial de la Propiedad Intelectual (OMPI), “Draft Issues Paper on Intellectual Property Policy and Artificial Intelligence”. [en línea], disponible en: https://www.wipo.int/meetings/en/doc_details.jsp?doc_id=470053 [consultado el 18/05/2020].
- Organización Mundial de la Propiedad Intelectual (OMPI), “Public Consultation on AI and IP Policy - Submissions. Query: Chile”, [en línea], disponible en: https://www.wipo.int/about-ip/en/artificial_intelligence/submissions- [consultado el 18/05/2020].[search.jsp?type_id=&territory_id=36&issue_id=](https://www.wipo.int/about-ip/en/artificial_intelligence/submissions-.search.jsp?type_id=&territory_id=36&issue_id=)
- OTERO GONZÁLEZ, L. y Durán Santomil, P., “Fintech, blockchain y big data”, en García Novoa, César y Santiago Iglesias, Diana (Dir.), *4ª Revolución industrial: impacto de la automatización y la Inteligencia artificial en la Sociedad y la economía digital*, Pamplona, Thomson Reuters Aranzadi, 2018, pp. 81-113.
- Parlamento Europeo, Resolución de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI)).
- PASQUALE, F., *The Black Box Society: The Secret Algorithms That Control Money and Information*, Londres, Harvard University Press, 2015.
- PEÑA TORRES, M., “Protección constitucional del secreto industrial”, en *Revista Chilena de Derecho*, 28, 2, 2001, pp. 413-424.
- PÉREZ SANZ, C., “Aspectos legales del Big Data”, en *Índice: Revista de Estadística y Sociedad*, 68, 2016, pp. 18-21.
- RÍOS RUIZ, W., “Los sistemas de inteligencia artificial y la propiedad intelectual de las obras creadas, producidas o generadas mediante ordenador”, *Revista la propiedad inmaterial*, n.º. 3, 2001, pp. 5-13.
- ROGEL VIDE, C. y SERRANO GÓMEZ, E., *Manual de Derecho de Autor*. Madrid, Reus, 2008.
- ROGEL VIDE, C., “Robots y personas”, en Rogel Vide, C. (Ed.), *Los robots y el Derecho* Madrid, Reus, 2018, pp. 7-23.
- RUSSELL, S. & NORVIG, P., *Artificial intelligence: a modern approach*. Upper Saddle River, N.J.: Prentice Hall, 2010.

- RUBINSTEIN, I., “Big Data: The End of Privacy or a New Beginning?”, en *International Data Privacy Law, NYU School of Law, Public Law Research Paper*, 2013, pp. 12-56. SSRN.
- SEARLE, J., “Minds, brains, and programs”. en *Behavioral and Brain Sciences* 3 (3), 1980, pp. 417-457. DOI: <https://doi.org/10.1017/S0140525X00005756>.
- SCHMITZ VACCARO, C., “Propiedad intelectual, dominio público y equilibrio de intereses”, en *Revista Chilena de Derecho*, vol. 36 n.º 2, 2010, pp. 343-367.
- SCHMITZ VACCARO, C., “Secretos empresariales en Chile: medidas de protección”, en *Revista Internacional Foro de Derecho Mercantil*, 37, 2012, pp. 13-41.
- SOLOVE, D., “Autogestión de la privacidad y el dilema del consentimiento”, en *Revista Chilena de Derecho y Tecnología*, 2(2), 2013, 11-47. DOI:10.5354/0719-2584.2013.30308.
- SUNSTEIN, C., “Algorithms, Correcting Biases”, [en línea], *Forthcoming, Social Research*, 2018, SSRN: <https://ssrn.com/abstract=3300171> [consultado el 26/02/2020].
- UREÑA, R., “Autoridad algorítmica: ¿cómo empezar a pensar la protección de los derechos humanos en la era del “big data”?”, en *Latin American Law Review*, 2, 2019, pp. 99-124. DOI.ORG/10.29263/lar02.2019.05.
- USTARÁN, E. y GARCÍA, P., “Transferencias internacionales de datos”, en Rallo Lombarte, A. (Dir.), *Tratado de Protección de Datos*. Tirant lo Blanch, 2019, pp. 459-490.
- VELASCO, P. y VIOLLIER, P., “Información financiera y discriminación laboral en Chile: un caso de estudio sobre Big Data”, en *Derechos Digitales* [en línea], disponible en: <https://www.derechosdigitales.org/wp-content/uploads/big-data-informe.pdf> [consultado el 26/02/2020].
- VERGARA, M., “Chile: Comentarios preliminares al proyecto de ley que regula la protección y tratamiento de datos personales y crea la Agencia de Protección de Datos Personales”, en *Revista Chilena de Derecho y Tecnología*, 6(2), 2017, pp. 135-152. DOI:10.5354/0719-2584.2017.45822.
- VIGURI CORDERO, J., “La implementación de nuevos esquemas de certificación en la UE como garantía de protección de los derechos fundamentales de consumidores y usuarios (especial referencia a la protección de datos personales)”, en *Revista CESCO de Derecho de Consumo*, n.º 19, 2016, pp. 28-40, [en línea], disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=5807262> [consultado el 10/01/2020].
- VIOLLIER, P., “El Estado de la Protección de Datos Personales en Chile. Derechos Digitales” [en línea], disponible en: <https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf> [consultado el 15/01/2020].
- WACHTER, S., MITTELSTADT, B. & FLORIDI, L., “Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation”, en *International Data Privacy Law*, 2017, SSRN: <https://ssrn.com/abstract=2903469>.

