

Comité Asesor sobre Observancia

Decimosexta sesión
Ginebra, 31 de enero a 2 de febrero de 2024

INTELIGENCIA ARTIFICIAL Y OBSERVANCIA DE LA PROPIEDAD INTELECTUAL

Documentos preparados por el Sr. Dennis Collopy, Countercheck, Universal Music Group y Mercado Libre

1. En la decimoquinta sesión del Comité Asesor sobre Observancia (ACE), celebrada del 31 de agosto al 2 de septiembre de 2022, el Comité acordó examinar, en su decimosexta sesión, entre otros temas, el "intercambio de información sobre experiencias nacionales en relación con acuerdos institucionales relativos a políticas y regímenes de observancia de la PI, en particular los mecanismos para resolver controversias de PI de forma equilibrada, holística y eficaz". En este contexto, en el presente documento se exponen las aportaciones de tres entidades del sector privado (Countercheck, Universal Music Group (UMG) y Mercado Libre) sobre sus experiencias con la inteligencia artificial (IA) y la observancia de la propiedad intelectual (PI).
2. En el documento del Sr. Dennis Collopy se resume el estudio de investigación *Artificial Intelligence and Intellectual Property Rights Enforcement* (Inteligencia artificial y observancia de la propiedad intelectual). Además se aclaran definiciones clave, se explica la metodología empleada y se ofrece una visión de conjunto de las conclusiones del estudio. Más concretamente, se señalan oportunidades en el uso de la IA para hacer valer los derechos de PI, como la mejora de la detección de contenidos que vulneren el derecho de autor, el reconocimiento de diseños y la detección más rápida del uso indebido de marcas. Por otro lado, se indican ciertas dificultades importantes, como los costos, la falta de transparencia, los problemas de intercambio de datos y algunas consideraciones éticas.
3. En el documento de Countercheck se examina el uso de la IA en la inspección de paquetes. En el documento se destaca la tecnología de Countercheck, así como los retos jurídicos que plantea la aplicación de la IA, y se hace hincapié en la necesidad de colaboración entre los sectores público y privado para combatir los delitos que atentan contra los derechos de PI y mejorar el marco jurídico.

4. En el documento de UMG se ponen de relieve sus opiniones sobre la IA, centrándose en el uso responsable de la IA en medio de una profunda preocupación por las infracciones de los derechos de PI. Se profundiza en actividades alarmantes, como el uso de IA para imitar a artistas y crear pistas fraudulentas, y en los medios con los que se entrenan los sistemas de IA, sobre todo el acceso no autorizado a obras musicales protegidas por derechos de autor. En el documento también se subraya la manera en que pueden utilizar la IA los titulares de derechos del sector musical, tanto para apoyar el proceso creativo como en calidad de herramienta para detectar infracciones.

5. En el documento de Mercado Libre se analiza el uso de la IA para detectar y eliminar automáticamente los anuncios de productos falsificados en su plataforma de comercio electrónico. Tras exponer someramente los marcos normativos de toda América Latina, en el documento se describen los esfuerzos proactivos que realiza Mercado Libre con la ayuda de la IA para detectar productos falsificados, así como las dificultades que entraña su utilización.

6. Los documentos figuran en el orden siguiente:

Inteligencia artificial y observancia de la propiedad intelectual: Panorama general sobre dificultades y oportunidades	3
Un enfoque innovador en la lucha contra la falsificación: Inspección de paquetes mediante inteligencia artificial para la observancia de la propiedad intelectual	11
El uso que hacen de la inteligencia artificial los piratas y los titulares de derechos en la industria musical.....	17
Uso de inteligencia artificial para la detección y remoción automática de ofertas de productos falsificados en los sitios de mercado libre	25

[Siguen los documentos]

INTELIGENCIA ARTIFICIAL Y OBSERVANCIA DE LA PROPIEDAD INTELECTUAL: PANORAMA GENERAL DE DIFICULTADES Y OPORTUNIDADES

*Documento preparado por el Sr. Dennis Collopy, investigador superior de la School of Creative Arts, University of Hertfordshire, Hatfield (Reino Unido)**

RESUMEN

En este documento se resumen los resultados del estudio de investigación *Artificial Intelligence and Intellectual Property Rights Enforcement* (Inteligencia Artificial y Observancia de la Propiedad Intelectual). También se explican definiciones clave y la metodología utilizada, antes de presentar información sobre los resultados del estudio. Más concretamente se indican oportunidades en el uso de la inteligencia artificial (IA) para hacer valer los derechos de propiedad intelectual (PI), como la mejora de la detección de contenidos que infringen el derecho de autor, el reconocimiento de diseños y la detección más rápida del uso indebido de marcas. Por otro lado, los costos, la falta de transparencia, los problemas de intercambio de datos y algunas consideraciones éticas son algunos de los retos que plantea la IA. En el documento se concluye que, aunque la IA ofrezca soluciones prometedoras, es fundamental realizar cuidadosamente pruebas piloto en ese ámbito y prestar atención a los límites éticos, morales y jurídicos antes de incrementar su adopción.

I. INTRODUCCIÓN

A. OBJETIVOS Y METAS DEL ESTUDIO.

1. Este documento se basa en el estudio de investigación *Artificial Intelligence and Intellectual Property Rights Enforcement* (Inteligencia Artificial y Observancia de la Propiedad Intelectual), encargado por la Oficina de Propiedad Intelectual del Reino Unido en 2021 para evaluar si la inteligencia artificial (IA) puede utilizarse para rastrear y localizar mercancías que vulneren derechos de propiedad intelectual (PI), y de qué manera, así como para evaluar el uso potencial de aquella tecnología por quienes vulneran estos derechos.
2. El objetivo del proyecto era examinar y cotejar bibliografía disponible y recabar opiniones de quienes tenían conocimientos especializados y experiencia en la esfera de la observancia de los derechos de PI vigentes, en cuanto a:
 - el modo en que los titulares de derechos utilizan actualmente la IA para proteger y hacer valer los derechos de PI y
 - la evaluación de amenazas de quienes infringen los derechos de PI.
3. En la investigación se estudiaron cinco derechos de PI: patentes, marcas, diseños, derechos de autor y, sobre todo, secretos comerciales.

* Las opiniones expresadas en el presente documento corresponden al autor y no reflejan necesariamente el punto de vista de la Secretaría de la OMPI ni el de sus Estados miembros.

B. METODOLOGÍA

4. El proyecto consistió en un proceso en dos fases:

- Un examen crítico de la bibliografía sobre la IA y la observancia de la PI relevante para los cinco derechos de PI en cuestión, elaborada por el sector gubernamental, el mundo académico y la industria para establecer temas centrales y resultados.
- Esto permitió elaborar un cuestionario que se utilizaría como base para una amplia gama de entrevistas con partes interesadas pertinentes del sector, organismos encargados de hacer cumplir la ley, el mundo académico y profesionales del Derecho y el poder judicial, con el fin de obtener una visión nueva y actualizada de los problemas del momento.

C. DEFINICIONES

5. Ante todo era importante definir cuidadosamente la terminología utilizada debido a la proliferación de definiciones de IA.

6. La definición más clara y sucinta de IA, “la inteligencia humana que muestran las máquinas”, fue la ofrecida por el profesor Kevin Curran, coautor del estudio y experto en IA.

7. La investigación se centró en el subconjunto de IA, conocido como IA estrecha, en forma de aprendizaje automático. El aprendizaje automático permite la creación de sistemas “que pueden aprender a partir de la experiencia para encontrar patrones dentro un conjunto de datos” y, así, ser capaces de inferir o predecir un resultado, incluso si los procesos plantean ciertos retos, así como oportunidades. El objetivo principal del estudio original fue determinar cuáles eran esos retos y oportunidades. Otras expresiones relevantes mencionadas en el documento son:

- En la actualidad la IA estrecha es la única forma de IA que existe y está entrenada para realizar una única tarea; a diferencia de la IA general, no puede operar fuera de esa tarea definida.¹ Según IBM, “cualquier otra forma de IA es teórica” e incluso ChatGPT, de OpenAI, es una forma de IA estrecha puesto que “se limita únicamente a las tareas relacionadas con el chat basado en texto”.²
- El PNL (procesamiento del lenguaje natural) consiste en la capacidad de las computadoras de entender textos y palabras habladas de forma similar a los seres humanos.
- La IA opaca (también conocida como IA de caja negra) no puede inspeccionarse del mismo modo que los sistemas con una pista de auditoría completa (*audit trail*).
- Las redes neuronales, un subconjunto del aprendizaje automático, son clave en los algoritmos de aprendizaje profundo, ya que utilizan datos de entrenamiento (*training data*) para aprender y mejorar la precisión, con el tiempo, a fin de lograr una clasificación de datos a alta velocidad.

¹ IBM Data and AI Team (19 de octubre de 2023), “Understanding the Different Types of Artificial Intelligence”, disponible en: <https://www.ibm.com/blog/understanding-the-different-types-of-artificial-intelligence/>

² Ibid.

II. RESULTADOS DE LA INVESTIGACIÓN

A. PRINCIPALES OPORTUNIDADES

a) Derecho de autor

8. Existe la oportunidad de aumentar el uso de las herramientas de IA en la observancia del derecho de autor, especialmente a la vista de ciertos sistemas automatizados antipiratería que han mostrado ser eficaces.

