GuIA.ai

Derechos de propiedad intelectual y transparencia de los sistemas de IA: un análisis desde el ordenamiento jurídico mexicano

Jorge Luis Ordelin Font

Noviembre 2021

CETyS | LATAM DIGITAL CENTRO DE POLÍTICA DIGITAL PARA AMÉRICA LATINA | En colaboración con: fAIr LAC | BID Banco Interamericano de Desenvolvimento

Derechos de propiedad intelectual y transparencia de los sistemas de IA: un análisis desde el ordenamiento jurídico mexicano

Autor: Jorge Luis Ordelin Font

Coordinadoras: Carolina Aguerre y Maia Levy Daniel

Revisión: Gonzalo Bustos Frati y Matías Jackson

Diseño: Mónica Castellanos

Edición: Paula Álvarez Arbelais

Licencia Internacional Pública de Atribución/ReconocimientoNoComercial-SinDerivados 4.0 de Creative Commons.

Las opiniones expresadas en las publicaciones incumben únicamente a los/as autores/as. No tienen intención de reflejar las opiniones o perspectivas del CETyS, CLD ni de ninguna otra organización involucrada en el proyecto.

Derechos de propiedad intelectual y transparencia de los sistemas de IA: un análisis desde el ordenamiento jurídico mexicano

Noviembre 2021

Jorge Luis Ordelin Font

Profesor y consultor en propiedad intelectual. Investigador del Sistema Nacional de Investigadores de México (SNI-1). Posdoctorado en Derecho (PNPD/CAPES), con especialización propiedad intelectual. Facultad Meridional IMED, Brasil. Doctor en Ciencias Jurídicas por el Tribunal Nacional de Grados Científicos de la República de Cuba. Magíster en propiedad intelectual por la Universidad Austral y la OMPI. Máster en Derecho Civil, Universidad de La Habana, Cuba. Miembro de la Línea de Investigación Derecho e Inteligencia Artificial del Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México (UNAM). Email:jlordelin@gmail.com

Resumen ejecutivo

Uno de los mayores retos que existen en materia de inteligencia artificial es cerrar o disminuir la brecha entre la transparencia como aspiración ética de estos sistemas y la regulación nacional de los derechos de propiedad intelectual. A partir de este contexto el presente trabajo tiene como objetivo analizar el régimen jurídico de los derechos de propiedad intelectual de protección de los sistemas de IA en correspondencia con el principio de transparencia de estos, tomando como objeto de análisis el ordenamiento jurídico mexicano. Para su elaboración se utilizaron métodos de investigación cualitativa. A partir del análisis teórico jurídico se explica la relación entre los derechos de propiedad intelectual y el principio de transparencia de un sistema de IA fiable, mientras que el análisis de contenido de normas jurídicas permite abordar esta relación en el ordenamiento jurídico mexicano. La principal conclusión a la que se arriba es que los derechos de propiedad intelectual no deberían constituir una barrera para garantizar la materialización del principio de transparencia de los sistemas de inteligencia artificial.

Contenido

1. Introducción

Desde el ámbito legal y ético existen múltiples debates sobre la regulación internacional de los sistemas de inteligencia artificial (en adelante IA). A nivel internacional, por ejemplo, la Unesco ha reconocido que los valores y principios éticos no son normas jurídicas, aunque coadyuvan a la armonización de las normas jurídicas, su elaboración y aplicación, y proporcionan orientación cuando el ámbito de estas normas no esté claro o cuando no se haya establecido debido a la rapidez del desarrollo tecnológico (2020). A nivel nacional confluyen normas jurídicas de diversa naturaleza, que van desde la protección de los derechos fundamentales (protección de datos, privacidad, igualdad, etcétera) hasta la protección de consumidores y responsabilidad civil, entre otros. Como ha examinado la Unión Europea, es necesario analizar si este marco regulatorio heterogéneo y difuso puede hacer frente a los riesgos que el uso de esta tecnología representa, en otras palabras, si es posible su observancia o si es preciso su adaptación o creación (Comisión Europea, 2020).

Uno de los regímenes jurídicos que interviene en la gobernanza de estos sistemas son los derechos de propiedad intelectual. Estos pueden o no impedir la monopolización de la IA, mientras que, por otro lado, impactan en el cumplimiento de los requisitos para una IA fiable. Los derechos de propiedad intelectual son derechos exclusivos que otorgan a sus titulares un monopolio jurídico. Su no reconocimiento sobre estos sistemas, como creaciones y/o invenciones podría desalentar la innovación en este campo tecnológico, mientras que, por otro lado, una protección excesiva podría ser disfuncional y también provocar el mismo efecto, desincentivar la innovación (Hilty, Hoffmann, Scheuerer, 2020). Es importante apuntar que no solo las normas de propiedad intelectual podrían provocar esta disminución de incentivos, dado que legislaciones demasiado estrictas en otras materias también podrían generar las mismas consecuencias[1]. En relación con los derechos de propiedad intelectual la creación de monopolios sobre la investigación, los datos, la tecnología y el mercado impactan sobre la aplicación y sus beneficios en la solución de problemas sociales al crear exclusiones de uso por parte de los titulares de derechos.

En principio, se pueden identificar al menos tres grandes tensiones que existen desde el ámbito de la propiedad intelectual y la gobernanza de los sistemas de IA:

1. Existencia de los mecanismos de certificación de estos sistemas viables y los sistemas de registros de propiedad intelectual: ¿es posible conceder protección a la propiedad intelectual cuando estos sistemas se encuentren sesgados? ¿Cuál o cuáles serían los criterios de valor para establecer criterios de protección? ¿Quién o quiénes los determinarían y aplicarían?

2. ¿Cuál es la relación que existe entre la opacidad y transparencia de los sistemas de inteligencia artificial y los derechos de propiedad intelectual?

1 V. gr. El establecimiento de cargas desproporcionadas a pequeñas y medianas empresas, como podría ser la certificación de los sistemas generados por estas.

3. ¿Se podría hablar de un régimen jurídico para los datos utilizados para entrenar el sistema de IA? La propiedad intelectual o cualquier otra forma de protección de datos podría devenir en una barrera para el acceso a estos y, por ende, al conocimiento que podría aportar la utilización de esta tecnología.

Este trabajo aborda la segunda de estas tensiones, es decir, el impacto de la regulación de los derechos de propiedad intelectual en la opacidad y transparencia de los sistemas de inteligencia artificial. Las principales preguntas de trabajo fueron las siguientes: ¿la concepción de un sistema de inteligencia artificial transparente es contradictoria con las normas de propiedad intelectual? ¿Son suficientes las previsiones legales establecidas en el ordenamiento jurídico mexicano para garantizar la transparencia de estos sistemas y su equilibrio con las normas de propiedad intelectual?

El **objetivo** perseguido es analizar el régimen jurídico de los derechos de propiedad intelectual de protección de los sistemas de IA acorde con el principio de transparencia de estos sistemas, tomando como objeto de análisis el ordenamiento jurídico mexicano. En correspondencia con este objetivo el documento se divide en dos apartados fundamentales, el primero dirigido a explicar la relación que existe entre el principio de transparencia de un sistema de IA fiable y los derechos de propiedad intelectual, incluyendo los secretos empresariales como mecanismo de protección, y, el segundo, cómo esta relación es solventada desde la actual regulación del ordenamiento jurídico mexicano. La relación entre la transparencia y los derechos de propiedad se aborda desde tres perspectivas fundamentales: cómo los tipos de protección de los derechos de propiedad intelectual pueden incidir o afectar el régimen de transparencia de un sistema, en qué supuestos o tipo de transparencia es necesario acceder a la protección que brinda los derechos de propiedad intelectual, y cómo se puede garantizar esta protección durante las diferentes etapas del ciclo de vida del sistema, teniendo en cuenta que la transparencia no es estática sino un proceso que debe ser garantizado durante todas las etapas de existencia del sistema.

Para su realización se ha utilizado una metodología cualitativa y métodos de investigación relacionados tanto con las Ciencias Sociales como Jurídicas, en particular el análisis teórico-jurídico y el análisis de contenido de normas jurídicas. Se toma como punto de referencia el ordenamiento jurídico mexicano. Por sus condiciones de desarrollo tecnológico en materia de inteligencia artificial, su ordenamiento jurídico y sus condiciones económicas y sociales, México es un país que reviste especial interés sobre hacia dónde se puede avanzar o no en la concepción de sistemas de IA fuertes e innovadores.

Como principal resultado se propone establecer una relación entre el tipo o nivel de profundidad de transparencia que es necesario garantizar y el acceso a la información de los sistemas de IA que pudiera estar protegida por derechos de propiedad intelectual. La configuración de un sistema armónico de protección y respeto de los derechos de propiedad intelectual y la obligación de transparencia parten del tipo de protección de estos sistemas, así como de las previsiones regulatorias y contractuales que entorno a este existen. Los derechos de propiedad intelectual no deberían constituir una barrera para evaluar los algoritmos, el uso de datos y los procesos de diseño de los sistemas de IA.

