MAXIMILIANO MARZETTI*

ISSN 2665-2714

La regulación de la inteligencia artificial en la Unión Europea

¿Un espejo para América Latina?

DOI: hhttp://dx.doi.org/10.15425/2022.650

Resumen

En este artículo de *status quaestionis* (estado del problema) se analiza la evolución de lo que llamaremos la *Lex Algorithmica* (Ley Algorítmica) de la Unión Europea (UE) en materia de inteligencia artificial, con la es-peranza de animar el debate sobre la materia en América Latina. En la sección 1 se describen los riesgos y oportunidades que representan los sistemas de inteligencia artificial (SIA). En la sección 2 se reseñan distin-tas alternativas para regular los SIA. En la sección 3 se explica el concepto *Estado de derecho algorítmico*. En la sección 4 se analiza el *iter* regulatorio en la UE según la ley positiva existente (*de lege lata*) y la legislación propuesta (*de lege ferenda)*. Se concluye con algunas recomendaciones para los países de América Latina.

Palabras clave

Derecho de la Unión Europea, inteligencia artificial, propiedad intelec-tual, secretos industriales, protección de datos personales, análisis eco-nómico del derecho, derecho comparado, técnica legislativa.

* Doctor en Derecho y Economía (PhD) por la Universidad Erasmo de Róterdam. Profesor de Dere-cho en IESEG School of Management, París, Francia. https://orcid.org/0000-0002-1620-6586. Correo: m.marzetti@ieseg.fr

ANUARIO DE DERECHO PRIVADO 04 – Universidad de los Andes – Facultad de Derecho – pp. 109-135 – DOI: hhttp://dx.doi.org/10.15425/2022.650

The European Union and Artificial Intelligence Regulation

A mirror for Latin America?

Abstract

This status quaestionis article analyzes the evolution of what we will call the *Lex Algorithmica* of the European Union on Artificial Intelligence, in the hope of encouraging the debate on the subject in Latin America. Section 1 describes the risks and opportunities represented by Artificial Intelligence Systems (AIS). Section 2 outlines different alternatives for regulating AIS. Section 3 explains the concept of the Algorithmic Rule of Law. Section 4 analyzes the regulatory *iter* in the EU, *de lege lata* and *de lege ferenda*. We conclude with some recommendations for Latin American countries.

Keywords

European Union law, artificial intelligence, intellectual property, trade secrets, personal data protection, economic analysis of law, comparative law, legislative options.

Introducción: la inteligencia artificial, nuevo paradigma socioeconómico y tecnológico

En este artículo se discurre sobre tecnología y derecho. Cómo la inteligencia artificial (IA) va a modificar nuestras sociedades, de hecho, ya estamos sintiendo algunos de sus efectos, y cómo deberá responder el derecho, regulador de la vida en sociedad, para minimizar sus potenciales externalidades negativas, particularmente las que pueden recaer sobre los sectores de la población más vulnerables, y a la vez maximizar las oportunidades derivadas de las nuevas tecnologías. Como siempre, el hecho social y tecnológico se impone primero, el derecho arriba tarde. El desacople es ya evidente, especialmente en América Latina. Por tal razón se sugiere como espejo la experiencia regulatoria de la Unión Europea (UE) en la materia que, si bien puede parecer lejana, es también cercana desde una perspectiva de cultura jurídica (en su mayoría, los países miembros de la UE pertenecen a la tradición jurídica romanista, los valores sociales en ambas regiones son similares, así como sus lenguas oficiales).

Cuando hablamos de IA, término cuya creación se atribuye a John McCarthy[1], nos referimos a sistemas informáticos que imitan procesos cognitivos similares a los de los seres humanos. El Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial, comité creado por la UE en 2018, define los sistemas de inteligencia artificial (SIA) como

> sistemas de software (y en algunos casos también de hardware) diseñados por seres humanos que, dado un objetivo complejo, actúan en la dimensión física o digital mediante la percepción de su entorno a través de la obtención de datos, la interpretación de los datos estructurados o no estructurados que recopilan, el razonamiento sobre el conocimiento o el procesamiento de la información derivados de esos datos, y decidiendo la acción o acciones óptimas que deben llevar a cabo para lograr el objetivo establecido[2].

Los SIA ejecutan algoritmos. Un algoritmo no es otra cosa que un conjunto de instrucciones determinadas para obtener un resultado específico. Una receta

1 Matemático e informático estadounidense, quien supuestamente utilizara por primera vez el término en una conferencia, en 1956.

2 Comisión Europea, Grupo de expertos de alto nivel sobre inteligencia artificial, *Directrices Éticas para una IA fiable* (Bruselas; CE, 2018), párr. 153.

de cocina es, según la definición antedicha, un algoritmo. Sin embargo, los SIA son capaces de procesar complejos algoritmos y aplicarlos a "macrodatos" (*Big Data*) con un enorme potencial predictivo. Sin que nos demos cuenta, muchísimos algoritmos influencian nuestra toma de decisiones diaria. Por ejemplo, los algoritmos de Netflix nos sugieren qué películas ver y los de Amazon qué productos comprar, entre otros. Los SIA prometen grandes oportunidades, pero pueden también ser fuente de amenazas a nuestro modo de vida y de organización política hodierna. Algunos autores han alertado contra los riesgos que entrañaría una *sociedad de la caja negra*[3], en alusión a una de las características de muchos algoritmos: su opacidad. La metáfora del algoritmo como una caja negra (*black box*) sugiere que sus instrucciones no son cognoscibles por ninguna persona ajena a este. Con respecto a la mayoría de los SIA podemos conocer las entradas (*inputs)* y las salidas (*outputs)*, pero no el proceso según el cual la información pasa de un estadio al otro. Ante esta consecuencia, o efecto de caja negra, surge una duda razonable: ¿Respetarán los SIA la norma positiva y los derechos fundamentales?

Desconociéndose el contenido del algoritmo, se hace imposible determinar si este viola o no el orden jurídico existente. La premisa es simple y parte de la selección racional, aplicable tanto a seres humanos (*homo oeconomicus*) como a máquinas racionales (*machina oeconomicus*)[4]. Un algoritmo programado para obtener un resultado de la manera más eficaz podría pasar por alto (o por encima) muchas reglas jurídicas. Podría ser racional para un algoritmo cometer un ilícito si ello fuera conducente al cumplimiento de sus fines y supiera que quedaría sin sanción (por ejemplo, porque no fuera posible para la autoridad estatal determinar si hubo infracción)[5]. Sin sanción jurídica, se priva a la sociedad de una herramienta disuasoria para desincentivar conductas antisociales.

3 Frank Pasquale, *Black box society: the secret algorithms that control money and information* (London: Harward University Press, 2019).

4 Martin Prause, *On the Trail of Machina Economicus* (Insights, Infosys, 2017), https://www.infosys.com/insights/ai-automation/machina-economicus.html; Zhuxi Li, "Machina Economicus: A Rational Mind," *The TSEconomist*, June, 6, 2017, https://thetseconomist.com/2017/06/06/machina-economicus-a-rational-mind/.

5 Siguiendo a Becker, un hombre racional, antes de realizar una conducta ilegítima, tendrá en cuenta el beneficio esperado y sus costos, que es una función de la sanción potencial multiplicada por la probabilidad de ser detectado y condenado. Un algoritmo racional tomaría en cuenta el mismo cálculo costo-beneficio. Gary S. Becker, *The Economic Approach to Human Behavior* (Chicago: University of Chicago Press, 1976) y *Essays in the Economics of Crime and Punishment* (New York: National Bureau of Economic Research [NBER], 1974). Una máquina racional, con la misma información y un algoritmo para maximizar su utilidad, podría llegar a las mismas conclusiones.