9. Como herramienta de filtrado, la IA ayuda a detectar contenidos ilícitos y a reducir la carga de trabajo humano, pero necesita datos precisos y adecuados de entrenamiento. Content ID de YouTube es un ejemplo de herramienta de IA visiblemente eficaz, y es que los investigadores consideran que “funciona relativamente bien para eliminar de YouTube contenidos que parecen ilícitos”,³ aunque su porcentaje de éxito no es del 100%.

b) Diseños

10. En cuanto a los diseños, mejorar las capacidades de reconocimiento de imágenes podría ayudar a detectar posibles infracciones. Anti Copying in Design (ACID) gestiona una base de datos de más de 300 000 diseños (incluidos diseños no registrados) que podrían utilizarse para entrenar a la IA a reconocer aquellos ilícitos.

c) Marcas

11. Si se entrenan con conjuntos de datos muy grandes, las herramientas de IA podrían servir de ayuda a los analistas de la observancia de marcas y, en consecuencia, liberar recursos humanos. Hay margen para seguir desarrollando soluciones de observancia en estrecha colaboración con las plataformas en línea orientadas al consumidor que utilizan herramientas de IA para supervisar contenidos.

12. Por ejemplo, una nueva gama de herramientas proporcionada por la Oficina de Propiedad Intelectual de la Unión Europea (EUIPO) ofrece soluciones de seguimiento y localización, sistemas de análisis de riesgos y utilización de IA y aprendizaje automático para detectar registros de nombres de dominio sospechosos y potencialmente abusivos.

13. La IA podría desempeñar un papel en la observancia de derechos que podrían vulnerar distintos tipos de ciberdelincuencia y en la detección de falsificaciones, como ayuda a las personas que trabajan en esas esferas.

d) Secretos comerciales

14. Los secretos comerciales, especialmente en el caso de las invenciones relacionadas con la IA, necesitan una mayor protección contra la apropiación indebida. Medidas de seguridad, como las técnicas basadas en IA, incluidas las técnicas de cifrado neuronal, pueden ofrecer una mayor protección.

³ Joanne E. Gray y Nicolas P. Suzor (2020), *Playing with machines: Using machine learning to understand automated copyright enforcement at scale*, Big Data & Society, disponible en: <https://doi.org/10.1177/20539517209199>.

e) Resumen

15. La detección de infracciones del derecho de autor es el ejemplo más común del uso de IA en la aplicación de los derechos de PI a escala, siempre que se disponga de sólidos conjuntos de datos de entrenamiento. Si se aplica de forma similar, la IA podría utilizarse también para detectar infracciones de diseños y marcas, lo que reduciría la demanda de recursos humanos.

16. El análisis de propiedad intelectual podría mejorar el descubrimiento de relaciones, tendencias y patrones de infracción de derechos de PI y mejorar así la toma de decisiones en materia de observancia.

17. La IA solo puede mejorar y hacerse más precisa y rápida, por lo que detectará patrones de forma muy superior a los humanos.

18. En general, la IA es una herramienta de filtrado útil y una ayuda al análisis humano para acelerar los procesos de detección de contenidos ilícitos.

B. PRINCIPALES DIFICULTADES

a) Derecho de autor

19. Preocupan los costos y recursos que implica utilizar herramientas automatizadas de observancia contra las infracciones del derecho de autor. Estas herramientas pueden estar fuera del alcance de muchas pymes titulares de derechos que dependen principalmente de organismos de gestión colectiva y organismos comerciales para hacer valer sus derechos.

20. Los sistemas antipiratería automatizados son opacos y dependen de reglas automatizadas de codificación rígida (*hard code*) que utilizan algoritmos dinámicos, potencialmente impredecibles y ocultos para la toma de decisiones.

b) Diseños

21. Las herramientas de IA podrían ayudar a consultar bases de datos de diseños registrados. Con todo, es posible que la IA no ayude a detectar infracciones de diseños no registrados o que dependen del derecho de autor.

22. Aparte de las bases de datos existentes, como la que gestiona ACID, los costos que conlleva el uso de la IA para detectar infracciones benefician a las grandes empresas propietarias de carteras de diseños.

23. Para la observancia de los derechos ligados a los diseños registrados y no registrados debe tenerse en cuenta el uso del diseño asistido por computadora (CAD, por sus siglas en inglés) y los diseños generados por IA, especialmente cuando los derechos sobre diseños no registrados se utilicen para entrenar a la IA.

c) Marcas

24. La observancia de las marcas se ve obstaculizada por los problemas de intercambio de datos entre organismos de observancia, gubernamentales y del sector, que impiden el uso de herramientas automatizadas a escala.

25. Los grupos que trabajan en el ámbito de la observancia se esfuerzan en obtener datos claros de sitios web con contenidos ilícitos y en recopilar grandes muestras de datos que sirvan para el entrenamiento de la IA.

d) Patentes

26. Al utilizar la IA para hacer valer los derechos de patentes deben combinarse conocimientos humanos y tecnológicos.

27. La complejidad del lenguaje que se utiliza en la solicitud de patentes y la complejidad, el costo y el esfuerzo de emprender acciones legales, suponen un reto para hacer valer los derechos de patente. Además, las restricciones a la utilización de pruebas de ingeniería inversa en los procedimientos judiciales ingleses hacen que sea difícil probar que se han infringido determinados derechos de patente.

28. Las infracciones de la propiedad intelectual generadas o asistidas por IA deben estar relacionadas con actos cometidos por una persona jurídica, por lo que puede ser necesario adoptar medidas de observancia contra aquellos que controlan la IA.

29. Las medidas de observancia que se aplican para luchar contra las infracciones de derechos de patentes relacionadas con la IA pueden verse dificultadas por la incertidumbre asociada a la IA “de caja negra”⁴ que desafía la comprensión humana.

30. Se considera que las herramientas de IA están poco adaptadas al Derecho de patentes, el cual requiere un pensamiento menos rígido y más imaginativo, así como capacidad de interpretación.

e) Secretos comerciales

31. La observancia de secretos comerciales se ve perjudicada por el miedo que existe a su divulgación pública en el marco de procedimientos judiciales, por lo que las controversias relacionadas con infracciones suelen resolverse extrajudicialmente. La observancia de secretos comerciales también se ve perjudicada por la incertidumbre relativa a su posible definición jurídica.

32. La IA se considera uno de los factores relevantes que intervienen en el aumento de robos de secretos comerciales en el entorno cibernético, problema que requiere a su vez nuevas herramientas de IA y aprendizaje automático para combatir los ciberataques.

33. También preocupa que la IA pueda utilizarse indebidamente para piratear secretos comerciales, y apoderarse de ellos, en lugar de para protegerlos.

34. Los secretos comerciales cubren información comercialmente valiosa que no está protegida por patentes ni por otros derechos de PI, y su respeto depende de la adopción de medidas razonables con las que mantener esa información en secreto, ya que solo así será esta de utilidad.

⁴ Es difícil entender cómo un modelo de IA de caja negra genera sus predicciones “porque su funcionamiento interno no está fácilmente disponible y es en gran medida autodirigido. Del mismo modo que es difícil mirar dentro de una caja pintada de negro, también lo es averiguar cómo funciona cada modelo de IA de caja negra”; véase Kinza Yasar e Ivy Wigmore, “Black Box AI”, disponible en: <https://www.techtarget.com/whatis/definition/black-box-AI>.

35. En ese sentido, la IA se considera menos útil en el futuro inmediato debido a los matices y la variedad de los secretos comerciales y al hecho de que en ningún momento se pretenda que estos sean públicos.

f) Cuestiones éticas

36. Dos de las limitaciones éticas de utilizar la IA para la observancia de los derechos de PI son la calidad de los conjuntos de datos de entrenamiento (por ejemplo, inadecuados o incompletos) que intervienen en los procesos de toma de decisiones y la sistemática parcialidad inherente de los humanos que podría dar lugar a decisiones injustas o incorrectas.

37. Hay también en la actualidad imperfecciones en la propia tecnología, como la falta de transparencia (especialmente en lo que respecta a la “IA de caja negra”) y de rendición de cuentas, así como un conocimiento incompleto de cómo funciona la IA.

38. También se teme que el proceso inflexible de toma de decisiones de la IA conduzca a un “bloqueo excesivo” de contenidos legales.

g) Cuestiones jurídicas

39. Sería necesario volver a entrenar las herramientas de IA para satisfacer las necesidades de las diferentes legislaciones sobre derechos de PI de los distintos territorios. También está el problema fundamental de seguir respetando el RGPD cuando los datos de entrenamiento de la IA impliquen utilizar volúmenes masivos de datos personales o sensibles.

40. Existe el peligro de que “agentes malvados” aprovechen la IA, por ejemplo su capacidad de volver a subir contenidos eliminados tras una notificación de retirada.

h) Resumen

41. Las principales dificultades son la calidad y la cantidad de datos de entrenamiento que se necesitan para utilizar eficazmente la IA en la observancia de la PI, así como las cuestiones fundamentales conexas en el ámbito ético y moral.

42. Un sistema de IA es un proceso que consume muchos recursos: existe una clara relación entre el volumen de datos utilizados por la IA y la precisión de los resultados.

43. El volumen, la calidad y la actualidad de los datos de entrenamiento suponen una preocupación común. Está claro que entrenar herramientas de IA lleva mucho tiempo y requiere constantes actualizaciones.

44. Dadas las limitaciones actuales de esta tecnología, así como las preocupaciones éticas que despierta, por el momento la IA solo debería utilizarse como una herramienta inicial que señale contenidos a un analista humano para su verificación, y no para hacer que se cumplan los derechos de PI de manera independiente.

III. CONCLUSIONES Y RECOMENDACIONES

A. CONCLUSIONES

45. En el uso de la IA y el aprendizaje automático para la observancia de cada uno de los cinco derechos de PI, las dificultades superan a las oportunidades, principalmente debido a cuestiones fundamentales relacionadas con el uso de la IA en la observancia de patentes y secretos comerciales.

