

Comité Asesor sobre Observancia

Decimoséptima sesión
Ginebra, 4 a 6 de febrero de 2025

HERRAMIENTAS TECNOLÓGICAS PARA COMBATIR LA PIRATERÍA DIGITAL Y LA FALSIFICACIÓN

Documentos preparados por la Oficina de Propiedad Intelectual de la Unión Europea (EUIPO) y NOS Technology

1. En la decimosexta sesión del Comité Asesor sobre Observancia (ACE), celebrada del 31 de enero al 2 de febrero de 2024, el Comité acordó examinar, en su decimoséptima 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". A ese respecto, en el presente documento se presentan las contribuciones de un Miembro no estatal (la Unión Europea) y de una entidad del sector privado (NOS Technology) sobre sus experiencias en el desarrollo y la utilización de herramientas tecnológicas para luchar contra la piratería digital y la falsificación.
2. La Unión Europea explica cómo la tecnología de cadena de bloques puede contribuir a hacer frente a los retos que plantea la lucha contra el comercio de productos falsificados, y qué infraestructura ha desarrollado la Oficina de Propiedad Intelectual de la Unión Europea (EUIPO) para la autenticación de productos y el intercambio de información sobre la cadena de suministro en apoyo de la lucha contra la falsificación.
3. A su vez, NOS Technology presenta su conjunto de instrumentos contra la piratería, una combinación de IA, aprendizaje automático, cadena de bloques y tecnologías de automatización para detectar, confirmar y responder a incidentes de piratería en tiempo real. El conjunto de instrumentos permite a los titulares de derechos emitir solicitudes de eliminación, bloquear transmisiones ilegales en *streaming* y rastrear a los infractores reincidentes, con lo que se reducen al mínimo la exposición y las pérdidas financieras.

4. Los documentos figuran en el orden siguiente:

Solución EBSI-ELSA basada en la cadena de bloques para la autenticación de productos 3

Por qué la tecnología avanzada es esencial para combatir las infracciones de la propiedad
intelectual en tiempo real..... 10

[Siguen los documentos]

SOLUCIÓN EBSI-ELSA BASADA EN LA CADENA DE BLOQUES PARA LA AUTENTICACIÓN DE PRODUCTOS

*Contribución preparada por Claire Castel, jefa de divulgación y conocimiento de la propiedad intelectual, Oficina de Propiedad Intelectual de la Unión Europea, Alicante (España).**

RESUMEN

Esta contribución presenta el reto de combatir el comercio de productos falsificados, así como la magnitud del problema y sus repercusiones negativas en la sociedad. En ella se expone cómo la tecnología de cadena de bloques puede ayudar a afrontar este reto y se describe la infraestructura que la Oficina de Propiedad Intelectual de la Unión Europea (EUIPO) ha desarrollado para la autenticación de productos y el intercambio de información sobre la cadena de suministro, con el fin de ayudar a los titulares de derechos de PI, a los intermediarios y a las administraciones competentes a hacer un seguimiento de los productos y combatir las falsificaciones. Por último, se presentan los resultados y las actividades de seguimiento previstas de la infraestructura desarrollada.

I. LUCHA CONTRA LA FALSIFICACIÓN

1. Los derechos de propiedad intelectual (PI) y su protección son fundamentales para la prosperidad económica actual y futura de la economía de la Unión Europea y para defender la creatividad, la innovación y el espíritu emprendedor de los ciudadanos y las pequeñas y medianas empresas (pymes) de toda Europa.¹ Por otro lado, las infracciones contra la PI, como la falsificación y la piratería, perjudican considerablemente el crecimiento económico de la Unión Europea, así como la seguridad de los consumidores. En un estudio conjunto realizado por la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y la EUIPO se puso de manifiesto que, en 2019, las mercancías falsificadas y pirateadas representaron el 2,5 % del comercio mundial y hasta el 5,8 % de las importaciones de la Unión Europea procedentes de terceros países.² La cantidad y variedad de productos falsificados interceptados en las fronteras de la Unión Europea ha aumentado de forma alarmante y, por consiguiente, ha incrementado la presión sobre todos los agentes implicados en la lucha contra la falsificación y la piratería, tal como se indica en un informe conjunto elaborado por la EUIPO y la Dirección General de Fiscalidad y Aduanas; publicado en noviembre de 2024, en el informe se señala que en 2023 se retuvieron alrededor de 152 millones de artículos falsificados en las fronteras y en el mercado interior de la Unión Europea.³

