El dilema de la transparencia algorítmica y los secretos empresariales. A cargo de Michelle Azuaje.

Deja un comentario / AD Internacional, Árbol del derecho, Mercantil, Nuevas tecnologías / Por A definitivas

AD 78/2020

El dilema de la transparencia algorítmica y los secretos empresariales

Michelle Azuaje Pirela[1]

Resumen: En el artículo se analiza el dilema jurídico que plantea el uso de algoritmos de inteligencia artificial (IA) protegidos por secretos empresariales frente a las crecientes obligaciones de transparencia en el uso de sistemas de IA.

Palabras clave: algoritmos, secretos empresariales, transparencia algorítmica, inteligencia artificial.

Abstract: The article analyzes the legal dilemma posed by the use of artificial intelligence (AI) algorithms protected by business secrets, against the increasing obligations of transparency in the use of AI systems.

Keywords: algorithms, business secrets, algorithmic transparency, artificial intelligence.

Introducción

Dentro de todo lo que rodea a la inteligencia artificial (IA) y a los nuevos modelos de negocios juegan un papel fundamental los algoritmos. Y es que con el uso de estos es posible extraer valor, obtener patrones e inferir información aplicando técnicas de *machine learning*[2] (aprendizaje automático) sobre grandes bases de datos. Lo más valioso de esta información es que ella puede convertirse en puntajes, clasificaciones, cálculos de riesgo, perfiles, u otros, que generan consecuencias muy importantes para la vida de las personas[3].

En ese sentido, de alguna manera los algoritmos están presentes en muchas actividades cotidianas, además "toman decisiones" o sirven de instrumento para ello; y se utilizan incluso para 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 creciente[4].

Por esas y otras razones, desde la perspectiva de la propiedad intelectual e industrial interesa proteger a los algoritmos. En efecto, la llegada de la cuarta revolución industrial ha traído consigo un incremento en el número de innovaciones relacionadas con el uso de sistemas de IA y de acuerdo con la Organización Mundial de la Propiedad Intelectual (OMPI), para el año 2019 se contabilizaron más de 340.000 solicitudes de patente relacionadas con la IA y 1.6 millones de documentos científicos publicados desde que se habló por primera vez de la IA en el decenio de 1950[5]. Sin embargo, en la actualidad una de las formas más recomendables para resguardar jurídicamente a los algoritmos es acogerse a la protección que proporciona el régimen especial de los secretos empresariales. Esto trae como consecuencia que ellos se mantienen normalmente en un plano de confidencialidad.

Ahora bien, si por una parte los algoritmos son secretos, por otra parte, su uso incrementado tanto en el ámbito público como en el privado ha puesto de relieve algunos dilemas ético-jurídicos. Esto porque algunos algoritmos han dado muestra de no ser tan objetivos como se esperaba generando consecuencias en ocasiones discriminatorias o violatorias de derechos fundamentales.

Así que, ante la eventualidad de la utilización de algoritmos injustos o sesgados que además tratan datos de carácter personal, en diversos ordenamientos a nivel mundial y particularmente en Estados Unidos y la Unión Europea, comienza a exigirse la "transparencia algorítmica" término que involucra 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 automatizadas que les afectan[6].

Pero esta exigencia -que es para algunos un derecho- deriva en un importante dilema pues implica otorgar transparencia a algo que desde otro punto de vista no la tiene o no puede tenerla: ¿Se puede explicar cómo funciona un algoritmo sin revelar el secreto empresarial que lo protege? ¿Deben las empresas tecnológicas revelar sus algoritmos?

Uno de los grandes desafíos asociados a la irrupción de la IA y su impacto en el Derecho se relaciona precisamente con la necesaria construcción de un marco jurídico adecuado en el que sea posible garantizar la transparencia algorítmica sin sacrificar la protección de los secretos empresariales.