46. El uso de la IA en la observancia de los derechos de PI sigue suscitando preocupación, a saber:

- Las advertencias en torno a los problemas metodológicos comunes relacionados con el uso del aprendizaje automático en las ciencias cuantitativas, subrayados en un estudio de Princeton de 2022.⁵
- El inacabable escándalo del programa informático Horizon del organismo de correos británico, que puso de manifiesto “los peligros de que los humanos acepten ciegamente los resultados de sistemas automatizados como pruebas fiables”. La expresidenta de la Law Society, Christina Blacklaws, advirtió de que el caso del organismo de correos debería “servir de advertencia para todas las organizaciones”. Podrían producirse problemas similares en otras organizaciones que han reducido sus recursos tecnológicos, externalizado conocimientos críticos y adoptado procesos de auditoría menos adecuados.⁶
- El fallido experimento del Gobierno australiano con Robodebt, que ACS calificó de “Desastre ético de la IA”.⁷
- La aparición del aprendizaje automático antagónico, en el que agentes con malas intenciones pueden aprovechar vulnerabilidades en los sistemas de IA y alterar su comportamiento al servicio de un objetivo malicioso. Estos ataques pueden consistir en el envenenamiento (de los datos de entrenamiento) o en ataques de evasión, muchos de los cuales pasan desapercibidos hasta que se produce un fallo crítico en el aprendizaje automático.

B. RECOMENDACIONES

47. Seguimos confiando en la capacidad de la IA y el aprendizaje automático para ofrecer soluciones ampliables que ayuden a la observancia de algunos, si no todos, los derechos de PI objeto de estudio. También insistimos en la mejora constante de la IA y el aprendizaje automático por sí mismos.

48. No podemos recomendar una mayor adopción de la tecnología sin hacer hincapié en las importantes advertencias descritas anteriormente.

49. Por ello, recomendamos que se realice cuidadosamente una prueba piloto de cualquier nuevo sistema de observancia de los derechos de PI basado en IA para determinar si en su

⁵ Sayash Kapoor y Arvind Narayanan (2023), “Leakage and the Reproducibility Crisis in Machine-learning-based Science”, *Patterns*, disponible en: <https://doi.org/10.1016/j.patter.2023.100804>.

⁶ John Thornhill (29 de abril de 2021), “Post Office Scandal Exposes the Risk of Automated Injustice”, *Financial Times*, disponible en <https://www.ft.com/content/08f485bf-6cea-46d6-962c-46263aaec5f3>.

⁷ El sistema Robodebt se diseñó para automatizar el cotejo de datos con miras a detectar discrepancias en los ingresos en el sistema fiscal y multiplicó casi por 40 el número de liquidaciones de impuestos, de 20 000 a casi 800 000 por año. En 2017, el defensor de pueblo del Commonwealth detectó problemas de transparencia, uso e imparcialidad en este sistema digital.

diseño se tienen en cuenta los inconvenientes mencionados y si la tecnología funciona dentro de los límites éticos, morales y legales para lograr sus objetivos principales.

[Fin de la contribución]

UN ENFOQUE INNOVADOR EN LA LUCHA CONTRA LA FALSIFICACIÓN: INSPECCIÓN DE PAQUETES MEDIANTE INTELIGENCIA ARTIFICIAL PARA LA OBSERVANCIA DE LA PROPIEDAD INTELECTUAL

*Documento preparado por la Sra. Karolina Zhytnikova, directora jurídica del Departamento de Protección de Marcas y Propiedad Intelectual, Countercheck GmbH, Berlín (Alemania)**

RESUMEN

La solución de Countercheck contra la falsificación utiliza una tecnología de inteligencia artificial (IA) que ayuda a proteger a los consumidores frente a mercancías peligrosas y a velar por la observancia de los derechos de los titulares de PI.

Incorporado en pleno corazón de la cadena logística, el *software* de Countercheck se integra directamente en los equipos informáticos ya instalados en los centros de clasificación de las empresas de logística. Este sistema supervisa todos los paquetes que pasan por el centro de distribución con miras a detectar e interceptar los paquetes susceptibles de contener productos falsificados.

Los marcos jurídicos obsoletos y desfasados con respecto al crecimiento exponencial del comercio electrónico son uno de los principales desafíos a los que se enfrenta Countercheck a la hora de poner en marcha su modelo de negocio. La rigidez de los mecanismos de incautación y destrucción de mercancías falsificadas en los flujos de paquetería postal y la falta de competencias para hacer frente con prontitud y eficiencia a los falsificadores que operan en los mercados interiores socavan la eficacia de las medidas destinadas a combatir la falsificación.

Cada vez son más las empresas de logística que adoptan un enfoque de tolerancia cero frente a las mercancías falsificadas en sus redes. Para responder con solvencia a los nuevos desafíos que se plantean en la lucha contra las falsificaciones, es indispensable una colaboración fluida entre todos los agentes de la industria tanto del sector público como del privado.

I. INTRODUCCIÓN

1. La popularización del comercio electrónico durante la pandemia instauró un nuevo modelo de comportamiento de los consumidores. Este fenómeno trajo aparejado un incremento drástico del volumen de productos pedidos por los consumidores de forma directa a través de las plataformas de comercio electrónico y las redes sociales. Por vía postal, los clientes no solo reciben productos auténticos, sino también artículos falsificados que entrañan una grave amenaza para su salud y su seguridad.

2. Por su parte, los distribuidores mayoristas de productos no auténticos también aprovechan en grado sumo este canal de distribución para surtirse de artículos falsificados. Los envíos postales no solo facilitan y abaratan las entregas, sino que la aleatoriedad del control de los envíos reduce el riesgo de que las autoridades encargadas de velar por la observancia de la ley los intercepten. Más aún, en caso de interceptación, el perjuicio que sufren los falsificadores es relativamente escaso en proporción a las cantidades que suelen transportarse

* Las opiniones expresadas en el presente documento corresponden a la autora y no reflejan necesariamente el punto de vista de la Secretaría de la OMPI ni el de sus Estados miembros.

en camiones y contenedores. Estos son los motivos esenciales que explican el atractivo de los paquetes postales o los envíos urgentes entre los falsificadores.

3. Conscientes de los desafíos expuestos, la industria logística, las autoridades encargadas de velar por la observancia de la ley y los titulares de derechos de propiedad intelectual destacan la conveniencia de proceder a la automatización del procesamiento y la preselección inteligentes de los envíos sospechosos en todo el recorrido de los paquetes.

II. LA TECNOLOGÍA DE INTELIGENCIA ARTIFICIAL DE COUNTERCHECK EN LA LUCHA CONTRA LAS MERCANCÍAS FALSIFICADAS

A. CONTRIBUCIÓN A LA INTEGRIDAD DE LA CADENA DE SUMINISTRO

4. La tecnología de IA encierra múltiples posibilidades en la lucha contra la falsificación. Entre ellas, cabe citar las soluciones de trazabilidad (seguimiento y localización), muy conocidas y utilizadas en la industria farmacéutica, tabacalera y automovilística. Con estos sistemas, los fabricantes y sus proveedores autorizados pueden verificar la autenticidad de los productos y detectar anomalías en las distintas fases de la cadena de suministro. Estas tecnologías ayudan a los titulares de derechos de PI a hacer un seguimiento en tiempo real del ciclo de vida de los productos auténticos y de las posibles desviaciones y alteraciones de los códigos de seguridad vigentes en el mercado.

5. El principio fundamental de la solución de Countercheck es el empleo de la tecnología de IA con el foco puesto en el análisis del flujo comercial en su totalidad, no solo en los productos auténticos. Con este método se pretende aislar los paquetes con un perfil de alto riesgo que puedan contener artículos falsificados y proporcionar a los titulares de derechos de PI y a las autoridades encargadas de velar por la observancia de la ley una idea más precisa y en tiempo real de los movimientos de los productos infractores de los derechos de PI (p. ej., nuevas rutas, puntos de entrada y países de tránsito, entre otros). La tecnología de Countercheck ayuda a detectar los tramos de la cadena donde el riesgo es mayor y a concentrar los esfuerzos de observancia en aras de la máxima eficacia.

B. MEJORA DE LA EFICACIA DE LAS INICIATIVAS DE LUCHA CONTRA LA FALSIFICACIÓN

6. La tecnología de IA de Countercheck interviene de forma directa en la cadena de suministro, en concreto, en los centros logísticos de clasificación. Con una interacción humana mínima, esta solución permite llevar un control automatizado de todo el flujo de paquetes y, cuando se detectan mercancías infractoras de los derechos de PI, interrumpirlo de manera selectiva y sin bloquear el resto de los productos legítimos.



7. Este proceso de detección consta de los pasos que se detallan a continuación.
- El sistema extrae toda la información de la apariencia externa de los paquetes sin analizar su contenido o interior.
 - El algoritmo de IA analiza la información conforme a más de 141 criterios sin intervención directa en el paquete y decide si hay que bloquear un envío para someterlo a un control más exhaustivo.
 - Si el sistema de evaluación de riesgos determina que el paquete puede contener un artículo falsificado con una probabilidad igual o superior al 80 %, da instrucciones al *hardware* para que deposite el paquete en una bandeja independiente.
8. Gracias a las últimas tecnologías de aprendizaje automático, se tarda 0,6 segundos en definir el “perfil de riesgo” de cada paquete que pasa por la cinta de clasificación. De este modo, es posible detectar con eficacia las falsificaciones eventuales sin interrumpir la actividad de los centros, ni provocar retrasos en las entregas de los paquetes.

III. OBSTÁCULOS A LA IMPLANTACIÓN DE LA TECNOLOGÍA BASADA EN INTELIGENCIA ARTIFICIAL EN EL MARCO JURÍDICO VIGENTE

A. FLUJO “INTERNO” DE PAQUETES

9. A escala europea, el Reglamento (UE) n.º 608/2013 del Parlamento Europeo y del Consejo, de 12 de junio de 2013, relativo a la vigilancia por parte de las autoridades aduaneras del respeto de los derechos de propiedad intelectual y por el que se deroga el Reglamento (CE) n.º 1383/2003 del Consejo (en adelante, Reglamento n.º 608/2013), dota a las autoridades aduaneras de mayores competencias para luchar contra las falsificaciones en las fronteras de la Unión Europea.