LEGISLACIÓN CITADA

Chile

Decreto Supremo n.º 100 (22/09/2005) Constitución Política de la República de Chile.

Decreto Ley n.º 211 (07/03/2005) Que fija el texto refundido, coordinado y sistematizado del decreto ley n.º 211, de 1973.

Ley 17.336 (02/10/1970) De propiedad intelectual.

Ley 19.039 (25/01/1991) De propiedad Industrial.

Ley 19.628 (28/08/1999) Sobre Protección de la Vida Privada.

Ley 20.285 (20/08/2008) Sobre acceso a la información pública.

Ley 20.609 (24/07/2012) Que establece medidas contra la discriminación.

Ley 21.096 (16/06/2018) Que consagra el derecho a protección de los datos personales.

España

Ley 1/2019 (20/02/2019) de Secretos Empresariales. *Boletín Oficial del Estado* Número 45, de 21 de febrero de 2019.

Organización Mundial del Comercio

Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio. Organización Mundial del Comercio. Disponible en: https://www.wto.org/spanish/docs_s/legal_s/legal_s.htm#TRIPs. Por Chile: Acuerdo de Marrakech por el que se establece la Organización Mundial del Comercio, y los acuerdos anexos que se indican. Decreto Supremo n.º 16, de 1995, del Ministerio de Relaciones Exteriores de Chile, publicado en el *Diario Oficial* n.º 35.169 de 17 de mayo de 1995.

Unión Europea

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) [en línea], disponible en: http://eur-lex.europa.eu/legal-content/ES/TX/T/?uri=uriserv:OJ.L_.2016.119.01.0001.01.SPA&toc=OJ:L:2016:119:TOC [consultado el 15/01/2020].

Directiva (UE) 2016/943, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas, [en línea], disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016L0943> [consultado el 19/09/2019].

Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, 2017, Grupo de Trabajo sobre Protección de Datos del Artículo 29.

JURISPRUDENCIA CITADA

Consejo para la Transparencia, 14 de octubre de 2011, Decisión amparo Rol C428-11.

Consejo para la Transparencia, 17 de noviembre de 2017, Decisión amparo Rol C2727-17.

European Patent Office (EPO), “Grounds for the decision (Annex) Application Nr.18275174.3”, [en línea], disponible en: <https://register.epo.org/application?documentId=E4B63OBI2076498&number=EP18275174&lng=en&npl=false> [consultado el 29/04/2020].

European Patent Office (EPO), “Grounds for the decision (Annex) Application Nr. 18 275 163.6”, [en línea], disponible en: <https://register.epo.org/application?documentId=E4B63SD62191498&number=EP18275163&lng=en&npl=false> [consultado el 29/04/2020].

Intellectual Property Office, 04 de diciembre de 2019, BL O/741/19, [en línea], disponible en: <https://www.ipo.gov.uk/p-challenge-decision-results/o74119.pdf> [consultado el 29/04/2020].