ANUARIO DE DERECHO PRIVADO 04 – Universidad de los Andes – Facultad de Derecho – pp. 109-135 – DOI: hhttp://dx.doi.org/10.15425/2022.650

No necesariamente estamos hablando de algoritmos programados dolosamente para violar la ley (algo que, por otro lado, tampoco podemos descartar). Algunos programadores o titulares de SIA podrían tener incentivos para violar la norma cuando hacerlo pueda darles algún tipo de beneficio (económico, competitivo, estratégico, etc.). Sin embargo, probablemente el mayor riesgo provenga de infracciones no dolosas, por ejemplo, debido a defectos de programación, sesgos cognitivos del programador o por contar con una base de datos de aprendizaje limitada para educar al algoritmo, entre muchas otras posibilidades.

En estos casos, el problema jurídico que se nos presenta es cómo determinar la juridicidad o antijuridicidad de un determinado algoritmo. Si determinar la juridicidad o antijuridicidad del algoritmo deviene imposible, dada su opacidad, no habrá sanción. Ergo, al menos desde una perspectiva puramente racional que soslaya toda inquietud ética, los incentivos de utilizar el algoritmo para violar la ley aumentan. Al respecto se han escrito muchos artículos sobre algoritmos que, actual o potencialmente, por dolo o negligencia, ponen en jaque distintas ramas del derecho: derecho laboral[6], derecho del consumidor, derecho penal[7], defensa de la competencia[8,] regulación del mercado de valores[9], etc.

Quizás la variante que ha ocupado más la atención de los tratadistas sea la llamada *discriminación algorítmica*. Es decir, situaciones en las que un algoritmo, por distintas razones, tome decisiones que puedan ser consideradas discriminatorias desde el punto de vista jurídico (discriminación ilegítima). Un documento del Banco Interamericano de Desarrollo define la discriminación algorítmica como

> procesos a través de los cuales los distintos tipos de discriminación que ocurren en el mundo real son reproducidos en entornos de datos, o a los que surgen exclusivamente en ellos, como cuando los sistemas de reconocimiento facial producen más errores al procesar rostros no caucásicos[10].

6 Natalia Ramírez-Bustamante y Andrés Páez, "Análisis jurídico de la discriminación algorítmica en los procesos de selección laboral," *Innovación en derecho y nuevas tecnologías* (Bogotá; Ediciones Uniandes, 2020).

7 Francesca Palmiotto, "The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings," in *Algorithmic Governance and Governance of Algorithms*, ed. Martin Ebers and Marta Cantero (Switzerland: Springer International Publishing, 2020).

8 Mark R. Patterson, "Algorithmic Opacity and Exclusion in Antitrust Law," *Italian Antitrust Review* 5, n.º 1 (2018): 23-31.

9 Sylvia Lu, "Algorithmic Opacity, Private Accountability, and Corporate Social Disclosure," *Vanderbilt Journal of Entertainment & Technology Law*, 23, n.º 1 (2020).

10 César Buenadicha, María Hermisilla Gemma Galdon, Daniel Loewe y Cristina Pombo Banco, *La gestión ética de los datos* (Santiago de Chile: Banco Interamericano de Desarrollo, 2019).

Los SIA opacos, por las razones descriptas, pueden exacerbar el riesgo de discriminación algorítmica. En muchos países ya se utilizan algoritmos para selección de personal, programas de computación conocidos como Applicant Tracking Systems (ATS). En dicho caso, el algoritmo del ATS determinará autónomamente si un ser humano es seleccionado para una entrevista o puesto de trabajo. Si bien el uso del ATS puede ser eficiente, económico y hasta podría parecer un medio más objetivo para la selección de personal, liberado de los sesgos y subjetividades del ser humano, sin embargo, no está libre de peligros. Ha sido probado que algunos ATS incurren en discriminación algorítmica negligente, en particular de tipo racial, al momento de seleccionar personal, en violación de la normativa federal de los EE. UU. en la materia (Título VII de la Civil Rights Act de 1964)[11]. En la mayoría de los casos las causas son defectos de programación, datos de entrenamiento sesgados o insuficiencia de datos. La frase *garbage in, garbage out* (basura entra, basura sale) captura la lógica de la discriminación algorítmica negligente. Es decir, si los datos con los que se entrena o trabaja el algoritmo se encuentran sesgados (por ejemplo, debido a un error de selección), el resultado al que arribará será sesgado.

2. Opciones regulatorias frente a los dilemas que plantea la inteligencia artificial

Ante estos y otros desafíos que los SIA aparejan, se han propuesto distintas soluciones tanto privadas como públicas, duras (*hard)* y blandas (*soft)*, nacionales y regionales. Siguiendo a Black, entendemos por regulación en sentido amplio (*lato sensu)*, un conjunto de reglas destinadas a influenciar la conducta humana, sean estas de origen estatal (leyes) o no[12].

¿Convendrá dejar librada la regulación algorítmica exclusivamente al mercado? Es decir, ¿a la autorregulación por parte de los actores económicos que operan en el mercado de la IA? Según la teoría económica neoclásica, los desarrolladores de SIA, movidos por su propio interés (e.g., obtención de ganancias, mantenimiento de una buena reputación, etc.) tendrían incentivos suficientes para autorregularse mediante

11 Andrés Páez, "*Negligent Algorithmic* Discrimination, " *Law and Contemporary Problems* 84, n.º 3 (2021): 19-33.

12 Julia Black, *Critical reflections on regulation* (London: Centre for Analysis of Risk and Regulation, London School of Economics and Political Science, 2002), 27.

la creación de mecanismos de cumplimiento no vinculantes (*soft laws)* autónomos, tales como códigos de buenas prácticas y estándares o certificaciones de adhesión voluntaria. Si bien sus defensores sugieren que la autorregulación favorece la inversión, no debemos olvidar que la crisis financiera global de 2008 (iniciada con las hipotecas subprime) tuvo como uno de sus factores disparadores la falla o ausencia de autorregulación eficaz por parte de los actores del mercado. Los incentivos de corto plazo (mayores ganancias) pueden nublar la visión y desplazar a los objetivos de largo plazo (sostenibilidad), originando una tragedia en la que todos pierden.

Frente a la opacidad algorítmica, por ejemplo, se han propuesto soluciones tecnológicas u organizacionales. La IA explicable (conocida por el acrónimo XAI) es un intento de transparentar algoritmos opacos, en particular los relativos a la tecnología de aprendizaje automático (*machine learning*). Si bien explicar no es lo mismo que transparentar, se trata de que los seres humanos sean capaces de entender lo que realmente hace ese algoritmo, para que puedan confiar en él. En otras palabras, pasar de la caja negra a una caja de cristal (*cristal box*). Sin embargo, la solución no es sencilla en la práctica. Pareciera que, como sostienen varios expertos, la transparencia de un algoritmo es inversamente proporcional a su efectividad[13]. Asimismo, algunas tecnologías de IA hacen muy difícil determinar los parámetros que algunos SIA usan para tomar decisiones. Tal es el caso de las redes neuronales, una de las tecnologías de IA más avanzadas actualmente.

Los mecanismos de cumplimiento no vinculantes también pueden ser heterónomos. Es decir, originarse en la labor de instituciones ajenas a la industria, generalmente organizaciones no gubernamentales, gubernamentales o intergubernamentales. Varios estándares éticos han sido propuestos para regular distintos aspectos de la IA, en particular desde una perspectiva global, dadas las dificultades para hacerlo a través del derecho internacional, teniendo en cuenta los intereses divergentes de los Estados involucrados (soberanía y proteccionismo de datos versus universalismo y libre transferencia de datos)[14]. Por ejemplo, en 2019, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) adoptó los *Principios sobre Inteligencia Artificial* que establecen una IA homocéntrica, que respete el Estado de derecho, los derechos humanos, la democracia, la

13 Arun Rai, "Explainable AI: From Black Box to Glass Box," *Journal of the Academy of Marketing Science* 48, n.º 1 (2020): 137-41.