10. Pese a la creencia generalizada de que la mayoría de los productos falsificados se producen fuera de la Unión Europea y llegan a los países comunitarios desde el extranjero, conviene saber que una gran cantidad de falsificaciones se producen⁸ o ensamblan en territorio europeo.

11. Por desgracia, las legislaciones nacionales de los países europeos no siempre prevén mecanismos y competencias eficaces para que las autoridades responsables de velar por la observancia de la ley puedan atajar las falsificaciones en el mercado interior, en particular en lo que respecta al flujo “nacional” de paquetes. Francia⁹ es un ejemplo de país con un marco legislativo favorable a la lucha contra esta lacra.

12. En Francia, los titulares de derechos de PI no solo pueden presentar una solicitud de intervención en virtud del Reglamento (UE) n.º 608/2013, sino que también pueden fundamentarla en el Código de Propiedad Intelectual francés. Gracias a esta solicitud de intervención, se puede hacer un seguimiento de las mercancías en el territorio nacional. Es decir, las mercancías pueden quedar retenidas, aunque hayan superado el despacho de aduanas y se encuentren en libre circulación.

13. En efecto, la ausencia de control lleva a los mayoristas de falsificaciones a optar por los canales logísticos postales para el abastecimiento de mercadillos locales, vendedores ambulantes, tiendas ilegítimas, almacenes y fábricas al considerar que se trata de un modelo B2B (de empresa a empresa).

B. PROCEDIMIENTO PARA LA DESTRUCCIÓN DE PEQUEÑOS ENVÍOS

14. El Reglamento n.º 608/2013 también establece un procedimiento simplificado para la destrucción de mercancías sospechosas de infracción de la PI que no exige una decisión judicial previa (artículo 26). Este conocido procedimiento para la destrucción de pequeños envíos de mercancías falsificadas sin contactar con los titulares de derechos de PI se utiliza con frecuencia en las aduanas para el control fronterizo de los flujos de paquetes de venta a particulares procedentes de plataformas de comercio electrónico.

⁸ Por ejemplo, en Francia, la Gendarmería Nacional clausuró un centro clandestino de producción de cigarrillos falsificados. Noticia (disponible en inglés): <https://www.europol.europa.eu/media-press/newsroom/news/counterfeit-tobacco-products-worth-eur-17-million-seized-in-france>.

⁹ El artículo 66 del Código de Aduanas de Francia reconoce a las autoridades aduaneras el derecho a inspeccionar y acceder a las instalaciones de los proveedores de servicios postales y las empresas de transporte urgente de mercancías: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071570/LEGISCTA000006138845/.

15. No obstante, en cuanto estas mercancías se despachan de aduana o en caso de que se hayan producido en un país de la Unión Europea y luego se hayan expedido a otro país comunitario por vía postal, este procedimiento de destrucción simplificada para pequeños envíos deja de ser aplicable. En la Unión Europea no hay un marco jurídico armonizado en la materia y son pocos los países que han incorporado planteamientos avanzados sobre el tema en sus legislaciones nacionales. Por ende, en la mayoría de los casos, la interceptación de mercancías sospechosas en el mercado interior entra en el ámbito de competencia de la policía. Para proceder a la incautación y posterior destrucción de las mercancías falsificadas, las autoridades responsables de velar por la observancia de la ley (la policía) han de poner en marcha y aplicar el procedimiento ordinario (no el simplificado), sin importar que se trate de un par de zapatos o de un lote de 500 artículos de productos presuntamente falsificados.

16. La ausencia de un mecanismo eficaz para la incautación y destrucción simplificada de todos los envíos postales es uno de los mayores escollos jurídicos a los que se enfrenta Countercheck en la implantación de su tecnología.

IV. UN NUEVO MODELO DE RESPONSABILIDAD SOCIAL Y EMPRESARIAL CON RESPECTO A LOS CONSUMIDORES FINALES Y LOS ASOCIADOS COMERCIALES EN EL MUNDO DE LA LOGÍSTICA

17. Para concluir, conviene señalar que las tecnologías de IA contribuyen a mejorar la eficacia de nuestro trabajo y que la automatización de procesos rutinarios ahorra mucho tiempo a las autoridades responsables de velar por la observancia de la ley. Ahora bien, hay que tener en cuenta otro elemento esencial en aras de una lucha aún más fructífera contra el tráfico ilícito de mercancías infractoras de la PI. Este elemento no es otro que la colaboración.

18. Cada vez es más habitual que las grandes empresas de logística adopten un enfoque de tolerancia cero ante las mercancías falsificadas en sus redes como medida de observancia de la ley y como muestra de responsabilidad empresarial para con sus asociados en el mundo de la logística. Por otra parte, así transmiten un enérgico mensaje a la comunidad sobre su responsabilidad social de cara a los consumidores y su voluntad de proteger a la sociedad de las mercancías peligrosas.

19. A través de la plataforma de Countercheck, las empresas de logística, los titulares de derechos de PI, las autoridades aduaneras y las encargadas de velar por la observancia de la ley trabajan en sintonía para dar una respuesta rápida y contundente a los falsificadores. La detección eficaz de mercancías sospechosas mediante tecnología de IA, la confirmación ágil de las falsificaciones por parte de los titulares de derechos de PI en la plataforma específica de Internet (en un plazo de 24 horas) y la estrecha colaboración con las autoridades aduaneras y las responsables de velar por la observancia de la ley son factores que favorecen la integridad de la cadena de suministro.

20. De cara al futuro, auguramos una cooperación aún más estrecha entre los sectores público y privado, pues se trata de una condición *sine qua non* para combatir los delitos que atentan contra los derechos de PI. En particular, esperamos que se produzcan ciertos cambios para democratizar la posibilidad de que el sector privado intervenga en las actividades pertinentes ante el fenómeno de la “fragmentación” del flujo de falsificaciones, a saber, el envío de falsificaciones en pequeñas partidas independientes en lugar de en grandes cantidades.

21. Asimismo, cabe esperar un ajuste del marco jurídico, hoy obsoleto, para reducir el exceso de precauciones y su consiguiente repercusión en los plazos previstos para la destrucción de las mercancías falsificadas, así como la puesta en marcha de procedimientos eficaces contra las falsificaciones en el flujo “nacional” de paquetes.

22. Por último, la solución de Countercheck incorpora una serie de funcionalidades, como un análisis de riesgos integrado de la totalidad del flujo de paquetes, un control en tiempo real de la cadena de suministro y una abundante fuente de información para profundizar en la investigación de las redes delictivas, todas ellas imprescindibles para abordar los nuevos desafíos que plantea la lucha contra las mercancías falsificadas. La unión de las fuerzas de todas las partes interesadas en el sector de la protección de las marcas es la única vía para lograr resultados más significativos y crear un ecosistema seguro donde no haya cabida para los falsificadores.

[Fin de la contribución]

EL USO QUE HACEN DE LA INTELIGENCIA ARTIFICIAL LOS PIRATAS Y LOS TITULARES DE LOS DERECHOS EN LA INDUSTRIA MUSICAL

*Documento preparado por el Sr. Graeme Grant, vicepresidente de Global Content Protection, Universal Music Group, Hilversum (Países Bajos)**

RESUMEN

En este documento se expone la opinión de Universal Music Group (UMG) respecto de la inteligencia artificial (IA), prestando atención especial a su uso responsable ante la gran preocupación que suscitan las infracciones de la propiedad intelectual (PI). UMG, como empresa líder de la industria musical, utiliza la IA con fines diversos, que van desde la ayuda al *marketing* hasta su empleo como herramienta creativa. Si bien la IA tiene un gran potencial de innovación y expansión, la IA generativa también plantea grandes riesgos, no solo para los creadores, sino también para la sociedad en general. Por ejemplo, los ultrafalsos y otros fraudes relacionados con la IA generativa también amenazan la privacidad de las personas y la seguridad de los consumidores. En el artículo se analiza el aumento de las actividades no autorizadas, como el uso de la IA para imitar a artistas y crear canciones fraudulentas y la utilización de obras musicales para entrenar plataformas de IA sin obtener la licencia correspondiente. Estos usos no autorizados son cada vez más frecuentes en las plataformas digitales, lo que plantea problemas en relación con la observancia de los derechos de PI y hace temer por la integridad del trabajo de los artistas en el futuro. UMG concluye que la IA puede servir a los intereses de los artistas y de la creatividad si se utiliza de manera responsable, pero que, si se utiliza de manera irresponsable, se convierte en una amenaza grave.

I. ANTECEDENTES

1. La música es un relato que se narra a través de la armonía entre la expresión y la emoción. Los compositores y los artistas cuentan sus relatos con una narrativa y una voz propias. A través de su música comparten experiencias que la mayoría de nosotros nunca viviremos y nos transportan a lugares a los que nunca iremos. Su creatividad es la banda sonora de nuestras vidas y, si no fuera por los fundamentos del derecho de autor, quizá nunca los habríamos conocido.
2. Universal Music Group (UMG) alberga una gran variedad de empresas relacionadas con la música, entre las que se incluyen empresas de grabación, edición musical, venta de artículos de promoción y contenidos audiovisuales. Asimismo, cuenta con un amplio catálogo de grabaciones y canciones de todos los géneros musicales y se dedica a descubrir artistas y compositores y a desarrollar sus carreras, así como a producir y distribuir en todo el mundo música de gran éxito comercial y de crítica.
3. UMG es una empresa comprometida con el arte, la innovación y el espíritu empresarial, que fomenta el desarrollo de servicios, plataformas y modelos empresariales con el fin de ampliar las oportunidades artísticas y comerciales de los artistas y crear nuevas experiencias para sus seguidores.
4. Por otra parte, la empresa ha apostado por la inteligencia artificial (IA), al igual que ha hecho con otras innovaciones tecnológicas desde hace varios decenios. La utiliza con fines de

* Las opiniones expresadas en el presente documento corresponden al autor y no reflejan necesariamente el punto de vista de la Secretaría de la OMPI ni el de sus Estados miembros.

marketing y para recopilar información a fin de aumentar los seguidores de los artistas, así como para impulsar el proceso creativo en los estudios y optimizar la producción. No en vano, UMG es titular de varias patentes de IA.