Implicaciones de que un algoritmo esté protegido por secretos empresariales

En primer lugar, es necesario precisar que general los secretos empresariales se relacionan con cualquier información, relativa a cualquier ámbito de la empresa, incluido el tecnológico, científico, industrial, 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 secreto.[7] De esta forma, para que exista un secreto protegible por este régimen jurídico especial no es suficiente con que el titular de la información aduzca simplemente 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.

Precisado lo anterior, para entender en qué situaciones podría requerirse el acceso a algoritmos protegidos por secretos empresariales, piénsese por ejemplo que, en febrero de 2020, un Tribunal 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. La decisión fue tomada por considerar que el algoritmo vulnera el derecho a la privacidad de los ciudadanos, además de estigmatizar y discriminar a ciertos grupos de la población. SyRI compara bases de datos de pensiones, seguros, tipo de casa, impuestos, multas, integración, deudas, ingresos o subsidios de empleo para determinar quiénes son probables defraudadores, por lo que el tribunal consideró que "puede tener efectos no deseados, como estigmatizar y discriminar a la ciudadanía".[8]

En este orden de ideas un problema entre la transparencia algorítmica y la propiedad intelectual o industrial se plantearía en al menos dos situaciones. Por ejemplo, si para dar transparencia al funcionamiento del algoritmo,

alguna persona sometida a él solicita a la Administración Pública el acceso al código fuente y una copia del programa porque éste está protegido por el derecho de autor, y esto incluye el programa fuente o programa objeto (e incluso la documentación preparatoria, su descripción técnica y manuales de uso), de tal manera que dicho acceso tendría que ser denegado si el titular del derecho no consiente en ello. Además, revelar el código fuente implica revelar el algoritmo que, se ha dicho, normalmente es secreto y su revelación podría disminuir las ventajas competitivas de su titular.

No existen en las legislaciones nacionales actuales normas que resuelvan expresamente una situación como la planteada.[9] Pero en cambio sí sobreviven en algunas legislaciones sobre acceso a la información pública normas en base a las cuales 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.[10]" En este último supuesto se incluyen los secretos empresariales, pero por medio del uso de ellos se podría afectar por ejemplo la esfera de la vida privada de las personas que está igualmente protegida.

De esta forma, en el ámbito público la protección de los secretos empresariales opera como un límite a la transparencia, pero en el contexto de la complejidad del fenómeno de la IA esto podría derivar en situaciones desequilibradas, injustas o resultar lesivo de otros derechos que también gozan de rango constitucional como el derecho a la igualdad y no discriminación y el derecho a la protección de datos personales, entre otros.

Algunas soluciones planteadas hasta ahora

Dado que, en muchos casos, con el uso de sistemas de IA se captan, tratan y almacenan datos personales, la tendencia es que las empresas tecnológicas que pretendan utilizarlos deban cumplir con ciertos estándares, derivados de nuevas categorías de derechos. En ese sentido, en la Unión Europea se ha desarrollado un vasto cuerpo de Documentos, Resoluciones, Declaraciones y Directivas encaminadas a la protección de los datos personales desde una perspectiva de derechos fundamentales, que se espera vaya trasladándose a las legislaciones de los Estados miembros, aunque sus efectos pueden extenderse incluso fuera de la Unión.

Entre dichos instrumentos 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, el Parlamento Europeo propugna "la responsabilidad y la transparencia algorítmica"[11]. Y, en virtud del GDPR, se proponen los más elevados estándares de protección de datos personales desde la fase de diseño que deben cumplir tanto instituciones públicas como privadas. Por tal motivo, los procesos de aprendizaje automático deben hacerse confiables y transparentes[12], más aún si involucran tratamiento de datos personales.

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 utilizados por los algoritmos de IA para hacer inferencias. Asimismo, recomienda que las empresas lleven a cabo 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 equidad.[13]

Por su parte, de acuerdo con el GDPR, se 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."