14 Lorna McGregor, Daragh Murray y Vivian Ng, "International human rights law as a framework for algorithmic accountability," *International and Comparative Law Quarterly* 68, n.º 2 (2019): 309-43.

diversidad, etc.[15]. Human Rights Watch, en su *Declaración de Toronto*[16] definió una serie de principios éticos para el desarrollo de SIA, entre los que se destacan la transparencia y la rendición de cuentas (*accountability*). Nueva Zelanda presentó la *Algorithm Charter for Aotearoa*[17] por la que adoptó una serie de principios de buen gobierno, transparencia y rendición de cuentas, en el uso de los datos y algoritmos, a fin de incrementar la confianza de los neozelandeses.

Finalmente, tenemos las reglas jurídicas (*hard laws*). Es decir, reglas cuyo cumplimiento es garantizado de manera externa por la probabilidad de aplicación de medidas coercitivas por parte de los órganos legitimados del Estado, de acuerdo con una definición de Weber[18]. El legislador cuenta con un amplio menú de opciones y de técnicas legislativas, dentro de los límites de la Constitución: principios jurídicos generales; reglas jurídicas específicas: normas nacionales, regionales (en el marco de procesos de integración), internacionales (tratados multilaterales o bilaterales), de naturaleza civil, penal, administrativa, procesal, substantiva; *lex generalis*, *lex specialis*, etc. Asimismo, las reglas jurídicas pueden imponer obligaciones horizontales, es decir, entre desarrolladores de SIA y usuarios; o verticales, entre desarrolladores de SIA y autoridades de aplicación. Dentro de este marco, el derecho algorítmico o *Lex Algorithmica* comienza a delinearse no como nueva rama jurídica, sino como un área transversal en la que el legislador echa mano de distintas técnicas legislativas (incluidas las leyes blandas o no vinculantes). La *Lex Algorithmica* sería entonces el conjunto de principios y de reglas jurídicas que regulan los SIA, incluyendo tanto normas que permiten maximizar los beneficios[19] y oportunidades[20] derivadas de esta, como aquellas que buscan minimizar sus riesgos y externalidades negativas en la sociedad.

15 The Organization for Economic Co-operation and Development (OECD), "Recommendation of the Council on Artificial Intelligence" (22 de mayo de 2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

16 Human Rights Watch, *The Toronto Declaration* (Toronto: HRW, 2018).

17 Gobierno de Nueva Zelanda, (julio de 2020), https://www.data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-charter/

18 Max Weber y Keith Tribe, *Economy and Society: A New Translation* (Cambridge, Mass.: Harvard University Press, 2019).

19 Por ejemplo, la legislación de protección de secretos industriales, de propiedad intelectual, incentivos fiscales, etc.

20 María del Carmen Aguilar del Castillo, "El uso de la inteligencia artificial en la prevención de riesgos laborales," *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo* 8, n.º 1 (2020): 262-93.

3. Hacia un Estado de derecho algorítmico

Lessig escribió no hace demasiado tiempo que en la *sociedad de la información* "el código (informático) es la ley (derecho positivo)"[21]. Es decir, no importa lo que la ley prohíba o tolere, a fin de cuentas, será el código informático el que determinará lo que efectivamente sucederá o no. La Constitución de un país puede garantizar la libertad de expresión, pero en la práctica será, por ejemplo, el algoritmo de Twitter el que decidirá si un determinado comentario será o no publicado. Ya dejamos atrás la sociedad de la información para vivir en una *sociedad algorítmica*. Corresponde entonces actualizar el *díctum* de Lessig. Hoy, *mutatis mutandis,* "el algoritmo es la ley". Es decir, una *regulación puramente algorítmica* conlleva el riesgo de que los SIA, o, mejor dicho, sus programadores o las empresas titulares de aquellos, se conviertan en legisladores de facto, anulando en la práctica las disposiciones constitucionales. La regulación puramente algorítmica pone en riesgo los derechos fundamentales de las personas y los principios básicos del orden democrático[22].

Además, a diferencia de la regulación estatal, en el caso de la regulación puramente algorítmica la aplicación (*enforcement*) es automática. El algoritmo toma la decisión y la ejecuta a la vez. Dependiendo del algoritmo, tal o cual comentario se mostrará o no en una red social, una persona recibirá o no una oferta de trabajo o un crédito inmobiliario. La voluntad del sujeto es ajena. Enfrentado a una norma ética o jurídica, el individuo podrá decidir cumplirla o no. En un contrato de compraventa, el vendedor podrá negarse a firmar la escritura traslativa de dominio, aun luego de haber recibido el pago. Dicha conducta podrá tener distintas consecuencias jurídicas (por ejemplo, una acción por incumplimiento contractual, seguida de una sentencia ordenando la indemnización de los daños y perjuicios o el cumplimiento forzado, etc.), pero en ningún caso será automático. Habrá un proceso, pruebas, garantías. En el caso de un contrato inteligente (*smart contract*), por ejemplo, una compraventa de bitcoin será un algoritmo apoyado en la cadena de bloques (*Blockchain)* el que determinará y ejecutará la transacción a la vez, si se cumplen las condiciones pautadas de antemano. La conducta de las partes no tendrá ninguna incidencia sobre su cumplimiento. No habrá proceso, ni pruebas, ni

21 En inglés, *code is law*. Lawrence Lessig, *Code 2.0* (Createspace, 2009).

22 Karen Yeung, "Algorithmic regulation: A critical interrogation," *Regulation & Governance* 12, n.º 4 (2018): 505-23; Mireille Hildebrandt, "Algorithmic regulation and the rule of law," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376, n.º 2128 (2018): 376.

garantías. La regulación puramente algorítmica gana en eficiencia, pero remueve el libre albedrío. Este es un tema no menor al que aquí, por razones de tiempo, no se hace referencia en profundidad.

El punto que se quiere resaltar, sin embargo, es que no debemos dejar nuestras libertades y derechos fundamentales a merced de la tecnología. En una sociedad gobernada de facto por algoritmos, la democracia y el Estado de derecho terminarán por convertirse en meras ilusiones. El imperio de la ley sería reemplazado por el imperio del algoritmo, en general opaco, para beneficio de su titular (generalmente una empresa con fin de lucro) y no de la sociedad toda. El Estado de derecho (*Rule of Law, Rechtsstaat*) es un valor fundamental de la democracia liberal moderna. En el caso europeo, no en vano ocupa un espacio destacado en los textos fundadores de la UE[23]. Si bien no es fácil encontrar una definición universalmente aceptada de qué es Estado de derecho (hay definiciones minimalistas, maximalistas, sustantivas, procesales, etc.)[24], la mayoría de los autores coinciden en que la igualdad ante la ley, el principio de legalidad y el respeto por los derechos humanos, entre otros, son componentes esenciales. El Estado de derecho algorítmico no es más que la adaptación de este viejo concepto a los tiempos que corren. Significa que robots y vehículos autónomos, SIA, programadores y las empresas que estén detrás de aquellos, estén sometidos al imperio de la ley, como todo el resto del mundo. No solo las personas, sean físicas o morales, sino también los sistemas autónomos (hardware o software, tengan o no personalidad jurídica)[25] deben estar sometidos al imperio de la ley.

4. La evolución de la *Lex Algorithmica* en la Unión Europea

En materia de regulación algorítmica, la UE es consciente de que, en volúmenes de inversión, viene por detrás de los EE. UU. y de Asia[26]. En los albores de la *cuarta revolución industrial*, la IA es una tecnología clave para la competitividad de las

23 Cfr. el preámbulo y el artículo 2 del Tratado de Funcionamiento de la Unión Europea.

24 Brian Z. Tamanaha, *On the Rule of Law: History, Politics, Theory* (New York: Cambridge University Press, 2004).

25 Simon Chesterman, "Artificial Intelligence and the Limits of Legal Personality," *International & Comparative Law Quarterly* 69, n.º 4 (2020): 819-44.