2. La transparencia como principio para una IA fuerte

La concepción de una IA fiable se apoya en tres componentes sustanciales: 1) debe ser lícita de modo que garantice el respeto de los derechos fundamentales, las leyes vigentes y los principios y valores esenciales, 2) debe ser ética, al permitir la garantía de un "fin ético", y 3) debe ser robusta, tanto desde un punto de vista técnico como social (Comisión Europea, 2019, p. 6). Entre los principios para el diseño y uso responsable de los sistemas de IA, también denominado *Fast Track Principles* (FTP por sus siglas en inglés), se encuentran la equidad, responsabilidad, sostenibilidad y transparencia, todos estrechamente interrelacionados.

De forma particular el término transparencia se relaciona con múltiples conceptos y cumple muchas funciones. Pese a la importancia que adquiere este principio para la gestión de los sistemas de IA no siempre queda determinado su alcance y cómo se materializa. Por lo general existen confusiones en cuanto a su sentido y alcance. La complejidad recae tanto en el concepto, qué entender por transparencia como en el objeto sobre el que esta recae. No hay dudas que este último determina la primera como un proceso complejo, integrador relacional y no estático, en el que existen diferencias entre el ideal normativo y su aplicación práctica.

La transparencia del sistema se asocia a la posibilidad de que este pueda ser observado y entendido con facilidad (Oliver, 2018). No solo en relación con los datos que utiliza el sistema, sino también, cómo funciona y el derecho de las personas a saber que está interactuando con sistemas artificiales. En otras palabras, conocer cómo se recogen los datos, las necesidades de estos en función del algoritmo, las fuentes de donde provienen, cómo se alimenta el sistema, su continuo de mejoramiento y autoajuste. (Qiang, 2018, p. 22).

En palabras de Hamon, Junklewitz y Sanchez no es más que "la documentación de la cadena de procesamiento de la IA, incluidos los principios técnicos del modelo, y la descripción de los datos utilizados para la concepción del modelo, incluidos cualquier elemento que proporcione una buena comprensión del modelo y relacionado con su interpretabilidad y explicabilidad" (2020, p. 2). Según la OCDE un sistema es transparente si proporciona información significativa, adecuada al contexto y coherente con el estado de la técnica; si las partes son conscientes de su interacción con éste, incluso en el lugar de trabajo; si permite que los afectados por un sistema de IA comprendan el resultado; y los afectados negativamente por su utilización cuestionen su resultado basándose en información fácil de entender, particularmente en relación con los factores y la lógica que sirvió de base para la predicción, recomendación o decisión (2019).

Sin embargo, lo cierto es que la aplicabilidad práctica de estos conceptos es mucho más compleja que las conceptualizaciones anteriormente planteadas. Al decir de Felzmann *et al*., ello provoca una brecha entre la aspiración y la realidad, movido en parte por la concepción amplia y difusa del término y por otro por la complejidad intrínseca del objeto de la transparencia, el algoritmo. Por ende, su concepción no puede verse limitada solo a la transferencia de información de un agente a otro, sino que resulta indispensable prestar atención a los significados, valores

y funciones sociales asociados a esta; en otras palabras, al carácter normativo y social que subyace en dicho concepto (Felzmann *et al*., 2020).

Siguiendo a Felzmann *et al*., (2020) es necesario integrar tres perspectivas de la transparencia para poder comprender su papel en los sistemas de IA. Una normativa, otra relacional y por último una sistémica. La noción normativa evalúa el comportamiento de agentes, sistemas u organizaciones, sus operaciones, intenciones o consideraciones. Si bien esta perspectiva es importante no especifica el destinatario o la audiencia a la que un actor debe ser transparente, aunque sí lo hace la perspectiva relacional: se analiza no desde una característica individual sino de la relación que existe entre el agente y el receptor, cómo el destinatario recibe y comprende la información. El diseño y evaluación de la medida se realiza teniendo en cuenta el impacto en las partes interesadas. Por último, la perspectiva sistémica toma en cuenta el contexto institucional de las relaciones de transparencia, dígase medidas legales, reglamentarias y organizativas asociadas. Este contexto es esencial para una comprensión realista del probable impacto práctico y su implementación efectiva, incluyendo el papel y eficacia de la rendición de cuentas.

El deber ser de un sistema de IA fiable toma en cuenta, entre otros criterios, la explicabilidad del sistema, la calidad e intención del proceso, sus resultados y cómo estos se producen (Comisión Europea, 2019, p. 6). Se halla estrechamente relacionada con la confianza, la autonomía, un mayor nivel de control y la rendición de cuentas. La falta de transparencia constituye uno de los principales riesgos a los que es necesario responder ante el desarrollo de esta tecnología, especialmente en cuanto a minimizar las posibilidades de que con el uso de esta tecnología se repliquen, refuercen y prolonguen los sesgos y errores preexistentes. Todo lo cual se podría traducir en la manipulación de comportamientos, el uso deshonesto, el desplazamiento laboral y la apropiación de la tecnología, entre otros (Herrera, 2019, p.15).

La transparencia es piedra angular de la gobernanza del sistema y en particular de su confianza, forma parte del conjunto significativo de salvaguardias que deben ser adoptados para convertir a los seres humanos en el centro de la toma de decisiones algorítmicas. En dependencia de su implementación práctica e información obtenida las personas pueden continuar utilizando o dejar de utilizar los sistemas de información, al propio tiempo que contribuye a aumentar la confianza y lealtad de los consumidores. Empero, ello no significa que la transparencia por sí sola garantice la efectividad del sistema y su precisión. Para lograr dicha confianza es necesario que sean tenidos en cuenta otros factores como son las expectativas del usuario, la implementación de la transparencia, tecnologías, factores individuales y contexto cultural (Felzmann *et al*., 2020).

Existe una relación directa entre la transparencia, la explicabilidad de los sistemas, la gobernanza de la responsabilidad algorítmica, los procesos de auditoría algorítmica y las evaluaciones de impacto algorítmicas. Un sistema de IA transparente también posibilita la atribución de responsabilidad y las consecuencias de su uso, en correspondencia con el rol de cada uno de los actores, el contexto y el estado de desarrollo de la tecnología. Desde un sistema objetivo, el riesgo y el daño no son asociados a la intencionalidad o culpa puesto que, aunque existan intenciones de no provocar un daño estos pueden estar presentes. De ahí que la transparencia tenga un peso importante en la identificación y gestión de los riesgos.

Aunque se hallan intrínsecamente relacionadas no se puede confundir la transparencia asociada al dato personal con la del sistema. Esta última, también denominada transparencia sistémica, es más profunda que el régimen de transparencia individualizado que recae sobre el titular del dato personal. La transparencia asociada a la calidad de la información sobre el sistema no puede ser solo analizada en relación con la protección de datos personales, sino en relación con el funcionamiento propiamente dicho del sistema. Si bien esta interrelación es indisoluble es importante su delimitación, a los efectos de poder tener claridad en relación con la responsabilidad del sistema. La transparencia individual no es suficiente especialmente en relación con la construcción del algoritmo o su desempeño continuo. En el primer caso la transparencia opera posterior al desarrollo algorítmico cuando la responsabilidad o corrección del sistema es más compleja, es continua y se implementa desde la primera etapa de desarrollo de un algoritmo.

La transparencia asociada a la protección de los datos personales está determinada por el hecho de que los titulares de estos tengan conocimiento de su uso, autoricen de forma expresa el mismo, conozcan los supuestos en los cuáles se modifiquen los fines inicialmente previstos, pero también, de los procesos de disociación de la información, la preservación de su identidad, posibilidades de riesgo, reversión del procedimiento de anonimización o el sometimiento a un proceso de seudonimización, etcétera.

3. La transparencia de los sistemas de IA y los derechos de propiedad intelectual: en la búsqueda de un equilibrio

La relación entre los derechos de propiedad intelectual y la transparencia de los sistemas de IA constituye uno de los supuestos más complejos de superposición entre la IA y la propiedad intelectual. Como se ha afirmado, estos últimos podrían crear barreras y plantear un conflicto de normas entre la protección de la propiedad intelectual y la necesidad social de transparencia y rendición de cuentas (Castets-Renard, 2020).

La opinión formulada por la Comisión de Mercado Interior y Protección del Consumidor del Parlamento Europeo del 9 de julio de 2020 reconoció la necesidad de reconciliar los derechos de propiedad intelectual, incluidos los secretos comerciales, con la aplicación de otros objetivos de políticas públicas, como el respecto de los derechos y libertades fundamentales (apartado 4). De manera similar el grupo de expertos de la Comisión Europea que elaboró las directrices éticas para una IA fiable reconoció la incidencia de los derechos de propiedad intelectual en la materialización del principio de equidad y el respeto de la proporcionalidad entre los intereses y objetivos contrapuestos. Dicho grupo señaló que la proporcionalidad entre el usuario y el responsable del despliegue parte de tener en cuenta los derechos de propiedad intelectual de las empresas y los derechos de los usuarios (Comisión Europea, 2019, p. 15).