Esto incluye, el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión. En el mismo orden, en el considerando 71 se establece que el titular tiene derecho a "a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión." No obstante, no queda claro cuál es el alcance de dicha explicación y qué hacer si ella implicase la revelación de un secreto empresarial.

Por otra parte, conforme al GDPR es imperativo no confiar únicamente en las manifestaciones de fabricantes y distribuidores, sino que obligatoriamente se establecen mecanismos basados en terceros confiables para determinar el cumplimiento de los niveles necesarios de calidad y confiabilidad de los sistemas de IA. Estos mecanismos pueden materializarse 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 es posible 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 y en el Considerando 100, 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.[14]

Sin embargo, el régimen descrito solo se aplicará en relación con la protección de datos personales el cual por cierto, se ha sostenido sobre un modelo de consentimiento que algunos afirman está quebrado y no es sostenible frente a la complejidad del contexto tecnológico de la IA.[15] Así que aunque ofrece un elevado estándar de protección es posible que otros derechos fundamentales que puedan entrar en conflicto con el secreto empresarial u otros derechos de propiedad intelectual, queden fuera de dicho marco si no se articulan

medidas adicionales.[16] Por eso en el derecho anglosajón se han propuesto otras alternativas como realizar auditorías por terceros independientes a los algoritmos[17] y, otras más tecnológicas como el uso de herramientas de software para detectar y/o mitigar los sesgos en los algoritmos. Es decir, utilizar algoritmos para que auditen a otros algoritmos.[18]

Conclusiones

A pesar de las alternativas que se han esbozado para promover la transparencia de los algoritmos cabe preguntarse si dichas iniciativas por sí solas serán suficientes cuando se generen conflictos con derechos de propiedad intelectual e industrial. Frente a esto se hace necesario analizar en paralelo algunas categorías tradicionales de este régimen 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 los privilegios y pequeños monopolios legales que confieren los derechos de propiedad intelectual incluidos los secretos empresariales, cuando estos entran en pugna con otros derechos fundamentales.

Así, por una parte, conviene analizar la posibilidad de incluir en los sistemas vigentes algunas disposiciones que flexibilicen la protección de los algoritmos *per se* para que estos puedan ser públicos, explicables y protegibles frente a la copia. Conviene también crear un nuevo régimen especial relativo a los secretos empresariales que incluya un catálogo de límites y excepciones con el objeto de aumentar los niveles de acceso y transparencia. Y finalmente, estas u otras medidas pueden complementarse con la adopción de sistemas de certificación. En todo caso, frente a un conflicto de derechos en los que se exija el acceso en el ámbito público, la confidencialidad tendrá que ser justificada y fundamentada para que pueda ser mantenida, debiéndose ponderar en cada caso si prevalecen los derechos e intereses protegidos por el secreto empresarial o los derechos e intereses de quienes requieren que este sea divulgado.

Michelle Azuaje

3 de junio de 2020

Referencias

Agencia Española de Protección de Datos (2020): "Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción" [en línea], texto disponible en https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

Arellano Toledo, W. (2019): "El derecho a la transparencia algorítmica en *big data* e inteligencia artificial", *Revista General de Derecho Administrativo*, 50, 3.

Chowdhury, R. & Mulani, N. (2018): "Auditing Algorithms for Bias" [en línea], texto disponible en: https://hbr.org/2018/10/auditing-algorithms-for-bias

Comisión europea (2019): "Directrices éticas para una IA fiable. Grupo de expertos de alto nivel sobre inteligencia artificial" [en línea], texto disponible en: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top

Comisión europea (2020): "White paper On Artificial Intelligence – A European approach to excellence and trust" [en línea], texto disponible en: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

Cotino Hueso, L. (2017): "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales" [en línea], *Dilemata*, 24, texto disponible en: https://ssrn.com/abstract=3413277

Ferrer, Isabel (2020): "Países Bajos veta un algoritmo acusado de estigmatizar a los más desfavorecidos" [en línea], texto disponible en: https://elpais.com/tecnologia/2020/02/12/actualidad/1581512850_757564.html