26 En 2016, se invirtieron unos 3 200 millones EUR en inteligencia artificial en Europa, frente a los cerca de 12 100 millones EUR en América del Norte y 6 500 millones EUR en Asia. Comisión Europea, *Libro Blanco sobre la inteligencia artificial - Un enfoque europeo orientado a la excelencia y la confianza* (Bruselas: CE, 2020).

naciones y las regiones[27]. El rezago se puede explicar también desde lo regulatorio. Las reglas jurídicas actúan sobre los operadores de mercado creando incentivos (derechos, premios, etc.) o desincentivos (obligaciones, sanciones, etc.)[28]. Ninguna modificación del *statu quo* es neutra. Desde una perspectiva económica, reconocer más derechos a los usuarios supone aumentar los costos y la responsabilidad de las empresas. En un mundo globalizado, donde el capital puede moverse libremente y las empresas deslocalizarse, los países con altos estándares jurídicos podrían quedar en desventaja. Consciente de ello, la *Lex Algorithmica* de la UE trata de conciliar dos objetivos aparentemente antagónicos. Por un lado, incentivar una mayor inversión en IA y la creación de empresas en la región (lógica utilitaria). Por otro, aumentar la confianza de los ciudadanos y el respeto por los derechos fundamentales y los valores democráticos (lógica deóntica).

4.1. Reglamentos y directivas (*Hard Laws*)

Las disposiciones que tocan a la IA se encuentran esparcidas en varias directivas y algunos reglamentos[29]. Se trata de una regulación fragmentaria e incompleta. Entre ellas, tal vez la más importante sea el *Reglamento general de protección de datos* (RGPD)[30]. La IA no puede funcionar sin datos y el RGPD establece las condiciones para acceder legítimamente a los datos personales, cómo tratarlos (procesarlos), los derechos de los interesados, las obligaciones de los responsables del tratamiento, etc. El artículo 2 del RGPD determina un ámbito de aplicación amplio, incluyendo todo tipo de tratamiento de datos personales ya sea total o parcialmente automatizado. La definición de "tratamiento" incluida en el artículo 4.4 claramente incluye el realizado por los SIA. Para mayor seguridad jurídica, la Agencia

27 Klaus Schwab, *The Fourth Industrial Revolution* (World Economic Forum, 2016).

28 Thomas L. Oomen, W*hy the EU Lacks behind China in AI Development – Analysis and Solutions to Enhance EU's AI Strategy* (Subang Jaya: Asia Study Centre, 2021); Daniel Castro & Michael McLaughlin, *Who Is Winning the AI Race: China, the EU, or the United States?* (Washington: Information Technology & Innovation Foundation, 2021).

29 El derecho de la UE, que se compone de derecho primario (los tratados fundacionales) y secundario (directivas, reglamentos y decisiones, entre otras). Es un ordenamiento jurídico regional y supranacional. Es decir, en las áreas donde la UE tiene competencia (principio de atribución) el derecho unionístico se impone por sobre los derechos nacionales de los Estados miembro, según la jurisprudencia del Tribunal de Justicia de la UE, fallos *Van Gend & Loos* (ECLI:EU:C:1963:1) y *Costa/ENEL* (ECLI:EU:C:1964:66), entre otros.

30 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, por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE).

Española de Protección de Datos ha especificado el ciclo de vida del tratamiento de datos personales de un SIA que quedan sujetos al RGPD, incluyendo su validación, despliegue, explotación y retirada de los datos, entre otros[31]. El artículo 5 del RGPD enumera una serie de principios generales relativos al tratamiento, entre los que se destacan la "licitud, lealtad y transparencia" (5.1 (a)). El artículo 6 establece las seis únicas condiciones que harán lícito el tratamiento de datos. Los artículos 13 y 14 imponen al responsable del tratamiento una serie de obligaciones de información. El artículo 15.1 otorga al interesado el derecho de acceso a sus datos personales y a conocer los fines del tratamiento, lo que ha sido interpretado por algunos autores como una obligación de transparencia o explicabilidad del algoritmo (derecho a una explicación)[32]. Sin embargo, ni las autoridades ni la doctrina están de acuerdo sobre su alcance[33]. El artículo 22 establece 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". Es decir, un algoritmo no podrá tomar este tipo de decisiones autónomamente, si bien hay algunas excepciones (22.1). El considerando 71 incluye dentro de la prohibición del artículo 22, a modo de ejemplo, la "denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna"[34]. Finalmente el RGPD establece limitaciones a la transferencia de datos personales. Transferir datos personales fuera de la UE puede ser más problemático de lo anticipado, como demuestran las sentencias en los casos *Schrems I* y *II* (que llevaron a la anulación del EU–*US Safe Harbor* y *EU–US Privacy Shield*, respectivamente)[35].

Ciertamente, el RGPD no ofrece soluciones a todos los desafíos que representa la IA[36]. Sin embargo, no debemos olvidar que la *ratio legis* del RGPD es, de

31 Agencia Española de Protección de Datos, *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción* (Madrid: AEDP, 2020).

32 Bryce Goodman & Seth Flaxman, "EU Regulations on Algorithmic Decision-Making and a 'right to Explanation," *AI Magazine* 38, n.º 3 (2016): 50-57.

33 Andrew D. Selbst & Julia Powles, "Meaningful Information and the Right to Explanation," International Data Privacy Law 7, n.º 4 (2017):233-42.

34 "Considerando 71. El interesado debe tener derecho a no ser objeto de una decisión, que puede incluir una medida, que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar, como la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna."

35 Schrems I, caso C-362/14 (ECLI:EU:C:2015:650) (2015), Schrems II, caso C-311/18 (ECLI:EU:C:2020:559).

36 Céline Castets-Renard, "Accountability of Algorithms in the GDPR and Beyond: A European Legal Framework on Automated Decision-Making," *Fordham Intellectual Property, Media and Entertainment Law Journal* 30 n.º 1 (2019): 91-137.

acuerdo con su considerando 1, "la protección de las personas físicas en relación con el tratamiento de datos personales", un derecho fundamental de la máxima jerarquía en el ámbito de la UE[37]. Asimismo, vale la pena recordar que algunos autores sugieren que el alto nivel de protección que el RGPD garantiza a los interesados impone un costo tal vez demasiado alto para las empresas europeas, convirtiéndose en un desincentivo a la inversión en el corto plazo[38] y una causa de pérdida de competitividad global en el largo plazo[39].

El *Reglamento 2019/1150 sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación* impone una obligación limitada de transparencia o explicabilidad de cierto tipo de algoritmos (aquellos relativos a los motores de búsqueda). En su artículo 5.2 dice que:

> Los proveedores de motores de búsqueda en línea expondrán los parámetros principales que, de forma individual o colectiva, sean más significativos a la hora de determinar la clasificación y la importancia relativa de esos parámetros principales, presentando una descripción de acceso fácil y público, redactada de manera sencilla y comprensible, en los motores de búsqueda en línea que ofrecen.

La *Directiva 2016/943 del Parlamento Europeo y del Consejo, 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*, ampara los algoritmos siempre que reúnan las condiciones de ser secreto, tener un valor empresarial (real o potencial) y haber sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto[40]. Asimismo, el artículo 1 de *Ley 1/2019, de 20 de febrero, de Secretos Empresariales*, que transpone la directiva mencionada anteriormente en España, agrega que se considerará secreto empresarial "cualquier información o conocimiento, incluido el tecnológico[41], científico, industrial, comercial, organizativo o financiero." Si bien, en principio, no

37 Artículo 16 del Tratado de Funcionamiento de la Unión Europea, y artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea.

38 Jian Jia, Ginger Zhe Jin & Liad Wagman, *The Short-Run Effects of GDPR on Technology Venture Investment* (Massachusetts: National Bureau of Economic Research, 2018).

39 Daniel Castro & Michael McLaughlin, *Ten Ways the Precautionary Principle Undermines Progress in Artificial Intelligence* (Washington: Information Technology & Innovation Foundation, 2019); Michal S. Gal & Oshrit Aviv, "The Competitive Effects of the GDPR," *Journal of Competition Law & Economics* 16, n.º 3 (2020): 349-91.