2. La compra de productos falsificados no siempre es un acto intencionado. Por el contrario, como se señala en diversos estudios realizados por la EUIPO, muchos consumidores compran productos falsificados sin estar seguros de si el producto que han adquirido es auténtico o no. De hecho, en 2023, el 15 % de los consumidores de la Unión Europea, lo que equivale a 68 millones de ciudadanos, compraron un producto falso pensando que se trataba de un producto

* Las opiniones expresadas en este documento son las del autor y no necesariamente las de la Secretaría o de los Estados miembros de la OMPI.

¹ Puede obtenerse más información sobre la protección de la PI en Europa en el sitio web de la EUIPO: <https://www.euipo.europa.eu/es>

² OCDE y EUIPO (2021), *Tendencias en el comercio de productos falsificados y pirateados*, disponible en: <https://euipo.europa.eu/ohimportal/es/news/-/action/view/5031024>

³ <https://www.euipo.europa.eu/en/publications/eu-enforcement-of-intellectual-property-rights-2024>

auténtico.⁴ Una proporción mucho mayor de ciudadanos de la Unión Europea (39 %) dudaba de si un producto que había comprado durante los 12 meses anteriores era auténtico o falso.⁵

3. Como se indicó en la anterior contribución de la EUIPO,⁶ los efectos negativos de la falsificación no se limitan a las pérdidas económicas, ya que también exponen a los consumidores a riesgos para la salud y la seguridad.⁷ Los productos falsificados no solo perjudican a las empresas legítimas, sino que también propician graves actividades delictivas que atentan contra la sociedad, como puso de relieve en 2024 un informe conjunto elaborado por la EUIPO y la Agencia de la Unión Europea para la Cooperación Policial (EUROPOL).⁸ Por ello, la Unión Europea debe seguir a la vanguardia de la lucha contra las falsificaciones y la EUIPO debe desempeñar un papel fundamental en la estrategia general de observancia de los derechos de PI.

4. Existen numerosas tecnologías, procedimientos y herramientas⁹ que ya contribuyen al control de las cadenas de suministro y a la lucha contra la falsificación, como los sistemas de seguimiento, la identificación por radiofrecuencia, la comunicación de campo cercano o la doble autenticación de la serialización, los controles aduaneros y el portal de la EUIPO para la observancia de la PI (IPEP).¹⁰ No obstante, esos sistemas suelen estar desarticulados, lo que aprovechan las redes delictivas.

5. Para hacer frente a los retos que plantean las amenazas delictivas a este respecto, la delincuencia contra la PI forma parte de las prioridades de la plataforma multidisciplinar europea contra las amenazas delictivas (EMPACT) para 2022-2025. Los principales agentes implicados en la lucha contra los delitos en materia de PI deben colaborar más estrechamente y adoptar nuevas estrategias para hacer frente a esos retos crecientes y llevar a cabo actividades específicas, tal como se destaca a escala de la Unión Europea en la recomendación sobre medidas para luchar contra la falsificación y mejorar la observancia de los derechos de PI,¹¹ así como en el Plan Estratégico de la EUIPO para 2030.¹²

6. Habida cuenta de los limitados recursos con que cuentan los funcionarios encargados de hacer cumplir la ley, las tecnologías como la cadena de bloques podrían ser decisivas en la lucha contra el comercio de productos falsificados. Una posible solución a esos retos es hacer uso de la tecnología de cadena de bloques, descentralizada y sincronizada, que permite crear un registro de autenticidad seguro y común. Ello debería permitir el seguimiento y rastreo de los productos auténticos a lo largo de la cadena de suministro y facultar a los agentes implicados

⁴ EUIPO (2023), *Los ciudadanos europeos y la propiedad intelectual: Percepción, concienciación y conducta*, disponible en: <https://www.euipo.europa.eu/es/publications/ip-perception-study-2023>

⁵ *Ibid.*

⁶ EUIPO (2023), nota 4.