Guszcza, J.; Rahwan, I.; Bible, W.; Cebrian, M. & Katyal, V. (2018): "Why We Need to Audit Algorithms" [en línea], *Harvard Business Review*, textodisponible en:https://hbr.org/2018/11/why-we-need-to-audit-algorithms

Lomas, N. (2018): "IBM launches cloud tool to detect AI bias and explain automated decisions" [en línea], texto disponible en: https://techcrunch.com/2018/09/19/ibm-launches-cloud-tool-to-detect-ai-bias-and-explain-automated-decisions/

Parlamento Europeo (2017): 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. (2015): The Black Box Society: The Secret Algorithms That Control Money and Information, Londres, Harvard University Press, 4.

Rubinstein, I. (2013): "Big Data: The End of Privacy or a New Beginning?", International Data Privacy Law, NYU School of Law, Public Law Research Paper, 12-56. SSRN.

Solove, D. (2013): "Autogestión de la privacidad y el dilema del consentimiento", Revista Chilena de Derecho y Tecnología, 2(2),11-47. doi:10.5354/0719-2584.2013.30308.

World Intellectual Property Organization (2019): "WIPO Technology Trends 2019: Artificial Intelligence" [en línea], texto disponible en: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf

[1] Doctora en Derecho, Universidad Autónoma de Chile. Académica e Investigadora, Coordinadora del proyecto IA+D: Inteligencia Artificial y Derecho, Universidad Autónoma de Chile, Temuco, Chile. Correo electrónico: michelle.azuaje@uautonoma.cl.

[2] *Machine learning* es el 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.

[3] Pasquale (2015) 4.

[4] Arellano (2019) 3.

[5] WIPO (2019).

[6] Cotino (2017) 142; Arellano (2019) 4.

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

[8] Ferrer (2020).

[9] De hecho, el régimen jurídico de los secretos empresariales ha sido históricamente uno de los más difusos del sistema de propiedad intelectual e industrial (incluso hay quienes niegan que pertenezca a él), por eso normalmente está dispersos en normas tales como códigos penales, leyes de propiedad industrial, de libre competencia, entre otras, siendo extraño encontrar en las legislaciones normas expresamente dirigidas al establecimiento de límites y excepciones a estos lo que sí ocurre por ejemplo, en materia de derecho de autor. Sin embargo, en el derecho español, recientemente entró en vigor la Ley 1/2019, de Secretos Empresariales (LSE) que contiene una regulación transversal del secreto empresarial. A través de ella se transpone la Directiva (UE) 2016/943, y se 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 límites. 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, lo que podría implicar en algunos casos la obligación de comunicar información confidencial a las autoridades administrativas o judiciales en el ejercicio de sus funciones en virtud de las obligaciones o prerrogativas que les hayan sido conferidas por el Derecho europeo o español.

[10] Véase por ejemplo la Ley 20.285, sobre acceso a la información pública en Chile, de acuerdo con la cual los organismos públicos tienen el deber de recibir solicitudes de información y entregar ésta, pero podrán abstenerse de aquello cuando exista un motivo de secreto o reserva. En ese sentido, conforme al artículo 21 N° 2

de la misma ley, los secretos empresariales forman parte de la categoría de derechos comerciales o económicos; y estos a su vez gozan de protección constitucional de acuerdo con el artículo 19 N° 25 de la Constitución Política chilena. En términos similares, en España la Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno, establece en su artículo 21. 1 g) que el derecho de acceso a la información pública puede ser denegado o restringido si el conocimiento o divulgación de la información conlleva un perjuicio para el secreto profesional y los derechos de propiedad intelectual e industrial.

[11] Parlamento Europeo (2017) Cons. N; Cons. general. 1 y 21.

[12] 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 (2019) 168; Comisión Europea (2020) 9.

[13] Parlamento Europeo (2017) Cons. general 21.