40 Mariateresa Maggiolino, "EU Trade Secrets Law and Algorithmic Transparency," *SSRN Electronic Journal,* https://ssrn.com/abstract=3363178

41 Subrayado agregado por el autor.

podrá mandarse la divulgación de los algoritmos de los SIA que cumplan con las condiciones mencionadas, su protección no es absoluta. El artículo 5 de la Directiva y el artículo 2.3(b) de la ley española enumeran varios casos de excepción: el secreto puede ceder en caso de colisión con el derecho a la libertad de expresión, para poner al descubierto alguna falta, irregularidad o actividad ilegal, en ejercicio de derechos de los trabajadores o para proteger un interés legítimo. Algunos autores sugieren que sería posible una interpretación expansiva de dichas excepciones a efectos de transparentar ciertos algoritmos por razones de interés público[42].

Finalmente cabe mencionar la *Directiva 2014/65 del 15 de mayo de 2014 relativa a los mercados de instrumentos financieros* (MiFID II), que ha incorporado algunas medidas para reforzar la seguridad de los mercados ante la proliferación de la "negociación algorítmica de alta frecuencia" (*high-frequency algorithmic trading*). Este tipo de negociación, en la que no hay intervención humana, permite comprar y vender activos financieros cotizados en mercados de valores, en milisegundos. Debido a su velocidad, volatilidad y volumen, ante fallos o errores sistémicos, se corre el riesgo de que en pocos minutos se produzca una caída abrupta del mercado (*flash crash*), con consecuencias nefastas para los inversores. Para mitigar estos riesgos, la MiFID II incorpora algunas obligaciones específicas que tocan a los SIA. Por ejemplo, el párrafo 1 del artículo 17 de la MiFID II, referido a la *negociación algorítmica*, establece que la empresa de servicios de inversión que se dedique a este tipo de transacciones

> deberá implantar sistemas y controles de riesgo adecuados a sus actividades y efectivos para garantizar que sus sistemas de negociación sean resistentes, tengan suficiente capacidad, se ajusten a los umbrales y límites apropiados y limiten o impidan el envío de órdenes erróneas o la posibilidad de que los sistemas funcionen de modo que pueda crear o propiciar anomalías en las condiciones de negociación.

A su vez, el párrafo 2 del mismo artículo incorpora una obligación vertical de notificación a las autoridades competentes[43].

42 Katarina Foss-Solbrekk & Ann Kristin Glenster, "The Intersection of Data Protection Rights and Trade Secret Privileges in Algorithmic Transparency," in *Research Handbook on EU Data Protection Law*, eds. Eleni Kosta and Ronald Leenes (Holland: Edward Elgar Publishing, 2022).

43 "La empresa de servicios de inversión que se dedique a la negociación algorítmica en un Estado miembro lo notificará a las autoridades competentes de su Estado miembro de origen y del centro de negociación en el que se dedique a la negociación algorítmica en calidad de miembro o de participante en el centro de negociación."

4.2. Comunicaciones y recomendaciones (*Soft Laws*)

Desde hace algunos años la Comisión Europea y en menor medida el Parlamento Europeo publican una serie de comunicaciones y recomendaciones no vinculantes para encuadrar la regulación de la IA. En abril de 2018 la Comisión expidió la comunicación *Inteligencia artificial para Europa*[44], seguida por otra del 7 de diciembre del mismo año[45], donde se describen los tres pilares que constituyen el núcleo duro de la propuesta de la Comisión: impulsar la capacidad tecnológica e industrial de la UE y favorecer la adopción de la IA en la economía; prepararse para los cambios socioeconómicos que provocará la IA; y garantizar un marco ético y jurídico adecuado, basado en los valores de la Unión, de conformidad con la Carta de los Derechos Fundamentales de la UE. En 2019, la nueva presidente de la Comisión, Ursula von der Leyen, expuso los avances en los primeros 100 días de su gestión, en los cuales se destaca el anunció de impulsar la legislación sobre las implicaciones humanas y éticas de la IA[46]. El 8 de abril de 2019 la Comisión divulgó la Comunicación *Generar confianza en la inteligencia artificial centrada en el ser humano*. En el mismo sentido se expresó la, entonces, canciller alemana Angela Merkel, quien en la cumbre del G-20 celebrada en Japón en junio de 2019 expresó que corresponderá a la Comisión impulsar una normativa similar al RGPD en lo que respecta a la IA, para que esta sirva a la humanidad y no viceversa.

Para ayudarla en su labor, en 2018 la Comisión creó el Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial (AI HLG, por sus siglas en inglés). A finales de 2018 el AI HLG presentó las *Directrices éticas para una IA confiable*, que establecen siete requisitos fundamentales para aumentar la confianza de los ciudadanos europeos en la IA: 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[47]. En abril de 2019 el AI HLG publicó las *Directrices éticas de IA*, haciendo referencia al potencial impacto de esta en la competitividad de la UE, además de sus implicaciones sociales y éticas, que fueron seguidas en junio de 2019 por las *Recomendaciones de política e inversión para una IA confiable*.

44 https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018DC0237&from=ES

45 "Los Estados miembros y la Comisión colaborarán para impulsar la inteligencia artificial 'fabricada en Europa'", https://ec.europa.eu/commission/presscorner/detail/es/IP_18_6689

46 https://www.cityam.com/ursula-von-der-leyen-pledges-action-on-artificial-intelligence-during-first-100-days-in-office/

47 Brent Daniel Mittelstadt, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter, & Luciano Floridi, "The Ethics of Algorithms: Mapping the Debate," Big Data and Society (2016): 1-21.

En febrero de 2020 la Comisión publicó el *Libro Blanco sobre la IA: un enfoque europeo orientado a la excelencia y la confianza*, mencionado anteriormente[48]. El *Libro Blanco* sugiere ajustes al marco legislativo existente, entre otros, para superar el efecto de caja negra, hacer frente a nuevos riesgos de seguridad y lagunas jurídicas en materia de responsabilidad civil. Asimismo, clasifica a los SIA según su potencial de riesgo, algo que será retomado por el proyecto de Reglamento. Al *Libro Blanco* le siguieron el *Informe sobre las implicaciones de seguridad y responsabilidad de las nuevas tecnologías* y la *Estrategia Europea de Datos*.

A su vez, el 16 de febrero de 2017 el Parlamento Europeo aprobó la *Resolución con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica*. Esta sugería la creación de una Agencia Europea de Robótica e Inteligencia Artificial integrada por reguladores, expertos en informática y ética para apoyar la labor legislativa del Parlamento Europeo y de los Estados miembro. Adicionalmente recomendó la creación de un registro en la UE para la inscripción de ciertas categorías de robots avanzados. El Parlamento también publicó una *Carta sobre robótica,* elaborada con la asistencia de la Unidad de Prospectiva Científica, un código de conducta para que investigadores y programadores actúen de manera responsable, respetando la dignidad, privacidad y seguridad de otros seres humanos. Finalmente, el Parlamento pidió a la Comisión que se ocupe de la responsabilidad y los daños que puedan causar los robots autónomos, sugiriendo la adopción de nuevas reglas sobre responsabilidad civil si fuera necesario. El 12 de febrero de 2020 el Parlamento presentó la *Resolución sobre los procesos automatizados de toma de decisiones: garantizar la protección de los consumidores y la libre circulación de bienes y servicios* (2019/2915(RSP). Si bien las comunicaciones y directrices no son documentos jurídicamente vinculantes, proveen lineamientos importantes para la elaboración de la futura legislación.

4.3. La Propuesta de Reglamento de de inteligencia artificial (*De Lege Ferenda*)[49]

El 21 de abril de 2021 la Comisión presentó la *Propuesta de Reglamento por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión*[50].

48 https://ec.europa.eu/info/files/white-paper-artificial-intelligence-european-approach-excellence-and-trust_es

49 Al momento de enviar este manuscrito, la propuesta estaba siendo debatida el Parlamento Europeo y el Consejo de la UE (colegisladores).