Garantizar los estándares de transparencia depende en gran medida de un marco de gobernanza colaborativa, en el sentido no solo de la capacidad de que el sistema se desempeñe como se espera o prometió, también supone que los diferentes actores estén dispuestos a revelar dicha información (Felzmann *et al.*, 2020). Para Felzmann *et al*., en cualquiera de las etapas del proceso de transparencia es necesaria la transmisión de conocimientos, documentación e instrucciones oportunas, solo de esta forma es posible garantizar que los diversos actores del ciclo de vida del sistema se encuentren comprometidos con su transparencia y sean responsables por el rol que desempeñan. Sin embargo, no nos puede ser ajeno que los derechos de propiedad intelectual pueden limitar el ejercicio de esta transmisión de información y documentación, en dependencia de los titulares y las formas de protección que se han utilizado.

Los derechos de propiedad intelectual tienen un efecto directo en la denominada opacidad intencional de los sistemas de IA. Este tipo de opacidad también se ha denominado barreras de acceso privadas (Felzmann *et al.*, 2020), y permite que los terceros sean excluidos deliberadamente del acceso al *software* y al algoritmo del sistema de IA con el fin de proteger la titularidad del primero así como mantener el valor comercial y competitivo del sistema de IA en el mercado. La opacidad intencional o de protección de la propiedad o secreto corporativo se relaciona con otras formas de opacidad de conjunto con las cuales debe ser analizada, la de conocimiento y la intrínseca, determinada esta última por la complejidad del sistema y su interpretabilidad[2].

2 Burrell habla de tres formas de opacidad, "(1) la opacidad como autoprotección y ocultación corporativa o institucional intencional, es decir la posibilidad de un engaño consciente; (2) opacidad derivada de la situación actual en la que escribir (y leer) código es una habilidad especializada y; (3) una opacidad que surge del desajuste entre la optimización matemática en la característica de alta dimensionalidad del aprendizaje automático y las demandas del razonamiento a escala humana y los estilos de interpretación semántica" (2016).

A medida que los sistemas son más complejos pueden procesar una mayor cantidad de datos y al mismo tiempo son más difíciles de interpretar. (Oliver, 2018, p. 26). Las limitaciones técnicas están ligadas a la naturaleza autónoma, compleja y escalable de la IA. Los algoritmos y el código son muy técnicos y complejos. No es solo la capacidad de leer el código, que ya de por sí es una habilidad especializada que no se encuentra en el público en general. Los modelos que resultan útiles por su precisión son cada vez más complejos y esto parece ser inevitable. Por ende, será cada vez más común que la comprensión e interpretación del sistema puede escapar por parte de los humanos, incluso para aquellos especializados, existe un desajuste entre los procedimientos matemáticos de los algoritmos de aprendizaje automáticos y los estilos humanos de interpretación.

Cada una de estas formas de opacidad deberá ser abordada a partir de diferentes estrategias herramientas y enfoques que van desde lo legislativo hasta lo organizativo o programático y técnico. Es necesario identificar el tipo para poder ser mitigada conforme a un plan de acción determinado en el que convergen soluciones técnicas y no técnicas, de disímil naturaleza como son aspectos regulatorios, tipos de auditorías, alternativas más transparentes como el código abierto, educación del público, sensibilización de los programadores, entre otros. Por ende, dado que en este trabajo se aborda particularmente la denominada opacidad intencional o la que tiene lugar a partir de la protección de la propiedad o secreto corporativo es importante comprender los límites de la propuesta que se analiza en este trabajo. Ello no implica que por sí sola se pueda cumplimentar con las demandas de transparencia, forma parte de un problema más complejo y, por ende, constituye una parte de la solución mas no la única.

Buscar un equilibrio entre estos sistemas no es algo fácil ni sencillo de solucionar. Para algunos autores, como Oliver, este tipo de opacidad se puede mitigar mediante la utilización de *software* abiertos, sin embargo, no puede desconocerse la existencia de intereses económicos y comerciales sobre estos tipos de desarrollo, por lo cual, aunque deseable no es posible aspirar a que este sea el tipo de protección que sería utilizada en todos los supuestos.

En este sentido, la propuesta de reglamento de la UE conmina que la obligación de transparencia no afecte de manera desproporcionada el derecho a la protección de la propiedad intelectual. Se podría decir que implícitamente se reconoce una afectación o al menos una incidencia. Asimismo, reconoce a la propiedad industrial y mercantil como una causal de excepción a la evaluación de la conformidad, de conjunto con la seguridad pública, la protección de la vida y la salud de las personas físicas. Aunque no se establecen de forma clara los supuestos bajo los cuales operaría la misma, sí queda clara su excepcionalidad teniendo en cuenta la rápida disponibilidad de las tecnologías innovadoras, su impacto en la salud, la seguridad de las personas y de la sociedad en su conjunto (considerando 68).

Para Castets-Renard (2020), satisfacer los objetivos de transparencia y de rendición de cuentas no concierne a las reglas algorítmicas sino a los resultados, a la explicación de la aplicación de estos. Por ello, para la autora no existe riesgo de vulneración de los derechos de propiedad intelectual y los secretos comerciales, estos derechos no deberían utilizarse para evitar la divulgación y explicación de los sistemas de inteligencia artificial. Sin embargo, como tendremos oportunidad de analizar sí existe una tensión entre estos, lo que sucede es que no se materializa de igual forma, dado que depende de los niveles de transparencia que sean necesarios.

La transparencia está relacionada con la capacidad de que un tercero pueda examinar el sistema para garantizar determinados estándares en la toma de decisiones, la verificabilidad o trazabilidad del sistema. El acceso al algoritmo permite establecer la relación entre el sistema y los resultados de su aplicación (Eticas Research and Consulting SL., 2021), lo que sucede es que no en todos los casos será necesario garantizar dicho acceso, dado que ello depende de los niveles de transparencia. La pregunta que hay que responder es cuánta transparencia es necesaria para cumplir con el "ideal" de un sistema fiable y las expectativas de las partes (Hamon, R., Junklewitz, H., Sanchez, I., 2020). Mucho se aborda la necesidad de tener en cuenta tanto el contexto en que tiene lugar, la etapa del ciclo de vida del sistema y los destinatarios, sin embargo, hay que tener en cuenta que demasiada transparencia también podría traer consigo efectos dañinos y no deseados. Como afirman Felzmann et al., no es claro que mayores niveles de transparencia sean siempre lo mejor. Idealmente un nivel óptimo de esta sería aquel en el cual "la transparencia deseada y lograda coincida con la persona o grupo respectivo" (2020, p. 3354), sin embargo, desde un punto de vista práctico lograr un equilibrio entre las diferentes perspectivas, posiciones e intereses no siempre es fácil de lograr. Los actores del sistema varían en dependencia de su ciclo de vida y con ello también los diversos intereses que en relación con este se manifiestan.

Desde la perspectiva de los derechos de propiedad intelectual una mayor transparencia podría provocar la pérdida de la exclusividad que supone el ejercicio de derechos sobre la creación y la consecuente pérdida de la ventaja competitiva (Burell, 2016). No hay que olvidar que los algoritmos como elementos técnicos y matemáticos que se encuentran ubicados en un modelo de negocios determinados se aplican a un grupo de usuarios específicos y buscan ganancias o una forma de lucro. Estos no solo recaban los datos de las personas sus resultados también se aplican sobre estas.

3.1. Niveles de transparencia y derechos de propiedad intelectual

Sin dudas la transparencia está relacionada con la profundidad de la información que se revela y con el momento en que esta revelación se lleva a cabo. En este sentido se habla de diversos niveles o visiones de transparencia debido a que su contenido varía en dependencia de su naturaleza y contexto. Pasquale, citado por Kaminski (2019) utiliza el término de "transparencia calificada", que define un sistema de revelaciones específicas de diferentes grados de profundidad y alcance que varía según al destinatario al que está dirigido. Se parte de que las revelaciones son diferentes tipos, ya sea que vayan dirigidas al público, a lo interno de la empresa, a los reguladores o a terceros. Para Kaminski (2019) algunos de estos sujetos deberán acceder al código fuente y otras no.

La "transparencia calificada" o la referencia de "cierto grado de transparencia" pareciera una forma de equilibrar los requerimientos de transparencia de los sistemas con las limitaciones que supone la opacidad intencional de estos. Sin embargo, hacer referencia a un "nivel de transparencia adecuado" no es un tema fácil. Sobre todo, si se tiene en cuenta que este nivel depende, no solo de la información que es necesaria transmitir y como se protege el sistema, sino también por otros factores como son la complejidad del algoritmo, tipo de opacidad, público objetivo, contexto, expectativa e información que le es necesaria transmitir para poder satisfacer la misma, entre otros.

Una posible solución se podría encontrar en la propuesta comunitaria que parte de la distinción entre: 1) la información mínima necesaria para que las personas ejerzan su derecho a una comprensión efectiva y, 2) la transparencia necesaria para las actividades de supervisión y las encargadas de aplicar la ley.

a. Nivel de transparencia adecuado en relación con los usuarios

Este nivel de transparencia parte desde una visión que se pudiera denominar individual, en cuanto a que la información no solo debe ser divulgada, sino también, recibida, interpretada y entendida por el receptor y conforme a su necesidad. Refiriéndose de la obligación de transparencia desde esta lógica Kaminski (2019) refiere que, si bien no es necesario proporcionar el código fuente a las personas, debe brindarse una descripción de cómo funciona el sistema algorítmico en la toma de decisiones, es decir no es necesario transmitir información sobre el algoritmo per se, sino sobre su utilización y resultados. El cumplimiento del principio de la transparencia no supondría en principio una vulneración de la protección deferida por los derechos de propiedad intelectual. La suficiencia de la información está determinada por lo comprensible, significativa y procesable que sea la información más que por el acceso o no que se tenga al código fuente y demás información asociada a esta.