5. Algunas tecnologías de IA más recientes, especialmente la “IA generativa”, que ha irrumpido con fuerza en los últimos meses, suponen tanto oportunidades como riesgos considerables para la comunidad creativa. La IA puede ofrecer herramientas de vanguardia, que mejoren la creatividad humana, a los artistas que deseen utilizarla, pero algunos de sus usos entrañan grandes riesgos.

6. Si se utiliza sin respetar los derechos de los artistas, la tecnología de la IA generativa plantea riesgos para la comunidad creativa y los contenidos creados por dicha comunidad.

II. USOS INFRACTORES DE LA INTELIGENCIA ARTIFICIAL EN LA INDUSTRIA MUSICAL

A. ENTRENAMIENTO NO AUTORIZADO DE PLATAFORMAS DE INTELIGENCIA ARTIFICIAL

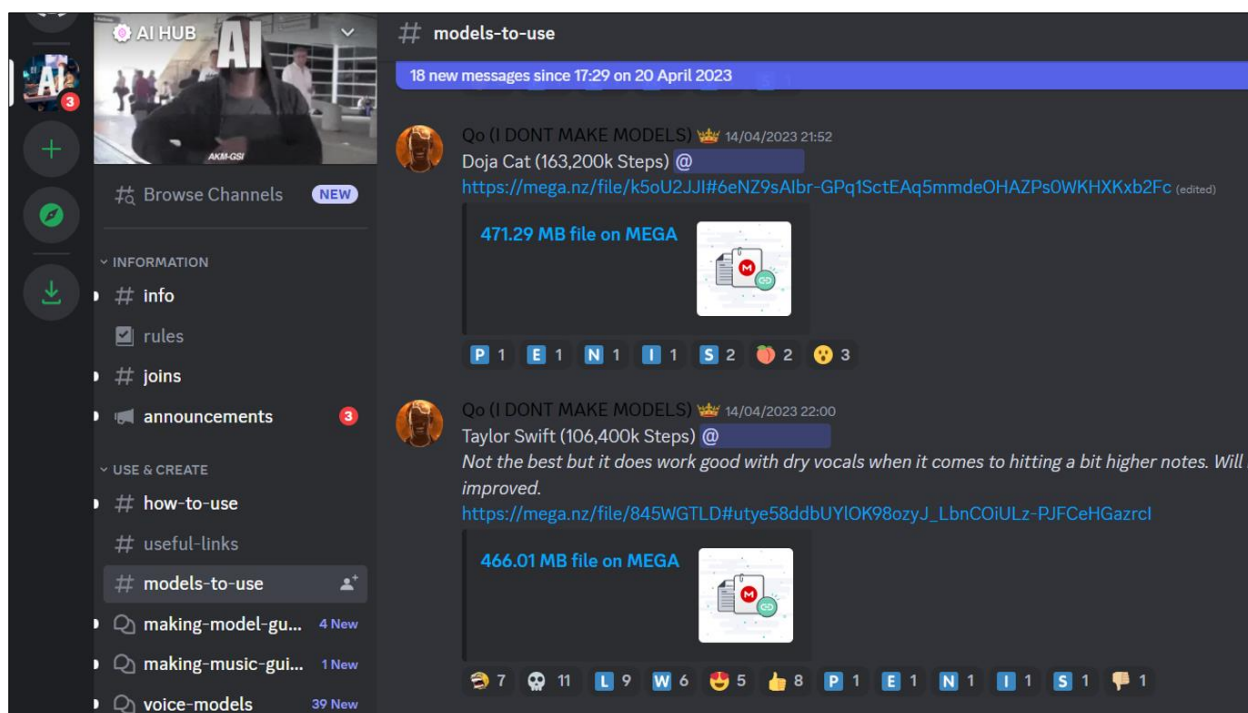
7. Algunas plataformas de IA se entrenan ilícitamente con contenidos protegidos por derecho de autor, con lo que se infringen los derechos de los creadores. Tras este entrenamiento, se utilizan para infringir aún más los derechos mediante la creación de productos que utilizan dichos contenidos. Las plataformas en cuestión no solicitan autorización prácticamente en ningún caso, y mucho menos la obtienen. Por el contrario, normalmente tratan de evitar toda transparencia en cuanto al uso que hacen de las obras musicales, al tiempo que utilizan estas infracciones para promover su propia actividad comercial.

8. En el último año UMG ha observado un aumento notable en la utilización de la IA para crear canciones en las que se imitan el estilo y la voz propios de los artistas. Están surgiendo comunidades en línea especializadas, no solo en crear y distribuir estas canciones fraudulentas, sino también en ofrecer tutoriales completos en los que se enseña a cualquier persona todo el proceso necesario para llevar a cabo esta actividad no autorizada, así como las herramientas, como los bots, que ejecutan automáticamente los procesos de clonación de voz mediante IA. El número de cargas generadas por IA en plataformas de contenidos creados por usuarios en las que se han visto afectados nuestros derechos ha crecido un 175 % desde agosto de 2023. Aproximadamente el 47 % de las notificaciones enviadas hasta la fecha se produjeron porque se detectó un disco matriz propiedad de UMG en la voz o en los instrumentos de base; el resto estuvieron motivadas por infracciones del derecho de autor de obras musicales o literarias, de marcas o del derecho de publicidad.

9. Las nuevas tecnologías conocidas como “separadores de pistas” aprovechan la IA para aislar las partes vocales e instrumentales de los discos matriz de audio (UMG utiliza esta tecnología para ayudar a sus artistas). Estos elementos separados se utilizan posteriormente para entrenar sofisticados modelos de IA. El uso total o parcial de los discos matriz de UMG sin autorización o licencia constituye una infracción del derecho de autor. Esta forma relativamente nueva de infracción se combina con métodos más antiguos, como el *stream ripping*, que consiste en extraer el componente de audio de una obra audiovisual (normalmente de una plataforma con licencia como YouTube) y reproducirlo. De este modo se sortean las medidas técnicas de protección que aplican las plataformas de *streaming* autorizadas para prevenir el uso no autorizado de los contenidos y se infringen las condiciones de uso de las plataformas. El contenido “copiado” sirve de base para estos algoritmos de separación de pistas.

10. Los proveedores de servicios digitales y las plataformas de contenidos cargados por los usuarios son utilizadas con frecuencia por los creadores de IA para publicar y rentabilizar sus creaciones, lo que a menudo implica el uso no autorizado de obras protegidas por derecho de autor (entre las que se incluyen ilustraciones de carátulas de discos, discos matriz, composiciones y letras de canciones) o de marcas registradas de los artistas (como sus nombres y logotipos). Aunque en algunos casos se pueden suspender o eliminar las cuentas de los infractores, muchas veces estos pueden crear cuentas nuevas para perpetuar sus actividades ilícitas. Por si fuera poco, estos infractores pueden manipular las transmisiones o cometer fraudes con las regalías inflando artificialmente el número de reproducciones para aumentar injustamente los ingresos a gran escala, en detrimento de los artistas y de los titulares legítimos de los derechos.

11. En los últimos meses, UMG ha observado con preocupación que los colectivos implicados en las infracciones de la PI han mostrado una agilidad alarmante para modificar sus técnicas. Inicialmente, durante las primeras etapas de desarrollo de las infracciones mediante IA generativa, era posible conseguir la retirada de los contenidos no autorizados con base en la legislación vigente en materia de derecho de autor en los casos en que una voz generada mediante IA se mezclaba sobre nuestro disco matriz original sin autorización. A medida que ha ido avanzando su desarrollo, la IA se ha ido utilizando para crear contenidos en los que se clona la voz de un artista, pero sin que se aprecie el disco matriz de forma tan evidente, lo que dificulta aún más la retirada de estos contenidos.



B. MODELOS DE VOZ DE INTELIGENCIA ARTIFICIAL

12. La colección de grabaciones de audio, letras e ilustraciones de carátulas protegidas por derecho de autor de UMG se ha utilizado de forma ilícita para entrenar algunos modelos de voz de IA. Asimismo, algunos creadores de música especializados han explotado de forma similar las obras musicales protegidas por derecho de autor de UMG. Con frecuencia, estas actividades no autorizadas se basan en el *stream ripping*. Una vez que los modelos están perfectamente entrenados, se suelen difundir a través de comunidades sociales en plataformas como Discord y Reddit, y en repositorios como GitHub y Hugging Face. Muchas veces los

modelos van acompañados de tutoriales completos y detallados sobre cómo emplearlos para generar nuevas obras derivadas.

13. En la figura 1 se muestra el uso no autorizado de una obra protegida por derecho de autor de UMG para crear un modelo de voz. Obsérvese que cada línea de la canción se ha dividido en archivos de sonido individuales con el fin de asignar el sonido a palabras específicas.