50 https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

La propuesta, que consta de 85 artículos, se inspira en ideas tomadas del *Libro Blanco* y tiene algunas coincidencias con el RGPD, como por ejemplo el énfasis en la protección de los derechos fundamentales, su alcance extraterritorial, multas de alto valor (pudiendo alcanzar hasta el 6 % de la facturación global de las empresas involucradas) que se espera tengan un fuerte efecto disuasivo, etc. Se trata de una regulación completa y detallada, pero no libre de incertidumbre en cuanto a si alcanzará los objetivos esperados, en caso de que se convierta en ley. El Proyecto de Reglamento también codifica algunos principios previamente mencionados en comunicaciones y directrices anteriores, por ejemplo, que la IA debe beneficiar a todos los seres humanos (IA *homo mensura*). A su vez, combina un enfoque basado en el riesgo, con un mecanismo de aplicación por niveles. Esto significa que, a medida que aumenta el riesgo, se aplican normas más estrictas.

En su artículo 1, el Proyecto enumera sus objetivos: a) normas armonizadas para la introducción en el mercado, la puesta en servicio y la utilización de SIA en la UE; b) prohibiciones de determinadas prácticas de inteligencia artificial; c) requisitos específicos para los sistemas de IA de alto riesgo y obligaciones para los operadores de dichos sistemas; d) normas armonizadas de transparencia aplicables a los sistemas de IA destinados a interactuar con personas físicas, los sistemas de reconocimiento de emociones y los sistemas de categorización biométrica, así como a los sistemas de IA usados para generar o manipular imágenes, archivos de audio o vídeos; y e) normas sobre el control y la vigilancia del mercado.

En líneas generales, la Propuesta adopta un criterio preventivo, tratando de acomodar los intereses de las diversas partes (*stakeholders)* involucradas para

- garantizar que los sistemas de IA introducidos y usados en el mercado de la UE sean seguros y respeten la legislación vigente en materia de derechos fundamentales y valores de la Unión;
- garantizar la seguridad jurídica para facilitar la inversión e innovación en IA;
- mejorar la gobernanza y la aplicación efectiva de la legislación vigente en materia de derechos fundamentales y los requisitos de seguridad aplicables a los sistemas de IA;
- facilitar el desarrollo de un mercado único para hacer un uso legal, seguro y fiable de las aplicaciones de IA y evitar la fragmentación del mercado[51].

51 Ibid. 1.1. Razones y objetivos de la propuesta.

En cuanto a los niveles de riesgo, la Propuesta propone cuatro, a saber:

a. Riesgo inaceptable. Los SIA que contravengan los valores básicos de la UE (como, por ejemplo, un sistema de *puntuación social* por parte de un gobierno) están prohibidos. En estos casos el riesgo se considera inaceptable. Por ejemplo, conforme al artículo 5, un SIA que "se sirva de técnicas subliminales que trasciendan la conciencia de una persona para alterar de manera sustancial su comportamiento de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra"; "aproveche alguna de las vulnerabilidades de un grupo específico de personas debido a su edad o discapacidad física o mental para alterar de manera sustancial el comportamiento de una persona que pertenezca a dicho grupo de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra"; "por parte de las autoridades públicas o en su representación con el fin de evaluar o clasificar la fiabilidad de personas físicas durante un período determinado de tiempo atendiendo a su conducta social o a características personales o de su personalidad conocidas o predichas"; y "el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley"[52].
b. Ato riesgo. Los SIA de alto riesgo se determinan en un anexo y son aquellos que puedan generar un impacto adverso en la seguridad de las personas o en sus derechos fundamentales. En estos casos, para garantizar la confianza y un alto nivel de protección de la seguridad y los derechos fundamentales de las personas, se deberá cumplir con una serie de requisitos obligatorios (obligaciones de *compliance*). Por ejemplo, su certificación previa a la comercialización.
c. De riesgo limitado. Estos SIA se encuentran sujetos a pocas obligaciones (por ejemplo, obligaciones de transparencia).
d. De riesgo mínimo. Esto es, aquellos SIA que no están sujetos a obligaciones legales específicas, más allá de tener que cumplir con el resto de la legislación vigente aplicable.

52 Ibid.

Con respecto de la transparencia, el considerando 47 dice que

> debe exigirse cierto grado de transparencia respecto de los sistemas de IA de alto riesgo para subsanar la opacidad que puede hacer a algunos de ellos incomprensibles o demasiado complejos para las personas físicas. Los usuarios deben ser capaces de interpretar la información de salida del sistema y de usarla adecuadamente. En consecuencia, los sistemas de IA de alto riesgo deben ir acompañados de la documentación y las instrucciones de uso oportunas e incluir información clara y concisa, en particular sobre los posibles riesgos para los derechos fundamentales y de discriminación, cuando corresponda.

El artículo 13, párrafo 1, agrega: "Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de un modo que garanticen que funcionan con un nivel de transparencia suficiente para que los usuarios interpreten y usen correctamente su información de salida".

De acuerdo con el artículo 6, apartado 1:

a) El sistema de IA está destinado a ser utilizado como componente de seguridad de uno de los productos contemplados en la legislación de armonización de la Unión que se indica en el anexo II, o es en sí mismo uno de dichos productos;

b) conforme a la legislación de armonización de la Unión que se indica en el anexo II, el producto del que el sistema de IA es componente de seguridad, o el propio sistema de IA como producto, debe someterse a una evaluación de la conformidad realizada por un organismo independiente para su introducción en el mercado o puesta en servicio.

El artículo 52 incorpora obligaciones de transparencia adicionales para casos específicos. Así, los proveedores:

1. garantizarán que los sistemas de IA destinados a interactuar con personas físicas estén diseñados y desarrollados de forma que dichas personas estén informadas de que están interactuando con un sistema de IA, excepto en las situaciones en las que esto resulte evidente debido a las circunstancias y al contexto de utilización [es decir, se prohíbe la "prueba de Turing"].

El párrafo 2 del mismo artículo adiciona: "Los usuarios de un sistema de reconocimiento de emociones o de un sistema de categorización biométrica informarán del funcionamiento del sistema a las personas físicas expuestas a él."

Y en el párrafo 3 señala:

> Los usuarios de un sistema de IA que genere o manipule contenido de imagen, sonido o vídeo que se asemeje notablemente a personas, objetos, lugares u otras entidades o sucesos existentes, y que pueda inducir erróneamente a una persona a pensar que son auténticos o verídicos (ultrafalsificación [*deepfakes*]), harán público que el contenido ha sido generado de forma artificial o manipulado.

Finalmente, la Propuesta prevé la creación de autoridades de aplicación nacionales, y otra a nivel de la UE: el Supervisor Europeo de Protección de Datos.

Actualmente, la propuesta está siendo debatida por los colegisladores, el Parlamento Europeo y el Consejo (Estados miembros de la UE). La cantidad y amplitud de las definiciones, así como las clasificaciones contenidas en los anexos de la Propuesta generan dudas. Un viejo brocardo latino advierte que en derecho toda definición es peligrosa (*omnis definitio in jure periculosa est*). Por ejemplo, el uso de *identificación* en lugar de *reconocimiento* con relación a SIA destinados a utilizarse en la identificación biométrica remota «en tiempo real» o «en diferido» de personas físicas (SIA de alto riesgo) ha sido criticado. Sostienen sus detractores que muchas tecnologías de reconocimiento biométrico no tienen como objetivo identificar a una persona, sino evaluar su comportamiento o sus características, por ejemplo, mediante los rasgos faciales, el movimiento de los ojos, la temperatura corporal, el ritmo cardíaco, etc. Tal como está redactada la Propuesta, no queda claro en qué nivel se encuentran los SIA que realizan reconocimiento biométrico de personas físicas[53]. Otros autores han criticado que la Comisión haya soslayado el derecho de la competencia, según ellos, un instrumento más idóneo y menos intrusivo para regular a las empresas de IA[54].