En este sentido el artículo 13 de la propuesta de reglamento comunitario europeo hace referencia a un nivel de "transparencia suficiente" para que los usuarios interpreten y usen correctamente su información de salida. El cumplimiento de este estándar es complejo, especialmente porque además de la persona o grupo de personas destinatario de la información, hay que tener en cuenta que la interpretación y comprensión de la información como actividad de carácter intelectual depende de varios factores[3]. Cuánta información es necesaria suministrar es complejo de delimitar. A estos efectos el artículo ya citado hace referencia en su apartado 3 al contenido mínimo de información que debe ser puesta en conocimiento del usuario para cumplir con las obligaciones de transparencia de los sistemas de alto riesgo[4].

Delimitaciones como las anteriores son importantes de adoptar no solo para garantizar el contenido mínimo de la transparencia, sino porque al propio tiempo se convierten en un límite de la información que puede ser o no protegida como confidencial o secreto comercial. De esta forma solo aquella información que no se halla dentro de este contenido será considerada como confidencial.

A nivel de usuarios el principio de transparencia está marcado por la necesidad de que la

3 Entre los que se pueden mencionar las habilidades digitales de la persona, su capacidad de comprensión, así como contexto educativo, cultural y económico en el que se desenvuelve.

4 Entre estos se encuentran: a) identidad y los datos de contacto del proveedor y, en su caso, de su representante autorizado; b) las características, capacidades y limitaciones del funcionamiento del sistema de IA de alto riesgo, y en particular: i) su finalidad prevista; ii) el nivel de precisión, solidez y ciberseguridad con respecto al cual se haya probado y validado el sistema de IA de alto riesgo y que puede esperarse de este, así como las circunstancias conocidas o previsibles que podrían afectar al nivel de precisión, solidez y ciberseguridad esperado; iii)cualquier circunstancia conocida o previsible, asociada a la utilización del sistema de IA de alto riesgo conforme a su finalidad prevista o a un uso indebido razonablemente previsible, que pueda dar lugar a riesgos para la salud y la seguridad o los derechos fundamentales; iv) su funcionamiento en relación con las personas o los grupos de personas en relación con los que se pretenda utilizar el sistema; v) cuando proceda, especificaciones relativas a los datos de entrada, o cualquier otra información pertinente en relación con los conjuntos de datos de entrenamiento, validación y prueba usados, teniendo en cuenta la finalidad prevista del sistema de IA; c)los cambios en el sistema de IA y su funcionamiento predeterminados por el proveedor en el momento de efectuar la evaluación de la conformidad inicial, en su caso; d) las medidas de vigilancia humana, incluidas las técnicas establecidas para facilitar la interpretación de la información de salida de los sistemas de IA por parte de los usuarios; e) la vida útil prevista del sistema de IA de alto riesgo, así como las medidas de mantenimiento y cuidado necesarias para garantizar el correcto funcionamiento de dicho sistema, también en lo que respecta a la actualización del *software*.

información que se transmita sea comprensible o legible para todos. Se requiere que la transmisión de información relacionada con los sistemas sea clara y concisa, en particular la relacionada con los riesgos para los derechos fundamentales y la discriminación. Por ejemplo, conforme la propuesta de reglamento europeo es necesario acompañar las instrucciones de uso, en formato digital o de otro tipo adecuado, con información "concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para los usuarios" (art. 13.2).

Debe tenerse presente que, si la información se presenta de forma compleja y oscura, no supone mayor autonomía y control por parte del usuario, así como tampoco cumplimiento de los requerimientos de la transparencia, sino afectar la comprensión de la comunicación de las personas y responsabilizar al usuario aun cuando la información no tenga sentido. Existe la posibilidad de que las empresas inunden a las personas con información inútil e innecesaria incluso es posible crear oscuridad a través del exceso de información. Por ejemplo, utilizar algo similar a los términos y condiciones de los servicios digitales y licencias que hoy se establecen en la realidad ha demostrado ser inoperante (AEPD, 2018 y Hidalgo Pérez, 2020). La complejidad de los términos y condiciones demanda un conocimiento técnico y jurídico superior al del ciudadano medio, y lo han convertido en una mera formalidad, deviniendo al propio tiempo ineficaz, al menos en cuanto a los objetivos perseguidos, en particular, su comprensión.

b. Nivel de transparencia adecuado en relación con las actividades de supervisión y certificación de los sistemas de IA

Para poder realizar las actividades de supervisión y certificación de los sistemas de IA otro nivel de profundidad es requerido en el acceso a la información y en la transparencia del sistema. Las auditorías y supervisiones de los sistemas de IA comienzan a ser vistos como parte de la gobernanza de las organizaciones que diseñan e implementan sistemas de IA. Cuando estas se realizan con un enfoque ético coadyuvan al fortalecimiento de la infraestructura ética de las sociedades de la información maduras (Mökander y Floridi, 2021).

Cuando se realiza la certificación o supervisión del sistema sí se requiere una visión completa del sistema ya sea estas realizadas en el proceso de diseño, implementación o evaluación. En este supuesto Hamon, Junklewitz y Sanchez (2020) señalan tres niveles de transparencia, en la implementación, en las especificaciones y en la interpretabilidad. El primer nivel referido es estándar y permite ver cómo el modelo actúa sobre los datos de entrada para generar una predicción, los principios técnicos del modelo y los parámetros asociados. El segundo hace referencia a toda la información que se relaciona con la implementación, las especificaciones del modelo, datos de entrenamiento, procedimiento, actuaciones, así como a cualquier otro elemento que permita reproducir la implementación. El tercer y último nivel se relaciona con la compresión de los mecanismos subyacentes del modelo, como son los principios lógicos detrás del procesamiento de datos, verificación de que el algoritmo sigue las especificaciones y se alinea con los valores humanos.

En las evaluaciones de impacto, las auditorías propias o de terceros independientes, así como en el control y supervisión por parte de las autoridades regulatorias se requieren niveles de

transparencia más profundos y mayores flujos de información incluidos el código fuente, por ende, el acceso a la información sobre los algoritmos es necesario, lo que incluye no solo el algoritmo en sí, sino también toda la información que se genera alrededor de este incluyendo los documentos interpretativos. Es importante tener en cuenta que el acceso a esta información no depende de la complejidad del algoritmo, sino de la finalidad perseguida con la auditoría y la supervisión. Aun cuando el algoritmo sea tecnológicamente oscuro, puede ser necesario el acceso a este tipo de información para analizar y corregir sus errores, inexactitudes, y sesgos.

Se puede concluir que existen dos aristas de la transparencia, una determinada por el ámbito individual del usuario o la persona que utiliza el sistema, su destinatario final y, otro, que toma como punto de partida la explicabilidad del sistema, las técnicas utilizadas, su complejidad técnica y la estructura interna. Solo en este último supuesto es que es posible referirnos al acceso del código fuente y de información que podría estar protegida como secreto comercial o por otro tipo de derecho de propiedad intelectual. Empero el mayor reto que en este último supuesto existe es garantizar dicho acceso a todos los actores que intervienen en el ciclo de vida del sistema ya se encuentren interesados en su diseño, gestión de riesgos, comercialización, distribución, e incluso, en la determinación de su responsabilidad jurídica.

4. Transparencia y derechos de propiedad intelectual en México

En la relación entre el principio de transparencia y los derechos de propiedad intelectual una de las principales contradicciones que existen residen entre el carácter territorial de la propiedad intelectual y la naturaleza global de la tecnología. Por ende, el estudio de esta relación debe partir de ordenamientos jurídicos particulares con el fin de cerrar la brecha existente entre la transparencia como principio y aspiración ética de la gobernanza de los sistemas de IA y la regulación nacional de los derechos de propiedad intelectual y demás regímenes regulatorios aplicables.

Bajo esta premisa México deviene en un país que reviste particular importancia para el estudio de esta relación en la región latinoamericana, tanto desde un punto de vista de desarrollo de la tecnología como por la regulación jurídica de esta materia. Ello convierte al país en un modelo de estudio para la región en el que es posible determinar el impacto de los regímenes de propiedad intelectual en el desarrollo y avance de la inteligencia artificial de manera general, y en lo particular en la materialización del principio de transparencia.

Según el índice elaborado por *The Economist Intelligence Unit* (EIU) y la empresa ABB en el 2018, entre los 25 países preparados para la ola de la automatización inteligente México ocupa el número 23, luego de Argentina (17), Brasil (19) y Colombia (20),. Asimismo, se encuentra en el puesto 55 de 172 en el índice de preparación del gobierno para la IA del 2020, conforme el estudio realizado por *Oxford Insights* y el Centro Internacional de Desarrollo de la Investigación (IDRC). Dicho ranking mide cómo los gobiernos hacen un uso responsable de la IA, una de las dimensiones que se miden es precisamente la transparencia de conjunto con la responsabilidad, privacidad e inclusividad.