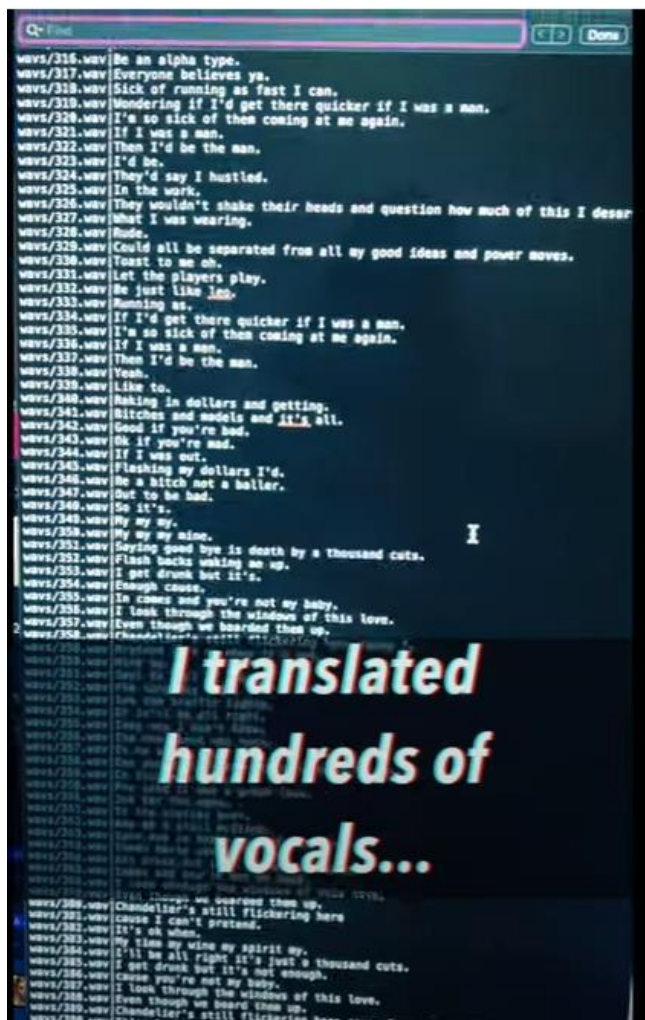


Figura 1 - Entrenamiento de un modelo de voz

14. Por poner otro ejemplo, una comunidad en línea ha creado una hoja de cálculo que contiene más de 100 modelos de voz previamente entrenados de artistas concretos, que se han cargado en servicios como Megaupload y Google Drive y que cualquiera de sus 15 000 miembros puede descargar y utilizar.

15. Estos modelos de voz se utilizaron para crear una pista fraudulenta titulada *Heart on My Sleeve*, en la que se imitaban las voces de Drake y The Weeknd y que se cargó en los proveedores de servicios digitales. La pista original contenía un *sample* de una canción perteneciente a UMG titulada *No Complaints*, de Metro Boomin, y tuvo que ser retirada por infringir el derecho de autor. Posteriormente se cargó en los proveedores de servicios digitales una nueva versión de *Heart on My Sleeve* sin el *sample* de Metro Boomin, que fue denunciada por infringir los derechos de marca y nombre, imagen y apariencia.

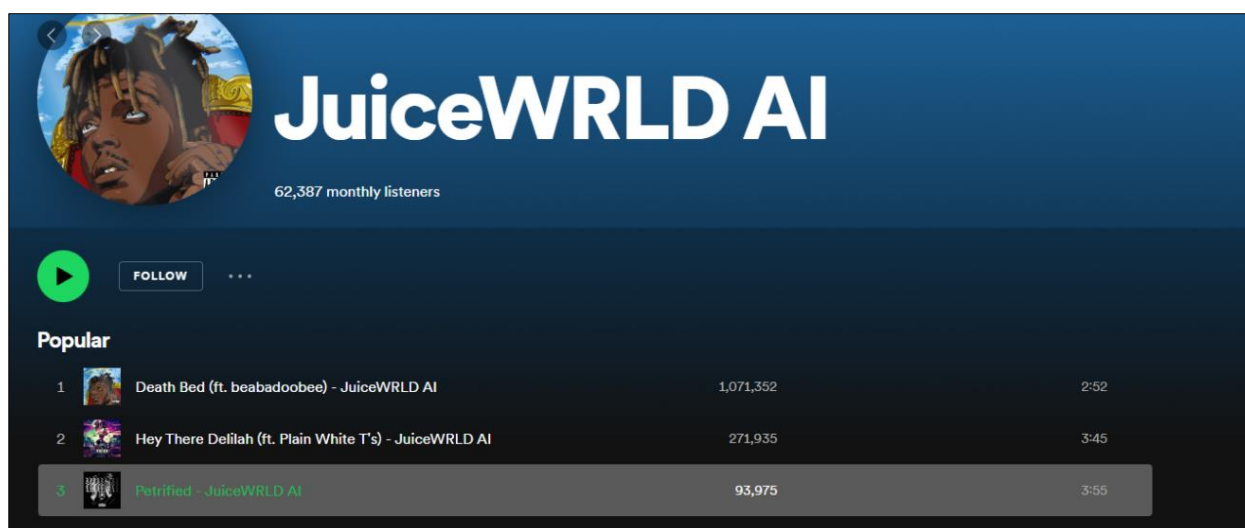
C. PRELANZAMIENTO DE CANCIONES FRAUDULENTAS

16. Cada vez es más frecuente que los estafadores utilicen la IA para decir que van a prelanzar canciones y ponerlas a la venta. Estas personas suelen cargar en sitios populares de descargas fragmentos breves de canciones generadas por IA en los que se suplantan las voces de artistas de UMG, afirmando falsamente que han obtenido las canciones directamente de los artistas a través de medios ilícitos como la piratería informática, la suplantación de identidad o la representación falsa. Los usuarios, convencidos de la autenticidad de estas canciones, suelen realizar “compras en grupo”, reuniendo sus recursos para alcanzar los precios exagerados que piden los estafadores, que pueden oscilar entre 5 000 y 30 000 dólares de los Estados Unidos. Los usuarios no suelen ser conscientes de que la canción en cuestión no ha sido creada por el artista, sino por tecnología de IA.



D. PUBLICACIÓN DE CANCIONES FRAUDULENTAS EN PROVEEDORES DE SERVICIOS DIGITALES

17. Los creadores de canciones fraudulentas a partir de modelos de IA entrenados previamente utilizan proveedores de servicios digitales como YouTube, Spotify, Deezer o Apple Music para generar ingresos. Para ello se sirven de agregadores a fin de cargar las canciones falsas en dichos proveedores y reclamar todos los derechos sin reconocer el uso de contenidos protegidos por derecho de autor, ni en la canción completa ni en el modelo de IA utilizado para imitar al artista. Las regalías procedentes de las “reproducciones” de la canción en los proveedores de servicios digitales no se destinan a los artistas ni a los titulares de los derechos, sino a la persona que cargó la canción fraudulenta (véase el ejemplo de JuiceWRLD).



18. A menudo se cargan canciones con perfiles falsos de los artistas (Juice AI, Drake AI) para que los titulares de los derechos y los propios proveedores de servicios digitales no las detecten. En los sitios de contenidos cargados por los usuarios como YouTube, TikTok e Instagram, las canciones se cargan utilizando el nombre del artista real o etiquetándolo para generar visitas y aumentar así los ingresos por publicidad.

19. Sirva como muestra del crecimiento del problema el caso de un proveedor de servicios cuyo número de cargas de IA aumentó de aproximadamente 50 a más de 400 al día en seis meses.

E. CIBERATAQUES CON AYUDA DE LA INTELIGENCIA ARTIFICIAL

20. La IA se ha convertido cada vez más en una herramienta fundamental para organizar ciberataques, lo que representa un cambio en el panorama de las amenazas contra la ciberseguridad. Los piratas informáticos pueden utilizar algoritmos de aprendizaje automático y otras técnicas computacionales avanzadas para automatizar el proceso de detección de vulnerabilidades en los sistemas y redes de las compañías discográficas, con lo que se reduce el tiempo y los conocimientos necesarios para llevar a cabo sus ataques, los cuales, a menudo se llevan a cabo con el fin de hacerse con las obras antes de su lanzamiento para venderlas u obtener partes de audio que luego se utilizan para entrenar modelos de IA y crear obras no autorizadas.

III. USO DE LA IA POR LOS TITULARES DE LOS DERECHOS

21. UMG ya pensaba en la IA mucho antes de que una grabación generada por IA en la que se imitaba a Drake y The Weeknd (ambos pertenecientes al catálogo de Universal Music) se hiciera viral y captara la atención de la prensa y de los encargados de formular políticas.

22. En noviembre se publicó una grabación nueva de los Beatles titulada *Now and Then*, en la que se utilizó la IA para extraer de una maqueta antigua la voz de John Lennon con una calidad suficiente para utilizarla en esta grabación nueva.

23. Ingrooves, una de las empresas que integran UMG, posee tres patentes relacionadas con la IA y destinadas a ayudar en la comercialización de artistas independientes. La IA también se utiliza desde hace tiempo como herramienta en el estudio, por ejemplo Apple Logic Pro X para generar pistas de batería, o Captain Plugins para crear progresiones de acordes. UMG también recurre con frecuencia a la IA como herramienta de ayuda para la creación de música inmersiva en Dolby Atmos.

24. El equipo de seguridad de UMG utiliza la IA para proteger a los empleados, a los artistas y a las partes interesadas contra las amenazas en materia de ciberseguridad, que son muy numerosas y cada vez más sofisticadas.

25. El equipo de protección de contenidos de UMG utiliza modelos de IA para ayudar a clasificar las infracciones basadas en un título, crear una puntuación de las infracciones basada en metadatos y utilizar el reconocimiento de imágenes para detectar falsificaciones físicas y usos no autorizados de nuestras marcas y logotipos. Por ejemplo, los vendedores de productos infractores pueden utilizar imágenes originales pero tomadas desde ángulos diferentes, en tamaños y colores distintos o con otros materiales. El reconocimiento de imágenes por IA es capaz de detectar que estas imágenes se basan en la misma imagen original, con lo que aumenta la tasa de detección. Así, la IA fue capaz de buscar la marca "Billie Eilish" y leer con

precisión las palabras en las imágenes de las falsificaciones que se muestran a continuación, y ello a pesar de la distorsión visual que se observa en el ejemplo 1.