Conclusión

En este artículo se ha descrito someramente el marco regulatorio de la IA en la UE, sin ser exhaustivo. El objetivo perseguido no es puramente especulativo, sino

53 AlgorithmWatch, *AlgorithmWatch's Response to the European Commission's Proposed Regulation on Artificial Intelligence – A Major Step with Major Gaps* (Berlin: AlgorithmWatch, 2021).

54 Divin de Buffalo Irakiza, "The Charter of Fundamental Rights, the Aims of EU Competition Law and Data Protection: Time to Level the Playing field," *Singapore Journal of Legal Studies* (2021): 39-55.

práctico. El *iter* regulatorio y el derecho de la UE puede servir de espejo a los países latinoamericanos, para reflejarse y proyectarse hacia el futuro. La elección de la UE no ha sido anodina: entre los países de América Latina y la mayoría de los Estados miembro de la UE existen sistemas jurídicos, lenguajes y valores compartidos. Esto hace ambas regiones equiparables, desde una perspectiva de derecho comparado.

Aunque en América Latina el impacto de la IA parezca hoy lejano, como muestran los espejos retrovisores del lado derecho de algunos automóviles, el nuevo paradigma está "más cerca de lo que parece". Los cambios socioeconómicos y tecnológicos que acarreará serán disruptivos, ergo, desestabilizantes. En consecuencia, los legisladores latinoamericanos harían bien en tomar nota sobre cómo otras regiones, con similitudes y diferencias, han encarado la tarea de adaptar sus derechos y políticas públicas para hacer frente a los nuevos desafíos que supone la IA, entre otras tecnologías. No solo para evitar lo que los economistas llaman *externalidades negativas*, es decir, costos que quienes se beneficien de la IA no pagarán y trasladarán a la sociedad (por ejemplo, aumento del desempleo, malestar social, etc.), sino también para incentivar la inversión en IA, la que podría generar riqueza y resolver problemas endémicos de la región, como la baja productividad de sus factores de producción[55]. Tal como están las cosas, un informe de PricewaterhouseCoopers sugiere que América Latina estará a la zaga de otras regiones[56]. La falta de un marco jurídico adecuado es una de sus causas. La ausencia de reglas de juego claras, justas y eficientes podría exacerbar la desigualdad de la región, ya una de las más altas en el mundo, medida según el índice de Gini[57]. Para ello se requerirá de un Estado de derecho algorítmico, como punto de partida. Es decir, un marco jurídico donde personas físicas, jurídicas y artificiales estén sujetas por igual a la misma ley.

El derecho foráneo y el derecho comparado proveen instrumentos útiles y de bajo costo para guiar la labor del legislador latinoamericano[58]. Pocos países de América Latina tienen los recursos o el capital humano para producir innovaciones jurídicas. Como sugiere López Medina, los países desarrollados invierten y producen innovaciones jurídicas, mientras que los en desarrollo las replican, adaptan y

55 Ramiro Albrieu, Martín Rapetti, Caterin López Brest, Patricio Larroulet, & Alejo Sorrentino, *Inteligencia artificial y crecimiento económico. Oportunidades y desafíos para Argentina* (Buenos Aires; Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento, 2019).

56 PricewaterhouseCoopers, *Sizing the Prize* (PWC, 2019).

57 Marina Pasquali, *Latin America: Gini coefficient income distribution inequality, by country* (2020).

58 Mathias Siems, *Comparative Law*, 2nd ed. (Cambridge University Press. 2018), que el autor llama usos prácticos del derecho comparado a nivel local (*practical use at domestic level*).

transforman, con mayor o menor éxito[59]. La legislación de la UE se ha convertido en referente internacional en algunas áreas, por ejemplo, en materia de protección de datos, lo que ha llevado a que terceros países copien o se inspiren en la normativa unionística para reformar la propia (lo cual ha sido llamado por Bradford *efecto Bruselas)*[60]. En materia de regulación de la IA, el estudio del caso europeo proporciona lecciones útiles a bajo costo. Al fin y al cabo, las buenas ideas regulatorias son libremente apropiables. Por supuesto, no se trata de cortar y pegar indiscriminadamente. El éxito de un trasplante jurídico depende en gran medida de su aptitud y adaptabilidad a la realidad, idiosincrasia e instituciones del país receptor[61].

El estudio de la *Lex Algorithmica* que se insinúa en la UE, así como de su proceso de gestación provee, al entender de quien esto escribe, interesantes reflexiones. Algunas de ellas se condensan a continuación:

- La regulación de la IA no debe dejarse exclusivamente en manos de la tecnología, del mercado o a la voluntad de los actores económicos (CSR).
- La *Lex Algorithmica* no es probablemente una nueva rama del derecho, sino un área transversal, fruto de dar respuesta a los variados desafíos de un nuevo cambio de paradigma tecnológico: la *cuarta revolución industrial*.
- La *Lex Algorithmica*, holísticamente entendida, requiere de incentivos y refuerzos para que las empresas inviertan en I&D en el área de la IA, y a la vez de reglas claras para proteger los derechos fundamentales y las garantías del sistema democrático.
- Existe una evidente compensación (*trade-off)* entre una mayor protección de los derechos humanos y la efectividad algorítmica, que también impacta el bienestar de los ciudadanos. El legislador deberá encontrar el justo equilibrio entre ambos objetivos.
- La experiencia europea parece demostrar que para regular la IA son tan necesarias las reglas jurídicas tanto no vinculantes como vinculantes (*hard laws*). La relación parece ser de complementariedad, no de competencia. Sin embargo, cada una tiene su razón de ser y el ámbito de aplicación adecuado.

59 Diego López Medina, *Teoría impura del derecho: La transformación de la cultura jurídica latinoamericana* (Bogotá; Legis, 2004).

60 Ann Bradford, "The Brussels Effect," *Northwestern University Law Review* 107, n.º 1 (2012).

61 Ugo Mattei, "Efficiency in legal transplants: An essay in Comparative Law and Economics," *International Review of Law and Economics* 14, n.º 1 (1994): 3-19.

- El Estado de derecho algorítmico no es más que la adaptación de antiguas nociones a los tiempos que corren, para evitar que la tecnología eluda el imperio de la ley. El Estado de derecho algorítmico sujeta a las personas físicas, jurídicas y artificiales (SIA y robots) a las mismas reglas y principios jurídicos.
- Si bien en América Latina las amenazas y oportunidades que plantea la IA parecen lejanas, sus efectos ya empiezan a sentirse y probablemente se aceleren a corto plazo. Para no "perder el tren" los países deberían pensar legislaciones, estrategias y políticas públicas tanto a nivel nacional como regional[62], para minimizar lo malo y maximizar lo bueno que promete la IA.
- El estudio de la evolución de la *Lex Algorithmica* en la EU ofrece lecciones útiles, a bajo costo. Sin embargo, no bastará con copiar recetas foráneas. La labor de reflexión y adaptación local será imprescindible.

Bibliografía

Agencia Española de Protección de Datos. *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*. Madrid: AEDP, 2020.

Aguilar del Castillo, María del Carmen. "El uso de la inteligencia artificial en la prevención de riesgos laborales." *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo* 8, n.º 1 (2020): 262-93.

Albrieu, Ramiro, Martín Rapetti, Caterina Brest López, Patricio Larroulet y Alejo Sorrentino. *Inteligencia artificial y crecimiento económico. Oportunidades y desafíos para Argentina*. Buenos Aires: Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento, CIPPEC, 2019.

AlgorithmWatch. *AlgorithmWatch's Response to the European Commission's Proposed Regulation on Artificial Intelligence – A Major Step with Major Gaps*. Berlin: AlgorithmWatch, 2021.

62 Al respecto cabe destacar la labor de la Red Iberoamericana de Protección de Datos, que en 2019 publicara las *Recomendaciones Generales para el Tratamiento de Datos en Inteligencia Artificial* y las *Orientaciones Específicas para el Cumplimiento de los Principios y Derechos que Rigen la Protección de los Datos Personales en los Proyectos de Inteligencia Artificial*.