En México existen importantes estudios de organizaciones y miembros de la sociedad civil para la elaboración de una estrategia de IA. El documento *Estrategia de IA en México: Aprovechando la Revolución de la IA* (British Embassy in Mexico, 2018, p. 8, en adelante la Estrategia de IA) recomendó la modernización de la normativa de la propiedad intelectual y de protección de la privacidad, de conjunto con la inversión en infraestructura, que soporte la tecnología, los datos de buena calidad y la conexión a Internet. Asimismo, existe la Agenda Nacional Mexicana de Inteligencia Artificial realizada por la Coalición IA2030Mx, donde se ofrecen un conjunto de recomendaciones en este sentido, incluida la puesta en marcha de políticas públicas que promuevan la obtención de patentes y productos comercialmente viables de los desarrollos en las academias (2020, p. 43).

A nivel normativo la entrada en vigor del Tratado de Libre Comercio entre México, Estados Unidos y Canadá (T-MEC) supuso la adopción de una nueva Ley Federal de Protección a la Propiedad Industrial (LPI), así como importantes modificaciones en la Ley Federal de Derechos de Autor (LFDA). Estas modificaciones sin dudas han supuesto la introducción de nuevas figuras jurídicas que impactan el régimen de protección de los sistemas de IA. Estas legislaciones ofrecen un marco normativo propicio para analizar la relación que se establece entre los derechos de

propiedad intelectual y el cumplimiento del principio de transparencia en los sistemas de IA en el ordenamiento jurídico mexicano.

4.1. ¿Cómo los derechos de propiedad intelectual pueden afectar la transparencia de los sistemas de IA?

Los fundamentos de protección de los derechos de propiedad intelectual y la transparencia de los sistemas de IA difieren. La transparencia no solo se relaciona con las características técnicas del algoritmo sino también con su implementación práctica dentro de las estructuras sociales existentes y sus significados culturales asignados (Felzmann *et al*., 2020). Para alcanzarla es necesario comprender la lógica del sistema y sus limitaciones, en otras palabras, el algoritmo operando con datos en un contexto y circunstancias determinadas. Se sustenta en la protección de intereses personales y de protección de las personas ante el uso de la tecnología.

El reconocimiento de los derechos de propiedad intelectual sobre estos sistemas, y la protección de los secretos tiene un marcado carácter comercial. Como se reconoce en el TMEC, estos permiten una protección efectiva en contra de la competencia desleal conforme a lo previsto en el artículo 10bis de la Convención de París. A partir de su utilización se impide su divulgación, adquisición o uso por otras personas sin el consentimiento de su titular y de manera contraria a los usos comerciales honestos. (art. 20.70 TMEC).

Mantener esta distinción en cuanto a fines de cada uno de los sistemas es importante; sin embargo, ello no significa que se desconozca el papel de la propiedad intelectual no solo como un incentivo para el fomento de esta tecnología, sino también, para garantizar a sus titulares sus derechos contra la apropiación indebida y las falsificaciones. Estos son riesgos que también se corren con la introducción de determinados productos que utilicen sistemas de inteligencia artificial.

Para poder determinar cómo los derechos de propiedad intelectual pueden incidir en la transparencia del sistema es necesario comprender cuál es el mecanismo de protección utilizado y su alcance. En principio el algoritmo como secuencia definida de pasos que se utilizan para resolver un problema u obtener un resultado (art. 19.1 TMEC) es considerado inapropiable, como afirma Plaza Penadés; sin embargo, en la práctica se identifican al menos tres posibilidades de protección a partir de su adecuación a cada una de estas figuras: el secreto comercial, los derechos de autor (*software*) y por medio de patentes. Los tres supuestos constituyen formas de ejercer un monopolio legal.

De hecho, un aspecto interesante del TMEC es la consideración en la nota 80 del capítulo 20 como objeto de apropiación indebida de los sistemas de cómputo. Lo que implica someter a estos al sistema de observancia y protección de los secretos industriales tanto en el ámbito civil como penal, siempre y cuando su adquisición, uso o divulgación de la información sea contraria a los usos comerciales honestos, o la persona o el tercero sabía o tenía motivos para saber que dicha adquisición era contraria a tales usos. En consecuencia, el programa de cómputo podría ser considerado como objeto de apropiación indebida siempre y cuando cumpla con los requerimientos para ser protegido como secreto, es decir, ser un conocimiento técnico e información comercial no divulgada, poseer valor comercial o real precisamente por ser secreto

y ser objeto de medidas razonables según las circunstancias por quien tiene su control legal[5].

Uno de los mayores riesgos que tiene esta forma de protección y su impacto en la transparencia es el hecho de que se generalicen los contratos de confidencialidad o las cláusulas relacionadas con estos, al ser el titular del secreto quien determina este carácter por su valor comercial, sin que exista forma alguna de comprobar si lo reviste. De hecho, puede proliferar información considerada como tal que no cumpla con los requerimientos legales establecidos en la ley, y en particular sobre los que no se hayan adoptado los medios o sistemas suficientes para preservar su confidencialidad y acceso restringido[6].

La otra forma de protección de estos sistemas es mediante patentes. La Estrategia de IA de México afirma que una futura reforma de la ley de propiedad intelectual debería de reconocer derechos de propiedad intelectual para tecnologías emergentes, permitiendo la protección de los programas de IA por patentes y "no solo que los productos físicos puedan patentarse" (2018, p. 46). Más allá de que existe una aseveración falsa, dado que no solo los productos físicos se patentan[7], lo cierto es que tras la adopción de una nueva ley de propiedad industrial esta figura no fue introducida. Dicha ley establece que no se consideran invención: 1) los métodos matemáticos, 2) los esquemas, planes, reglas y métodos para el ejercicio de actividades intelectuales, para juegos o para actividades económico-comerciales o para realizar negocios; 3) los programas de computación (art. 47). Si bien los algoritmos y programas de computación quedan excluidos de la materia patentable *per se*, ello no impide que un producto o procedimiento pueda ser considerado novedoso precisamente por la implementación de un algoritmo. De hecho, a nivel mundial, lo datos arrojan que existe un incremento sustancial en la protección de estos sistemas a partir de la utilización de las patentes como mecanismos de protección[8].

El sistema de patentes presenta algunas limitaciones que podrían incidir en la protección de estos sistemas y en su transparencia, particularmente en aquellos que sean opacos debido a la voluntad de sus titulares como tecnológicamente. Los procedimientos para obtener una patente no solo son procedimientos dilatados, lo que puede ir en contra del desarrollo vertiginoso de la tecnología, sino también la reivindicación de la patente no muestra el sistema o algoritmo propiamente dicho, por lo que no coadyuva a la transparencia del sistema, al menos en los términos a los que nos hemos estados refiriendo.

El patentamiento garantiza, en principio, transparencia respecto a la inventiva humana, no respecto al sistema de IA. Según Früh (2019), las leyes de patentes dejan claro que la invención debe funcionar, por tanto, el inventor no tiene que saber por qué algo funciona, solo es necesario que funcione, el requisito de divulgación no es un problema. La divulgación de la técnica de IA debería ser suficiente. De hecho, se puede conocer y patentar la invención aun cuando no se divulgue el método de IA exacto. Generalmente la reivindicación se elabora a

5 Tras la aprobación de la Nueva Ley de Propiedad Industrial en el ordenamiento jurídico mexicano se regula esta figura incluyendo los requerimientos para su aplicación e interpretación. Estos requerimientos coinciden con la establecida en el artículo 20.73 del TMEC.

6 Si bien esta figura legal permite una protección más reforzada que la del software, y más rápida que la de las patentes, no puede obviarse que ello no impide que terceros puedan utilizar el sistema de IA de forma lícita siempre y cuando se obtenga por sus propios medios. Tampoco garantiza la protección contra la información que se obtiene por ingeniería inversa, o de forma independiente o de forma legítima por personas que no tienen obligación de confidencialidad o simplemente no tienen conocimiento de que esta información era secreta y no se obtuvo vulnerando usos comerciales honestos. En estos casos no es posible alegar incumplimiento del contrato o inducción de incumplimiento.

7 El objeto de la patente es una invención, esta puede ser un producto o un proceso. Como se reconoce en la LPI ello incluye también la patentabilidad de sustancias, compuestos o composición.

8 Según el informe de la OMPI de 2019 sobre esta tecnología desde la década del cincuenta a nivel global se han solicitado más de 340.000 patentes de invenciones relacionadas con IA y se han publicado más de 1,6 millones de publicaciones científicas al respecto, más de la mitad de estas cifras fueron a partir de 2013. Las solicitudes relacionadas con el aprendizaje automático han experimentado un crecimiento medio anual del 28% (WIPO, 2019, p. 7).

partir de frases como “Un sistema implementado por computadora que facilita y realiza …”, “Un medio legible por ordenador que incluye instrucciones ejecutables por ordenador para…”, entre otras. Lo que es lógico que trae implicaciones en el ámbito de la transparencia y auditoría del sistema. De hecho, la divulgación de la invención por medio de la patente no describe aquella explícitamente.