[14] Agencia Española de Protección de Datos (2020) 34.

[15] Rubinstein (2013) 1; Solove (2013) 11-47.

[16]Cotino (2017) 146.

[17] Guszcza et. al (2018).

[18] Lomas (2018); Chowdhury y Mulani (2018).

Michelle Azuaje Pirela

Académica e Investigadora, Coordinadora del proyecto IA+D: Inteligencia Artificial y Derecho, Universidad Autónoma de Chile, Temuco, Chile. Correo electrónico: michelle.azuaje@uautonoma.cl.

La profesora Azuaje Pirela es Doctora en Derecho por la Universidad Autónoma de Chile, Máster en Derecho de la Empresa por la Universidad de Alcalá de Henares, Especialista en Mediación para la Resolución de Conflictos por la Universidad de La Rioja y Abogada por la Universidad del Zulia. Además, es autora de diversas publicaciones en las áreas de Derecho Tributario y Derecho de la Propiedad Intelectual y es corresponsal para Chile de la Asociación para el Estudio y la Enseñanza del Derecho de autor (ASEDA).

Su actual agenda de investigación se encuadra dentro de la línea de Regulación Económica y se fija en el análisis del impacto de la Inteligencia Artificial en el Derecho y, particularmente en el Derecho de Propiedad Intelectual.

Redes sociales:

LinkedIn: https://www.linkedin.com/in/michelleazuajep/

Twitter: @michelleazuajep

Twitter Proyecto IA+D: @IADerecho_UA

Comparte esto:

Me gusta esto:

Cargando...

Relacionado

¡LA INTELIGENCIA ARTIFICIAL Y SUS "BIAS" EN EL SISTEMA DE JUSTICIA! A cargo de la Mg. Karin Tafur
En «AD Internacional»

Desarrollo de la IA en relación con la Protección de Datos de Carácter Personal, la ética y la desigualdad. A cargo de Marta Vargas González.
En «Árbol del derecho»

¡Sonríe! la inteligencia artificial te está "interpretando" A cargo de Michelle Azuaje-Pirela
En «AD Internacional»

← Entrada anterior

Entrada siguiente →

Deja un comentario

Introduce aquí tu comentario...

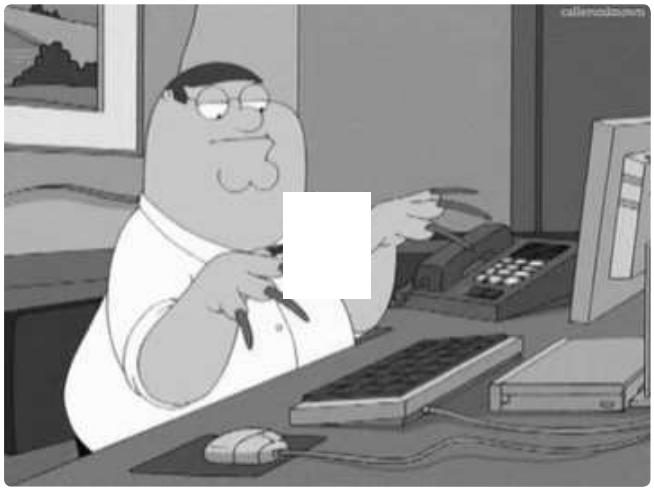
Buscar ...

Lo más leído del día:

Tweets por @A_definitivas

A definitivas - Portal Jurídico
@A_definitivas
En respuesta a @A_definitivas
Además, podemos elaborar los avisos legales para tu página web y demás exigencias y particularidades legales que tiene estar presente en internet

¡No lo dudes y contáctanos en Hola@adefinitivas.com!



25 jun. 2021

Insertar Ver en Twitter

ADEFINITIVAS
COMPARTIMOS DERECHO

Publicación editada en Palma, con número de ISSN: 2605-485X

Condiciones de Uso y Privacidad

Política de Cookies