Ejemplo 1



Ejemplo 2

26. Hasta la fecha hemos detectado y eliminado más de 200 000 anuncios de productos falsificados o no autorizados valorados en más de 45 millones de dólares.

27. El equipo de tecnología de UMG utiliza la IA para hacer que el catálogo de UMG sea más fácil de buscar y encontrar, lo que ayuda a los equipos internos y aumenta las oportunidades comerciales de los artistas de UMG.

IV. REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL

28. La IA es una gran tecnología si se utiliza de forma responsable, y UMG la utiliza en todas las fases del desarrollo musical.

29. La política pública en materia de IA está dando sus primeros pasos a nivel internacional. En los Estados Unidos de América, la Unión Europea y el Reino Unido se están adoptando iniciativas destinadas a regularla.

30. UMG respalda los compromisos adquiridos por el G7, incluidos los que se recogen en el comunicado emitido por los líderes en la cumbre de Hiroshima en mayo de 2023. En el comunicado y en la declaración se hace hincapié en los aspectos siguientes: 1) la participación de “múltiples partes interesadas” en la elaboración de normas sobre IA en las que se dé prioridad a la imparcialidad, la transparencia y el cumplimiento de las leyes vigentes; 2) el compromiso con una “IA centrada en las personas y digna de confianza”; y 3) el examen y análisis continuos sobre la mejor manera de salvaguardar los derechos de propiedad intelectual (PI), incluido el derecho de autor.

31. En la Ley de Inteligencia Artificial de la Unión Europea se incluyen propuestas útiles para su examen por los gobiernos en relación con los modelos de IA generativa previa al lanzamiento, la evaluación continua de esos modelos, las disposiciones relativas al mantenimiento de registros, la transparencia, las obligaciones de etiquetado, etcétera. Asimismo, se recogen muchos de los principios generales anunciados por el G7, entre ellos el

énfasis en la aplicación de normas de IA impulsadas por los creadores, justas y transparentes que, entre otras cosas, respeten los derechos de PI. La versión final de la Ley está siendo objeto de debate actualmente en las negociaciones tripartitas (“diálogo tripartito”), y UMG espera que se adopte la posición del Parlamento Europeo en lo que respecta a contabilidad y transparencia.

32. Es fundamental que las entidades más importantes de la cadena de la IA generativa mantengan registros detallados, incluso de los materiales, las obras u otras materias protegidas de terceros que se hayan utilizado, además de la base que permitió acceder a ellos, y que pongan esta información a disposición de las partes legítimamente interesadas.

33. Se deberían evitar algunas políticas, por ejemplo las excepciones a la legislación en materia de derecho de autor que se promulgaron en 2021 en Singapur en relación con la prospección de textos y la extracción de datos. Asimismo, en la legislación introducida en el Japón en 2009 y modificada en 2018 también se incluye una excepción demasiado amplia que, si bien no es ilimitada e incluye algunas protecciones para los titulares de los derechos, puede causar confusión. En un contexto en el que la IA generativa engulle cantidades enormes de datos de forma incontrolada, este tipo de excepciones son contrarias a los principios básicos de equidad y a la finalidad de la legislación en materia de derecho de autor de recompensar el esfuerzo creativo. UMG se alegra de que el Reino Unido rechazara explícitamente la aplicación de este tipo de políticas el año pasado, consciente del daño irrevocable que ello infligiría a sus industrias creativas.

34. En general, UMG opina que no es necesario modificar la legislación actual en materia de derecho de autor, siempre que se interprete, se aplique y se observe correctamente. No obstante, en algunos territorios puede ser necesario aumentar la protección de los derechos personales (es decir, la voz y la apariencia).

V. CONCLUSIÓN

35. La IA al servicio de los artistas y la creatividad puede dar lugar a herramientas maravillosas que utilizamos en las distintas fases de la creación musical. UMG colabora con numerosas plataformas, empresas, artistas y creadores que utilizan la IA de forma responsable.

36. Por el contrario, si se utiliza para socavar el uso legítimo de la música, ingiriendo música sin permiso para influir indebidamente en la relación que los seguidores desean tener con los artistas y creadores en la vida real o, lo que es peor, apropiándose de su trabajo (o de su nombre, imagen, apariencia o voz) sin autorización, la IA no aporta nada al ecosistema musical.

[Fin de la contribución]

USO DE INTELIGENCIA ARTIFICIAL PARA LA DETECCIÓN Y REMOCIÓN AUTOMÁTICA DE OFERTAS DE PRODUCTOS FALSIFICADOS EN LOS SITIOS DE MERCADO LIBRE

*Documento preparado por el Sr. Gustavo Bertelli, director de aprendizaje automático, ejecución y tecnologías de aprendizaje automático, y Sra. Guadalupe Yamila García Crespo, directora de protección de marca, relaciones jurídicas y gubernamentales, Mercado Libre, Buenos Aires (Argentina)**

RESUMEN

Distintas normativas alrededor del mundo regulan sobre la limitación de la responsabilidad de los intermediarios en Internet y sobre la implementación de mecanismos de instancia privada para la denuncia de ofertas que infrinjan derechos de Propiedad Intelectual e Industrial de terceros. Pero en América Latina son pocos los países que cuentan con regulación al respecto.

Por ese motivo, una plataforma de comercio electrónico que opere en la región se enfrenta a los desafíos de la autorregulación y a los riesgos de no poder ampararse en puertos seguros, debiendo equilibrar estos aspectos con la necesidad de combatir las ofertas de productos falsificados en su entorno para mantener altos estándares en la calidad de los servicios que brinda a sus usuarios.

A esta situación se suma que la implementación de las buenas prácticas de la industria en esta materia, implica complementar a esos mecanismos de denuncia de instancia privada con modelos de Inteligencia Artificial que detecten de manera proactiva y automática ofertas infractoras. Esto conlleva al desafío adicional de contar con una fuente segura y constante de conocimiento sobre esas infracciones, que pueda obtenerse del análisis de las denuncias que los titulares de derechos realicen, y de mantener actualizado su sistema para que la detección sea fidedigna. El presente trabajo explora estos escenarios desde la experiencia de Mercado Libre.

El desarrollo de soluciones para combatir la oferta de productos falsificados en el comercio electrónico presenta desafíos particulares en América Latina. El presente trabajo se concentra en la experiencia de Mercado Libre relacionada a la remoción automática de productos falsificados que pudieran ofrecerse en sus sitios y explora brevemente la temática desde un punto de vista legal y tecnológico, sin pretender agotarla.

I. BREVE CONTEXTO DE LA NORMATIVA EN LATINO AMÉRICA Y DEL MECANISMO DE DENUNCIA DE INSTANCIA PRIVADA IMPLEMENTADO POR MERCADO LIBRE

1. El marco normativo que regula la responsabilidad de los intermediarios de Internet en materia de infracciones a la Propiedad Intelectual o Industrial ha evolucionado de manera diferente en los distintos países que conforman la región.
2. El primer antecedente podemos encontrarlo en Chile con la modificación en 2010 a la Ley de Propiedad Intelectual Nro 17.336. Esta modificación introdujo en ese país un sistema de notificación judicial para la remoción de contenidos que infrinjan derechos de autor, a la vez que contempla la posibilidad de una solicitud extrajudicial que solo obliga al intermediario a

* Las opiniones expresadas en el presente documento corresponden al autor y no reflejan necesariamente el punto de vista de la Secretaría de la OMPI ni el de sus Estados miembros.

notificar a su usuario del reclamo recibido por la existencia de una supuesta infracción. Desde esa fecha, otros países como Paraguay y Brasil han regulado la limitación de la responsabilidad de los intermediarios de Internet, estableciendo principalmente la necesidad de una notificación judicial para que se configure el conocimiento específico y efectivo a fin de que el contenido en supuesta infracción sea removido.

3. Recién en 2020 las modificaciones a la Ley de Derechos de Autor en México replicaron, como resultado del Tratado entre México, Estados Unidos y Canadá, un mecanismo de notificación extrajudicial de instancia privada como el contemplado en la modificación de 1998 a la Copyright Act estadounidense, norma conocida como la Digital Millennium Copyright Act o DMCA por sus siglas en inglés.
4. Al mismo tiempo, distintos pronunciamientos judiciales fueron recepcionando los criterios del conocimiento efectivo mediante la identificación de los contenidos en supuesta infracción, aún en países como Argentina donde todavía no se cuenta con una legislación específica en la materia pero si consolidada con jurisprudencia del máximo tribunal local enfatizando este dogma.
5. En este escenario, las buenas prácticas en la industria del comercio electrónico, desarrolladas tanto en la región como en otras partes del mundo, fueron imponiéndose a lo que resultara obligatorio por la ley, y abrieron camino a la implementación de medidas voluntarias o autorreguladas por parte de los intermediarios.
6. Esas medidas voluntarias, en ocasiones consensuadas con otros actores del sector privado y con organismos de gobierno, se enmarcan en el principio rector que no impone un monitoreo general obligatorio por parte del intermediario, y requieren del conocimiento y la experiencia que poseen los titulares de Propiedad Intelectual o Industrial así como de su compromiso en el ejercicio de sus derechos a través de mecanismos de denuncia y retirada.
7. En ese contexto, las infracciones a derechos de Propiedad Intelectual e Industrial en general, y en particular aquellas que involucren falsificación marcaria en la publicación de un producto que se ofrezca utilizando los servicios de una plataforma, pueden denunciarse a través de estos mecanismos de denuncia y retirada que se ponen a disposición del usuario. En el caso de Mercado Libre pueden denunciarse a través de un canal exclusivo que la compañía pone a disposición de los titulares de derechos, denominado Brand Protection Program o BPP.
8. Pero las soluciones de Mercado Libre para combatir la oferta de producto falsificado en su entorno no se limitan a ese canal de denuncias. La compañía ha desarrollado distintas iniciativas que la llevan a buscar aprender de las denuncias que recibe para detectar patrones infractores que le permitan remover publicaciones sin la necesidad de una denuncia del titular de derechos, combinando en ciertos casos estos aprendizajes con un trabajo en conjunto llevado a cabo directamente con los propietarios de esos derechos.
9. Esto se relaciona con la constante evolución de las buenas prácticas que tiene la industria y también con la evolución de la normativa y jurisprudencia en la materia. En ese sentido, en la actualidad los mecanismos de denuncia y retirada son complementados por esfuerzos proactivos que realizan las plataformas de comercio electrónico que intentan aprender tendencias en la infracción a marcas, esfuerzos que también realiza Mercado Libre en los países donde opera.
10. El siguiente paso luego de brindar un canal de denuncias a los titulares, es educar a los usuarios explicando cuáles son los derechos de Propiedad Intelectual e Industrial existentes y la manera que tienen de publicar sus productos sin infringir derechos de terceros o de contestar las denuncias que recibieran para acreditar ante el titular que su producto fuera original. En el