Desde el sistema de patentes la transparencia no la define el carácter de transparente o no del sistema de IA, su explicabilidad o no, sino el equilibrio de divulgación, “¿Qué información debe revelar el solicitante a la oficina de patentes para que el público comprenda lo que obtiene a cambio de la concesión de derechos de monopolio?” (Früh, 2019, p. 15). Esto no significa que se deba comprender la tecnología. Por tanto, es posible que el titular de un sistema de IA se encuentre protegido por patente y este no sea transparente, dado que no se encuentra en la obligación de someterlo a un proceso de transparencia para garantizar dicha protección, al contrario, la exclusividad que otorga este título permite excluir a terceros de uso y acceso de la información que obra en poder del titular porque el sistema de patentes no condiciona a aportar esta información.

Sin embargo, aun cuando para lograr la protección por patente no sea necesario saber cómo el sistema funciona y cuáles son las relaciones que se establecen, sí debe ser reproducible. En principio los sistemas de IA deberían ser reproducibles, pero no siempre lo son. Hay que tener en cuenta que ello puede obedecer tanto a limitaciones tecnológicas del propio sistema como a los datos que son utilizados para realizar el entrenamiento de este. Algunas de estas invenciones no se pueden divulgar por medio del título de la patente sin la divulgación adicional del conjunto de datos utilizados en su entrenamiento, algo que las empresas pueden no estar dispuestas a realizar. También es posible que la evolución del algoritmo a través del tiempo marque claras diferencias entre el título inicialmente concedido y el que se aplica a un producto o servicio determinado.

La imposibilidad de reproducir estos sistemas no solo impacta en su transparencia, desde el punto de vista que se analiza en este trabajo, sino también, en los propios fundamentos del sistema de patentes. Según Frühlas (2019) el déficit de divulgación de los algoritmos que carecen de reproducibilidad , exige, repensar los requisitos de divulgación de la ley de patentes por parte de los sistemas de IA, en particular en cuanto a la reproducción de la solución técnica deseada. En principio, la complejidad del sistema de IA y su uso no debería suponer un incremento de este déficit.

Otra forma de protección del sistema de IA es como software, mediante los derechos de autor. Habitualmente se hace referencia a los sistemas de inteligencia artificial basados en programas informáticos, en los cuales en su núcleo se encuentra un *software*[9]. Como ya se ha reseñado el algoritmo en sí mismo no es objeto de protección, al menos desde la perspectiva del ordenamiento jurídico mexicano[10], sin embargo, si dicho algoritmo es llevado a un lenguaje de programación sí sería posible su protección dentro del marco regulatorio de la LFDA, específicamente al que se reconoce a los programas de cómputo como a las bases de datos, conforme a lo previsto en los apartados XI y XIV del artículo 13 de la LFDA.

9 Algunas concepciones de la IA parte de este concepto para explicarla, es el caso, por ejemplo, del artículo 3 apartado 1 de la propuesta de Reglamento de la UE que a partir de este concepto precisa que, entre sus objetivos se encuentran contenidos, predicciones, recomendaciones o decisiones que influyen en el entorno, los cuales son definidos por los seres humanos.

10 No son objeto de protección las ideas en sí mismas, las fórmulas, soluciones, conceptos, métodos, sistemas, principios, descubrimientos, procesos e invenciones de cualquier tipo; así como tampoco los esquemas, planes o reglas para realizar actos mentales, juegos o negocios, entre otros (art. 14 apartados 1 y III LFDA).

Lo anterior significa que el sistema de IA puede ser protegido si cumple los requisitos establecidos por la norma y le concede determinadas facultades exclusivas que impiden su utilización por parte de terceros no autorizados por su titular. A partir del primer significado el sistema de IA deberá ser considerado como "la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica" (art. 101 LFDA). Su protección se realizará en los mismos términos que las obras literarias e incluye tanto a los programas operativos como a los aplicativos, ya sea en forma de código fuente o de código objeto (art. 102 LFDA).

Proteger al sistema de IA como software, bajo el régimen jurídico de los derechos de autor, implica también reconocer un poder de disposición de su titular sobre el mismo que excluye a terceros, y que se materializa en un conjunto de facultades morales y patrimoniales. Entre estas últimas el ordenamiento jurídico mexicano reconoce la de autorizar o prohibir: a) la reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma; b) la traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante; c) cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler; d) la adaptación, arreglo o modificación del programa, así como la reproducción del resultante, la decompilación, los procesos para revertir la ingeniería de un programa de computación y desensamblaje, e) así como la comunicación pública del programa, incluida la puesta a disposición pública del mismo (art. 106 LFDA).

Estas facultades garantizan el control del titular del software, su carácter privativo, así como el acceso que este podría conceder o no a terceros del código fuente. Este acceso en múltiples casos se encuentra en dependencia de si solo ha sido autorizada la utilización de una o alguna de estas facultades o la cesión de estas facultades. Es importante apuntar que, si bien estas facultades posibilitan privar del acceso al código fuente como parte del poder de disposición de los titulares del derecho, lo cierto es que el reconocimiento de estas facultades no es contradictorio a los denominados softwares abiertos, modelo que se preconiza a favor de un régimen transparente de los sistemas de IA, alternativo al modelo privativo que no concede dicho acceso.

Un aspecto que merece ser resaltado es que las formas de protección anteriormente referidas no son excluyentes, de hecho, pueden existir dos o las tres sobre el mismo sistema de IA. De esta forma se intenta, en lo posible, poder conjugar los beneficios y desventajas de cada forma de protección con la otra, siempre y cuando el sistema cumpla con los requerimientos que cada forma en lo particular demanda. Sin dudas, por un lado, si bien garantiza la efectividad de la protección del sistema y la menor probabilidad de apropiación por parte de terceros, por el otro provoca que los sesgos que representan cada una de estas formas en relación con la transparencia también incidan en la gestión de la transparencia del sistema de IA.

Generalmente los derechos de propiedad intelectual impiden la disposición pública de la implementación y las especificaciones. Sin embargo, ello no quiere decir que no se prevean posibilidades para hacer compatibles las demandas de protección de los derechos de propiedad intelectual y los requerimientos de transparencia. Tanto en el supuesto de protección de la patente como del secreto comercial existen excepciones que pueden ser aplicables, aunque

es más difícil en el caso del *software* donde las normas no prevén posibilidades expresas de compatibilizar mecanismos de supervisión con el acceso al código fuente.

En el ordenamiento mexicano la norma de propiedad industrial, por ejemplo, no considera que la información relacionada con el secreto entra a dominio público o es divulgada cuando es proporcionada a la autoridad a los efectos de obtener licencias, permisos, autorizaciones, registros o cualesquiera otros actos de autoridad (art. 163.1 LPI), como pudiera ser la existencia de un régimen de certificación[11]. Una disposición similar se encuentra en el artículo 168 de la Ley de Propiedad Industrial de México, la cual prevé que, cuando sea obligatorio suministrar información considerada secreto para determinar la seguridad y eficacia de productos farmoquímicos o agroquímicos que utilicen nuevos componentes, esta información quedaría protegida en los términos de la legislación aplicable o, en su caso, de los tratados internacionales (art. 168 LPI). Si bien dicha disposición no resulta aplicable expresamente a los sistemas de IA, sí podría ser modificada o aplicada de forma analógica a este supuesto.

En materia de patentes, por ejemplo, el registro es público, con excepción de aquellas solicitudes que tengan carácter confidencial (art. 22 LPI). Así, los expedientes no podrían ser abiertos a consultas y promociones si contienen información de este tipo (art. 23 LPI), y podrían ser consultados por el solicitante, su representante legal o por personas autorizadas por este. La observancia de la preservación de confidencialidad implica la responsabilidad administrativa de los servidores públicos en relación con guardar absoluta reserva sobre el contenido de los expedientes. Obligación que, conforme lo previsto en la norma, se extiende al personal de los organismos públicos o privados que podrían conocerlo en el ejercicio de sus funciones de apoyo al Instituto Mexicano de Propiedad Industrial (IMPI). Las únicas excepciones son las informaciones de carácter oficial o requeridas por la autoridad judicial (art. 24 LPI).

También existe la posibilidad de solicitar, de parte o de oficio, la adopción de las medidas necesarias para impedir la divulgación no autorizada a terceros ajenos a la controversia y garantizar su confidencialidad en cualquier procedimiento judicial o administrativo relacionado con esta materia (art. 169 LPI),dado que existe de forma expresa la prohibición de que ningún interesado pueda divulgar o usar el secreto industrial.

En resumen, la comprobación de este tipo de productos de forma confidencial podría encuadrarse dentro de lo previsto y de lo posible por el mismo régimen jurídico de los derechos de propiedad intelectual como una vía para proteger a los titulares de los sistemas de IA. Sin embargo, es importante tener en cuenta que este marco solo opera para los supuestos en los que existen obligaciones de acceso de autoridades públicas, en otras palabras, mecanismos de certificación. El sistema de excepciones de acceso a la información solo se contempla para un régimen jurídico en el cual se prevén obligaciones de certificación, que en el caso de los sistemas de IA deberían estar relacionadas con la transparencia de estos.