Buenadicha, César, Gemma Galdon, María Hermisilla, Daniel Loewe y Cristina Pombo. *La gestión ética de los datos.* Santiago de Chile: Banco Interamericano de Desarrollo, 2019.

Becker, Gary S. *The Economic Approach to Human Behavior*. Chicago: The University of Chicago Press, 1976.

Becker, Gary S. and William M. Landes (Eds.). *Essays in the Economics of Crime and Punishment*. New York: National Bureau of Economic Research, NBER, 1974.

Black, Julia. *Critical reflections on regulation*. London: Centre for Analysis of Risk and Regulation, London School of Economics and Political Science, 2002.

Bradford, Anu. "The Brussels Effect". *Northwestern University Law Review* 107, n.º 1 (2012): 1-68.

Castets-Renard, Céline. "Accountability of Algorithms in the GDPR and Beyond: A European Legal Framework on Automated Decision-Making." *Fordham Intellectual Property, Media and Entertainment Law Journal* 30, n.º 1 (2019): 91-137.

Castro, Daniel and Michael McLaughlin. *Ten Ways the Precautionary Principle Undermines Progress in Artificial Intelligence*. Washington: Information Technology & Innovation Foundation, 2019.

Castro, Daniel, & Michael McLaughlin. *Who Is Winning the AI Race: China, the EU, or the United States?* Washington: Information Technology & Innovation Foundation, 2021.

Chesterman, Simon. "Artificial Intelligence and the Limits of Legal Personality." *International & Comparative Law Quarterly* 69, n.º 4 (2020): 819-44.

Comisión Europea. Grupo de expertos de alto nivel sobre inteligencia artificial. *Directrices Éticas para una IA fiable.* Bruselas: CE, 2018,

Comisión Europea. *Libro Blanco sobre la inteligencia artificial - Un enfoque europeo orientado a la excelencia y la confianza*. Bruselas: CE, 2020.

Comisión Europea. *Propuesta de Reglamento por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión* Bruselas: CE, 2021 https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

Foss-Solbrekk, Katarina and Ann Kristin Glenster. "The Intersection of Data Protection Rights and Trade Secret Privileges in Algorithmic Transparency." In *Research Handbook on EU Data Protection Law*, edited by Eleni Kosta and Ronald Leenes. Holland: Edward Elgar Publishing, 2022.

Gal, Michal S. and Oshrit Aviv. "The Competitive Effects of the GDPR." *Journal of Competition Law & Economics* 16, n.º 3 (2020): 349-91.

Goodman, Bryce and Seth Flaxman. "EU Regulations on Algorithmic Decision-Making and a 'right to Explanation'." *AI Magazine* 38, n.º 3 (2016): 50-57.

Hildebrandt, Mireille. "Algorithmic regulation and the rule of law." *Philosophical Transactions of the Royal Society: Mathematical, Physical and Engineering Sciences* 376, n.º 2128 (2018).

Human Rights Watch (HRW). *The Toronto Declaration*. Toronto: Human Rights Watch, 2018.

Irakiza, Divin De Buffalo. "The Charter of Fundamental Rights, the Aims of EU Competition Law and Data Protection: Time to Level the Playing Field." *Singapore Journal of Legal Studies*, (2021): 39-55.

Jia, Jian; Ginger Zhe Jin and Liad Wagman. *The Short-Run Effects of GDPR on Technology Venture Investment*. Massachusetts: National Bureau of Economic Research, 2018.

Lessig, Lawrence. *Code 2.0*. Createspace, 2009.

Li, Zhuxi. "Machina Economicus: A Rational Mind." *The TSEconomist,* junio 6, 2017 https://thetseconomist.com/2017/06/06/machina-economicus-a-rational-mind/

López Medina, Diego. *Teoría impura del derecho: La transformación de la cultura jurídica latinoamericana*. Bogotá: Legis, 2004.

Lu, Sylvia. "Algorithmic Opacity, Private Accountability, and Corporate Social Disclosure." *Vanderbilt Journal of Entertainment & Technology Law* 23, n.º 1 (2020).

Maggiolino, Mariateresa. "EU Trade Secrets Law and Algorithmic Transparency." *(SSRN Electronic Journal*. https://ssrn.com/abstract=3363178Elsevier BV, 2019)

Mattei, Ugo. "Efficiency in legal transplants: An essay in Comparative Law and Economics." *(International Review of Law and Economics* 14, n.º 1. (1994),: 14.1: 3-19.

McGregor, L.orna, Daragh Murray, D., and & Vivian Ng, V. "International hHuman rRights lLaw as a fFramework for aAlgorithmic aAccountability." *(International and Comparative Law Quarterly* 68, n.º 2 (2019): 68.2: 309–3-43.

Mittelstadt, Brent Daniel, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter and Luciano Floridi. "The Ethics of Algorithms: Mapping the Debate". *Big Data and Society*, (2016): 1-21.

Oomen, Thomas L. *Why the EU Lacks behind China in AI Development – Analysis and Solutions to Enhance EU's AI Strategy*. Subang Jaya: Asia Study Centre, 2021.

Páez, Andrés. "Negligent Algorithmic Discrimination". *Law and Contemporary Problems* 84, n.º 3 (2021): 19-33.

Palmiotto, Francesca. "The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings." In *Algorithmic Governance and Governance of Algorithms*, edited by Martin Ebers and Marta Cantero. Switzerland: Springer International Publishing, 2020.

Pasquale, Frank. *The Black Box Society: The Secret Algorithms that Control Money and Information*. London: Harward University Press, 2019.

Pasquali, Marina. *Latin America: Gini coefficient income distribution inequality, by country*. 2020.

Patterson, Mark R. "Algorithmic Opacity and Exclusion in Antitrust Law." *Italian Antitrust Review* 5, n.º 1 (2018): 23-31.

Prause, Martin. "On the Trail of Machina Economicus." https://www.infosys.com/insights/ai-automation/machina-economicus.html

PricewaterhouseCoopers. *Sizing the Prize*. PWC, 2019.

Rai, Arun. "Explainable AI: From Black Box to Glass Box." *Journal of the Academy of Marketing Science* 48, n.º 1 (2020): 137-41.

Ramírez-Bustamante, Natalia y Andrés Páez. "Análisis jurídico de la discriminación algorítmica en los procesos de selección laboral." En *Innovación en derecho y nuevas tecnologías*, editado por René Urueña y Natalia Ángel. Bogotá: Ediciones Uniandes, 2020.

Red Iberoamericana de Protección de Datos. *Orientaciones específicas para el cumplimiento de los principios y derechos que rigen la protección de los datos personales en los proyectos de inteligencia artificial*. Naucalpan de Juárez: Red Iberoamericana de Protección de Datos, 2019.

Red Iberoamericana de Protección de Datos. *Recomendaciones generales para el tratamiento de datos en inteligencia artificial*. Naucalpan de Juárez: Red Iberoamericana de Protección de Datos, 2019.

Schwab, Klaus. *The Fourth Industrial Revolution*. Davos: World Economic Forum, 2016.

Selbst, Andrew D. and Julia Powles. "Meaningful Information and the Right to Explanation". *International Data Privacy Law* 7, n.º 4 (2017): 233-42.

Siems, Mathias. *Comparative Law*, 2nd ed. Cambridge: Cambridge University Press, 2018.

Tamanaha, Brian Z. *On the Rule of Law: History, Politics, Theory*. New York: Cambridge University Press, 2004.

The Organization for Economic Co-operation and Development (OECD). "Recommendation of the Council on Artificial Intelligence". https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

Weber, Max and Keith Tribe. *Economy and Society: A New Translation*. Cambridge, Mass.: Harvard University Press, 2019.

Yeung, Karen. "Algorithmic regulation: A critical interrogation." *Regulation & Governance* 12, n.º 4 (2018): 505-23;