caso de Mercado Libre, una denuncia implica el pausado inmediato de la publicación, y la apelación o contestación de una denuncia por parte del usuario vendedor no reactiva su publicación. Es el titular de derechos el que analiza la respuesta del vendedor y comunica a la plataforma su decisión de reactivar la publicación o removerla definitivamente. Las remociones definitivas son el insumo para aprender tendencias o patrones infractores y para sancionar infractores reincidentes.

11. Ahora bien, en una región donde como hemos explicado prevalece la falta de regulación sobre la responsabilidad de los intermediarios, y con ello también la falta de puertos seguros a los que esos intermediarios puedan acogerse para dar fundamento a la remoción de contenido en supuesta infracción, la denuncia de los titulares de derechos es muy relevante no sólo para justificar la medida directamente tomada sobre la publicación denunciada, sino también para fundamentar cualquier medida proactiva tomada en base al aprendizaje de las denuncias. En el próximo capítulo se analizarán las cuestiones técnicas que involucran el uso de Inteligencia Artificial (IA) para intentar detectar de manera proactiva ofertas de productos falsificados en la plataforma.

II. LA INTELIGENCIA ARTIFICIAL COMO HERRAMIENTA PARA LA DETECCIÓN DE PRODUCTOS FALSIFICADOS

12. La Organización Mundial de la Propiedad Intelectual explica que a la fecha no contamos con una definición de la IA aceptada de manera uniforme y universal. Generalmente, la IA se considera una disciplina de la informática que tiene por objetivo elaborar máquinas y sistemas que puedan desempeñar tareas que requieren una inteligencia humana. El aprendizaje automático y el aprendizaje profundo son dos esferas de la IA. En los últimos años, con el desarrollo de las nuevas técnicas y equipos informáticos basados en redes neuronales, la IA se ha venido entendiendo como un sinónimo de “aprendizaje automático profundo supervisado”¹⁰.

13. Por su lado, la Red Iberoamericana de Protección de Datos en sus Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial, referenciando a la *Royal Society* explica que “si bien no existe una única definición sobre IA, podría afirmarse que en su concepción amplia, se trata de un término “*sombrilla*” que incluye una variedad de técnicas computacionales y de procesos enfocados a mejorar la capacidad de las máquinas para realizar muchas actividades, los que comprenden desde modelos algorítmicos pasando por los sistemas de *machine learning*, hasta llegar a las técnicas de *deep learning*. Particularmente se vincula el uso de algoritmos a la IA, los cuales son un conjunto de reglas o una secuencia de operaciones lógicas que proporcionan instrucciones para que las máquinas tomen decisiones o actúen de determinada manera.”¹¹

14. El gran volumen de datos involucrados en una plataforma como Mercado Libre ofrece múltiples oportunidades para la aplicación de IA como así también desafíos. Como se comentó anteriormente, las denuncias de los titulares de Propiedad Intelectual e Industrial a través del BPP son una fuente de aprendizaje clave para las personas, que pueden también utilizarse para entrenar a los algoritmos, los cuales pueden identificar patrones y comportamientos que indiquen la existencia de irregularidades, que en el caso del presente trabajo se relacionan con la oferta de producto falsificado.

¹⁰ Inteligencia artificial y propiedad intelectual. Preguntas frecuentes sobre la Inteligencia Artificial. Organización Mundial de la Propiedad Intelectual. https://www.wipo.int/about-ip/es/artificial_intelligence/#:~:text=%C2%BFQu%C3%A9%20es%20la%20inteligencia%20artificial,que%20requieren%20una%20inteligencia%20humana.

¹¹ Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial. Red Iberoamericana de Protección de Datos. 2019. Página 6. <https://www.redipd.org/sites/default/files/2020-02/guia-recomendaciones-generales-tratamiento-datos-ia.pdf>.

15. A efectos de poder dimensionar ese volumen de datos, es importante tener en cuenta que al momento de la redacción del presente trabajo, Mercado Libre opera en 18 países de Latino América y es una plataforma utilizada por más de tres millones de vendedores en la región que generan cuarenta y cinco ventas por segundo.

16. En ese escenario, la tarea de identificar y remover ofertas de productos falsificados en Mercado Libre implica el trabajo de varios equipos conformados por personas con diferentes perfiles y disciplinas, así como también la implementación de múltiples procesos, cuya explicación en profundidad excede la extensión posible para el presente trabajo. Por ese motivo, nos enfocaremos sólo en algunos criterios y flujos principales que brinden contexto y aporten una mejor comprensión de la problemática que conlleva la implementación de IA y ML en la detección de ofertas de productos falsificados.

17. La dificultad puede girar en torno a tres situaciones principales. Por un lado, la cantidad de ofertas que son identificadas por los titulares de derechos como productos falsificados es un porcentaje ínfimo del total de publicaciones activas en los sitios de Mercado Libre. Según el último Reporte de Transparencia¹² publicado por la compañía, que informa sobre el primer semestre de 2023, sólo el 0,11% del total de publicaciones activas fueron denunciadas a través del BPP por incurrir en supuestas infracciones a derechos de Propiedad Intelectual o Industrial. Esto implica que el aprendizaje que pudiera obtenerse del análisis de esas denuncias podría aumentar con una mayor actividad de los propietarios de las marcas en el uso del BPP.

18. Por otro lado, una de las variables que puede utilizarse como un insumo adicional en los procesos de detección de productos falsificados es el precio de los artículos originales. Los precios pueden servir como un *benchmark* para complementar el análisis, ya que permiten identificar productos que tengan un precio significativamente menor al de mercado para productos idénticos y/o similares y de distintas marcas. Al menos preliminarmente, la existencia de precios excesivamente bajos en relación con *benchmarks* razonables es consistente con los precios que normalmente tienen productos falsificados. Sin embargo, aún cuando el precio puede ser un dato importante a la hora de la detección, no puede ser el único insumo que determine la falsedad de un producto. Por ejemplo, en ocasiones, descuentos y/o promociones transitorias, que los mismos titulares de derechos otorgan sobre sus productos, pueden reducir los precios y tergiversar la utilidad de este criterio. Asimismo, los propios infractores pueden adaptar su oferta, equiparando el precio de sus productos falsos con el de uno auténtico, para evadir tanto este tipo de detección como la percepción del consumidor de tratarse de productos falsificados.

19. Por último, también con la finalidad de evadir una detección, los infractores pueden adaptar otras condiciones de su oferta o la descripción de sus productos y demás informaciones que brindan en su publicación para que sus ofertas tengan la apariencia de versar sobre productos originales. Esto implica la necesidad de un constante re-entrenamiento de los sistemas que depende del aprendizaje sobre tendencias infractoras que pudiera obtenerse al analizar las denuncias de los titulares de los derechos a través del BPP.

20. La atención a estas problemáticas se intenta abordar mediante la construcción de modelos predictivos, que se constituyen en componentes de un sistema y que resultan de entrenar al algoritmo con los datos (*features*) para que devuelvan un valor que indicaría un patrón infractor en base a las tendencias aprendidas de las denuncias en BPP. El sistema de detección consiste entonces en un ensamble de modelos de clasificación basados en aprendizaje supervisado. Esos *features* se obtienen al analizar los títulos de las publicaciones,

¹² Los avances de Mercado Libre para generar un entorno digital confiable y transparente: creció la detección proactiva de publicaciones en infracción. 2023.
<https://www.mercadolibre.com.ar/institucional/comunicamos/noticias/reporte-de-transparencia-primer-semestre-2023>.

sus imágenes, las formas de referenciar a las marcas de los productos, las categorías de productos más denunciadas y el comportamiento de los vendedores, entre otras informaciones.

III. CONCLUSIONES

21. La automatización de procesos mediante IA contribuye a simplificar el análisis de grandes volúmenes de información y amplificar los resultados que se obtendrían mediante una revisión manual del contenido. En el caso de la detección de productos falsificados publicados en una plataforma de comercio electrónico como Mercado Libre, esto implica el aumento en la remoción de ofertas infractoras. Según el último Reporte de Transparencia publicado por la compañía, la implementación de esta tecnología resultó en que el 87% del total de publicaciones removidas por violaciones a derechos de Propiedad Intelectual e Industrial fuera por la acción proactiva de la plataforma, y que sólo el 13% se debiera a denuncias recibidas de parte de los titulares de esos derechos.

22. Sin embargo, los infractores constantemente sofistican sus prácticas para ofertar en línea un producto falsificado, y crean nuevas maneras para darlo a entender o para inducir a la creencia de que sus artículos son auténticos. En ese escenario, la utilización por parte de los titulares de derechos de mecanismos de denuncia de instancia privada como el BPP sigue siendo esencial para un efectivo combate a la comercialización en línea de productos falsificados.

[Fin del documento]