11 Existe a nivel internacional un amplio debate en relación con la existencia o no de mecanismos de certificación para los sistemas de IA, y bajo cuales supuestos se deberían aplicar. En principio, se habla de establecer mecanismos de certificación en dependencia del impacto en la vida de las personas y los riesgos. Que evalúen el impacto de estos sistemas, realicen auditorías de seguimiento y cumplimiento ético y normativo. Empero existen dudas sobre cómo operarían estos mecanismos de certificación, los cuales deben garantizar confianza y seguridad jurídica, y al mismo tiempo, no devenir en un obstáculo a la innovación ni al desarrollo de las pequeñas y medianas empresas. Las propuestas discurren entre la evaluación de conformidad que propone el Reglamento Europeo, la certificación según los diferentes niveles de auditoría del Comité de Ética de Datos alemán, el sello de ética de datos danés o el sistema voluntario de certificación maltés. En México se debate el establecimiento de un consejo mexicano de ética de IA integrado por expertos, líderes empresariales y la Oficina de IA con el fin de a) establecer los lineamientos y los límites que reflejan los valores mexicanos y b) otorgar un sello de calidad a las empresas de IA que respetan las normas (British Embassy, 2018).

4.2. Transparencia y propiedad intelectual en la transmisión y adaptación de los sistemas de IA

Desde el ámbito tecnológico el sistema debe ser transparente desde la fase de diseño y durante todo su ciclo de vida. El ciclo de vida del sistema de IA consta de varias fases[12], que pueden tener lugar de manera iterativa y no necesariamente secuencial y en la cual intervienen diversos grupos de interés, como son los titulares de derechos de propiedad intelectual, proveedores de servicios, importadores, distribuidores y usuarios. Ello significa que, si se pretende que en cualquiera de estas fases el sistema sea transparente y susceptible de ser auditado, entonces quien esté a su cargo debe poseer la información técnica necesaria para garantizarlo.

En otras palabras, si dicha información técnica está asociada a un *software*, patente y/o secreto, debe ser transmitida junto con el sistema y adoptar las medidas necesarias para su protección y garantizar su actualización conforme a su fase y ciclo de vida. En México la LPI contempla la posibilidad de que la persona que ejerza el control legal del secreto pueda transmitirlo o autorizar su uso a tercero, bajo la obligación de no divulgarlo (art. 165). Asimismo, se considera que en los convenios donde se transmiten conocimientos técnicos, asistencia técnica, provisión de ingeniería básica o de detalle, se pueden establecer cláusulas de confidencialidad para proteger los secretos industriales, siempre y cuando se precisen los aspectos que se consideran como confidenciales.

Por ende, el cumplimiento del principio de transparencia dependerá del rol de cada uno de los actores, así como del nivel de información que se le haya transmitido. El proveedor, como persona física o jurídica que desarrolla un sistema de IA o para el que se desarrolla el sistema, desempeña un papel fundamental en el cumplimiento de esta obligación, y particularmente en aportar la documentación necesaria, implementar el código, realizar su trazabilidad, casos de uso, especificaciones adecuadas y demás.

Debe tenerse en cuenta la diferencia entre el titular de los derechos de propiedad intelectual sobre el sistema y de quien posea el control legal del secreto industrial o comercial. En determinados momentos del ciclo de vida esta figura puede coincidir, pero a los efectos de materializar la transparencia en dependencia del tipo de protección ambas figuras son importantes dada la capacidad que pueden tener o no para autorizar el acceso de dicha información. Por ejemplo, el proveedor puede haber desarrollado el sistema de IA o ser para quien se desarrolla el sistema. En este último supuesto la relación puede tener su causa en un contrato laboral o de prestación de servicios, aunque también es posible que la persona sea titular del sistema de IA por una cesión de derechos de propiedad intelectual (software o patente). Sea cual fuere la causa por la que el proveedor devenga titular de los derechos no significa que sea la persona que lo introduzca en el mercado o ponga bajo su nombre o marca comercial el sistema.

A tenor de lo anterior cabe la posibilidad de que el proveedor no fuere per se el titular de los derechos sobre el sistema, pero sí el titular de la marca o signo distintivo que lo identifica en el mercado. A efectos de transparencia lo trascendente no es quién tiene la titularidad sobre el sistema sino quién es la persona responsable de cumplir la obligación de transparencia.

12 Según las recomendaciones de la OCDE estas fases son: i) *diseño, datos y modelos*, que abarca la planificación y el diseño del sistema, la recopilación y el procesamiento de datos y la construcción de modelos; ii) la etapa destinada a su *verificación y validación*; iii) el despliegue; y por último iv) *la operación y vigilancia*.

Empero, no basta con ser identificado como tal, sino que, a su vez, debe tener a su disposición la información necesaria para poder realizar la correspondiente valuación o inspección y las autorizaciones necesarias para ello.

En este último supuesto es de medular importancia determinar quién tiene el control legal de la información confidencial, es decir, la persona que puede transmitir o autorizar el uso de esta información (art. 65 de la LPI mexicana). Bajo dicho concepto queda comprendido tanto al titular de los derechos y de la información como quien la posee porque así se le ha transmitido o autorizado su uso. Sin embargo, los acuerdos de cesión o autorización de uso deben ser muy claros en relación con los límites de este uso y la posibilidad de cumplir o no con las obligaciones de transparencia. Por otro lado, deben diferenciarse las personas que tienen acceso a dicha información debido al cargo que desempeñan de las que adquieren la obligación de preservarla pero no pueden autorizar su uso a terceros, su transmisión ni entrega a los fines de cumplimiento de la obligación de transparencia.

De manera general, todos los miembros de la cadena de valor de un sistema podrían verse comprometidos en mayor o menor grado con el cumplimiento de las obligaciones de transparencia, con el deber de aportar la consabida información. Las garantías de que esto tenga lugar son los contratos que se suscriben entre las partes, así como la adopción de las medidas de protección necesarias para garantizar la protección de los secretos empresariales. Todos los agentes de la cadena de valor son sujetos obligados para proteger esta información dado que si existe fuga inmediatamente esta pierde su carácter secreto.

Por último, debe abordarse el tema relacionado con las modificaciones o mejoras del sistema. Debe diferenciarse el hecho de que el sistema puede continuar aprendiendo y perfeccionándose después de su introducción en el mercado o puesta en servicio, o ser sometido intencionalmente a una modificación sustancial. En este último supuesto podría existir una afectación en la implementación, documentación y mantenimiento del sistema, en la gestión de riesgos asociada a este o en la modificación de la finalidad prevista para la que este se ha evaluado. En este supuesto la modificación solo podría llevarse a cabo si se realiza con la autorización de los titulares de los derechos de propiedad intelectual del sistema original, teniendo que ser sometido a una nueva evaluación.

Al ser un *software*, para poder realizar cualquier tipo de mejora o cambio sustancial debe contarse con la autorización del titular o los titulares de los derechos de autor. Como ya se ha referido anteriormente entre las facultades de los titulares de los programas de computación se encuentra la de autorizar o prohibir la adaptación, arreglo o modificación del programa, así como la reproducción del resultante, la decompilación, los procesos para revertir la ingeniería de un programa de computación y desensamblaje así como la comunicación pública del programa, incluida la puesta a disposición pública del mismo (art. 106 LFDA). A estos efectos si el contrato no autoriza estas facultades o no tiene contemplada su cesión estas acciones infringirían el derecho de los titulares del programa.

En la propuesta de reglamento europeo existe una delimitación interesante, que marca el sentido de hasta dónde se puede entender que es necesaria o no la autorización del titular del sistema. A estos efectos no se considera que existe una modificación sustancial cuando los cambios en el algoritmo y en su funcionamiento han sido predeterminados por el proveedor y fueron tenidos en cuenta en el momento de evaluación de la conformidad (considerando 66). Empero, la modificación del sistema deviene difícil de acreditar en el supuesto de que exista

una protección como secreto industrial o comercial. Si no existe un sistema de certificación no podría quedar acreditado el nivel de estas modificaciones, cuán sustanciales son o, al menos, el sentido de su realización. En algunos supuestos estas pueden ser mínimas y hasta lógicas, tomando como punto de partida modelos algorítmicos iguales o similares. La única forma de acreditar esta distinción sería cuando existiera un cambio en sus finalidades. En este caso, la protección por vía de secreto podría quedar resquebrajada al no poder impedir que terceros puedan utilizar el mismo de forma lícita siempre y cuando lo obtenga por sus propios medios.

5. Conclusiones

A partir de lo anteriormente expuesto podríamos concluir que los derechos de propiedad intelectual pueden constituir una barrera o un mecanismo de impulso para el desarrollo de los sistemas de IA. Desde la configuración de una política pública de IA es necesario concebir un modelo de protección de los derechos de propiedad intelectual sobre estos sistemas que sea coherente con un régimen transparente y que permita su auditoría. Los derechos de propiedad intelectual no deberían devenir en una barrera para llevar a cabo la auditoría, trazabilidad y la explicabilidad de los sistemas de IA.

El nivel de transparencia para lograr una IA fiable es distinto y depende no solo de la información que se transmite, sino también, del contexto y del destinatario de esta información. En este sentido se diferencian los requerimientos de transparencia destinados a cumplir las expectativas de los usuarios y consumidores de estos sistemas y aquellos que se realizan con fines de auditoría y/o certificación. Cuando los requerimientos de transparencia están dirigidos a cumplir las expectativas de los usuarios y consumidores no es necesario transmitir información relacionada con el código fuente o el algoritmo del sistema, así como tampoco información asociada a estos. Sin embargo, la situación es diferente cuando la transparencia tiene como finalidad sustentar los requerimientos para la certificación y/o auditoría de los sistemas. En este caso sí es necesario acceder al código fuente y la información asociada a este.

La cadena de valor de los sistemas de IA es compleja e intervienen múltiples actores. La obligación de transparencia permanece en cabeza de cada uno de estos, por ende, para que cada uno de los actores pueda cumplir con dicha obligación durante todo el ciclo de vida de la IA deben existir obligaciones claras en los contratos de transmisión y uso de los sistemas que garanticen la puesta a disposición de la información necesaria para cumplir con dicha obligación, así como garantizar el respeto de los derechos de propiedad intelectual.

Los sistemas de IA pueden ser protegidos por patentes, por derechos de autor como *softwares* o secretos industriales. Estas formas de protección no son excluyentes y dependen de las regulaciones nacionales. Dada las particularidades de cada una de estas formas de protección impactan de forma diferente en la opacidad intencional de los sistemas de IA y en el cumplimiento de los requerimientos de transparencia. Por ello, es necesario, encontrar un equilibrio entre transparencia y derechos de propiedad según cada una de estas formas de protección.

En el ordenamiento jurídico mexicano, al igual que acontece en otros países de la región de América Latina, los principales mecanismos de protección de estos sistemas son por los derechos de autor como software o como secreto empresarial. El régimen jurídico de estas figuras contempla soluciones viables que impiden convertir los derechos de propiedad intelectual en una barrera a la obligación de transparencia de los sistemas de IA.

Existen excepciones que permiten proteger los derechos de propiedad intelectual y la información empresarial confidencial o los secretos comerciales de una persona física o

jurídica, incluido el código fuente, siempre y cuando sean utilizados en el cumplimiento de la obligación de confidencialidad de las autoridades nacionales competentes en relación con la información y los datos obtenidos en el ejercicio de sus funciones y actividades para certificar dichos sistemas. La inexistencia de mecanismos de certificación, en principio, no permite cumplimentar los requerimientos de estas excepciones.

6. Referencias

AEPD (2018). El examen de aplicaciones (III): los términos y condiciones. https://www.aepd.es/es/prensa-y-comunicacion/blog/el-examen-de-aplicaciones-iii-los-terminos-y-condiciones

Bengio, Yoshua (2018). Resistirse al monopolio de la investigación. Inteligencia Artificial, promesas y amenazas. El correo de la UNESCO. Julio-septiembre, (3), 18-20.

Bielan, Adam (2020). Opinión de la Comisión de Mercado Interior y Protección del consumidor para la Comisión de Asuntos Jurídicos sobre los derechos de propiedad intelectual para el desarrollo de las tecnologías relativas a la inteligencia artificial. https://www.europarl.europa.eu/doceo/document/A-9-2020-0176_ES.html

British Embassy in Mexico (2018). Estrategia de IA en México: Aprovechando la Revolución de la IA.

Burrell, Jennav (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. Big Data & Society, 3(1)-2053951715622512. https://journals.sagepub.com/doi/pdf/10.1177/2053951715622512

Castets-Renard, Ce´line (2020). The Intersection Between AI and IP: Conflict or Complementarity? Max Planck Institute for Innovation and Competition (IIC), 51, 141–143. https://doi.org/10.1007/s40319-020-00908-z

Cminds (2020). Agenda Nacional Mexicana de Inteligencia Artificial. México: Coalición IA2030Mx.

Comisión Europea (2019). Directrices Éticas para una IA Fiable. https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence.

Comisión Europea, (2020). Libro Blanco sobre la inteligencia artificial, un enfoque europeo orientado a la excelencia y la confianza. https://op.europa.eu/es/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1

Eticas Research and Consulting SL (2021), Guía de Auditoría Algorítmica. Madrid: Agencia Española de Protección de Datos.

Felzmann, Heike, Fosch Villaronga, Eduard, Lutz Christoph y Tamò Larrieux, Aurelia (2020). Towards Transparency by Design for Artificial Intelligence. Science and Engineering Ethics, 26(6), 3333–3361. https://link.springer.com/content/pdf/10.1007/s11948-020-00276-4.pdf

Früh, Alfred (2021). Transparency in the Patent System – Artificial Intelligence and the Disclosure Requirement. En Pacud, Žaneta y Sikorski, Rafał (Ed.). Patents as an Incentive for Innovation. Kluwer Law International.

Hamon, R., Junklewitz, H., Sanchez, I. (2020). Robustness and Explainability of Artificial Intelligence - From technical to policy solutions. Publications Office of the European Union. DOI:10.2760/57493.

Herrera Triguero, Francisco (2019). Inteligencia computacional: sistemas inteligentes inspirados en la naturaleza. http://www.raing.es/sites/default/files/PUBLICACI%C3%93N%20FRANCISCO%20HERRERA.pdf

Hidalgo Pérez, Montse (2020). Leer las condiciones de tus 'apps' te puede llevar más tiempo que el Quijote. El País. https://elpais.com/tecnologia/2020-06-23/leer-las-condiciones-de-tus-apps-te-puede-llevar-mas-tiempo-que-el-quijote.html

Hilty Reto, M., Hoffmann, Jörg y Scheuerer, Stefan (2020). Intellectual Property Justification for Artificial Intelligence. Max Planck Institute for Innovation and Competition Research Paper (02). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3539406

Kaminski, Margot E. (2019). The right to explanation, explained. Berkeley Technology Law Journal (34). https://scholar.law.colorado.edu/articles/1227

Mökander, Jakob y Floridi, Luciano (2021). Ethics Based Auditing to Develop Trustworthy AI. Minds and Machines. https://doi.org/10.1007/s11023-021-09557-8

Ley Federal del Derecho de Autor. Nueva Ley publicada en el Diario Oficial de la Federación el 24 de diciembre de 1996. Texto vigente última reforma publicada DOF 01-07-2020.

Ley Federal de Transparencia y Acceso a la Información Pública. Nueva Ley publicada en el Diario Oficial de la Federación el 9 de mayo de 2016. Texto vigente última reforma publicada DOF 20-05-2021.

Ley Federal de Protección a la Propiedad Industrial. Texto vigente. Nueva Ley publicada en el Diario Oficial de la Federación el 1 de julio de 2020.

Tratado de Libre Comercio entre México, Estados Unidos y Canadá, entrada en vigor el 1 de julio de 2020.

The Economist Intelligence Unit (EIU) y la empresa ABB (2018). Índice de Preparación para la automatización.

OECD (2019). Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449. https://legalinstruments.oecd.org› api › print

Oliver Ramírez, Nuria María (2018). Inteligencia artificial: Ficción, realidad y... Sueños. http://www.raing.es/sites/default/files/TOMA%20DE%20POSESI%C3%93N%20NURIA%20OLIVER%2011.12.18.pdf

Oxford Insights (2021). Government AI Readiness Index 2020. Canada's International Development Research Centre (IDRC). https://www.oxfordinsights.com/government-ai-readiness-index-2020

Parlamento Europeo y Consejo (2021). 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, 2021/0106(COD). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2021:206:FIN

Paz Hermosilla, María; Garrido, Romina y Ioewe, Daniel, (2020). Transparencia y responsabilidad algorítmica para la inteligencia artificial.

Plaza, Javier (2019). Aspectos legales del Big Data y la Inteligencia Artificial. Big Data e Inteligencia Artificial: Una visión económica y legal de estas herramientas disruptivas.

Qiang, Yang (2018). La cuarta revolución. Inteligencia artificial. Promesas y amenazas.El Correo de la Unesco.

Unesco (2020). Primera versión del proyecto de recomendación sobre la ética de la inteligencia artificial SHS/BIO/AHEG-AI/2020/4 REV.2. https://unesdoc.unesco.org/ark:/48223/pf0000373434_spa

Verheyen, Sabine (2020). Opinión de la Comisión de Cultura y Educación para la Comisión de Asuntos Jurídicos sobre los derechos de propiedad intelectual en el desarrollo de tecnologías de inteligencia artificial, 3/09/2020 (2020/2015(INI). https://www.europarl.europa.eu/doceo/document/A-9-2020-0176_ES.html

WIPO (2019). WIPO Technology Trends 2019: Artificial Intelligence. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf

Descargo de responsabilidad. *Las opiniones expresadas en la publicación incumben únicamente a los/as autores/as. No tienen intención de reflejar las opiniones o perspectivas del CETyS, CLD ni de ninguna otra organización involucrada en el proyecto.*