⁷ EUIPO y OCDE (2022), *Falsificaciones peligrosas: El comercio de productos falsificados que entrañan riesgos para la salud, la seguridad y el medio ambiente*, disponible en: <https://euipo.europa.eu/ohimportal/es/web/observatory/report-on-dangerous-fakes>

⁸ EUIPO y EUROPOL (2024), *Uncovering the Ecosystem of Intellectual Property Crime: A Focus on Enablers*, disponible en: <https://www.euipo.europa.eu/es/news/joint-euipo-europol-report-exposes-far-reaching-consequences-of-ip-crime-in-europe>

⁹ La EUIPO ha creado una herramienta de vigilancia tecnológica en Internet para comparar los distintos métodos y tipos de lucha contra la falsificación disponibles en función de su finalidad, principales características técnicas y comerciales y plazos de adopción, disponible en: <https://euipo.europa.eu/anti-counterfeiting-and-anti-piracy-technology-guide/>

¹⁰ <https://euipo.europa.eu/ohimportal/es/web/observatory/ip-enforcement-portal-home-page>

¹¹ CE, C(2024)1739: *“Commission Recommendation on measures to combat counterfeiting and enhance the enforcement of intellectual property rights”*, disponible en: https://single-market-economy.ec.europa.eu/publications/commission-recommendation-measures-combat-counterfeiting-and-enhance-enforcement-intellectual_en

¹² El Plan Estratégico está disponible en: <https://www.euipo.europa.eu/es/about-us/governance/strategic-plan/sp2030>

para que centren sus esfuerzos en los productos falsos y luchar contra el fraude con mayor eficacia.

7. El objetivo es utilizar la cadena de bloques en una infraestructura de autenticación, en la que cualquier parte interesada (fabricantes, consumidores, servicios de transporte, etc.) pueda comprobar fácilmente la autenticidad de un producto y alertar a los titulares de derechos cuando se detecte un producto fraudulento.

8. Desde 2018, la EUIPO ha encabezado la aplicación de este tipo de tecnologías para hacer frente al comercio de falsificaciones mediante el proyecto Blockathon.¹³ El proyecto surgió tras un concurso de tipo *hackathon* para comprobar la viabilidad de la idea. Posteriormente, se constituyó un foro de partes interesadas y se creó una plataforma de autenticación mediante cadena de bloques, que se publicó en 2024.¹⁴

II. PROYECTO DE INFRAESTRUCTURA BLOCKATHON CONTRA LA FALSIFICACIÓN

A. HISTORIA DEL PROYECTO

9. Desde una serie de talleres en 2017 hasta un Blockathon de 48 horas en 2018,¹⁵ la EUIPO ha llevado a cabo diversas actividades en los últimos cuatro años para estudiar las ventajas que ofrece la tecnología de cadena de bloques para la observancia de los derechos de PI. En 2019 y 2020, la EUIPO mantuvo una serie de reuniones con el ganador del Blockathon de 2018 y creó el foro Blockathon¹⁶ para definir los casos prácticos¹⁷ y llevar a cabo un estudio piloto, que demostró la viabilidad de la idea y condujo al desarrollo de una infraestructura contra la falsificación¹⁸ para impulsar la iniciativa. Posteriormente, en 2023 se presentó un proyecto piloto con cuatro titulares de derechos de PI, dos operadores de transporte y logística y las autoridades aduaneras neerlandesas.¹⁹ El nombre de EBSI-ELSA ha cambiado a *AUTHENTIC view*, junto con el lema “Transparencia en la cadena de suministro”.

B. INFRAESTRUCTURA DEL PROYECTO

10. En junio de 2024 se publicó la estructura, que incluye las siguientes herramientas descargables y servicios temporales:

¹³ El resumen del proyecto hasta 2022 puede consultarse en EUIPO (2019), “Nuevas oportunidades tecnológicas para la protección y observancia de los derechos de propiedad intelectual: Blockathon, la lucha contra la falsificación mediante la tecnología de cadena de bloques” (páginas 8 a 11 del documento WIPO/ACE/14/6), disponible en: https://www.wipo.int/edocs/mdocs/enforcement/es/wipo_ace_14/wipo_ace_14_6.pdf#page=8, y EUIPO (2022), “Nuevas oportunidades tecnológicas para la protección y observancia de los derechos de propiedad intelectual: Actualización sobre la lucha contra la falsificación mediante la tecnología de la cadena de bloques” (páginas X a Y del documento WIPO/ACE/15/10, disponible en: https://www.wipo.int/meetings/es/doc_details.jsp?doc_id=580571). La presente contribución actualiza los informes de la EUIPO de 2019 y 2022.

¹⁴ Toda la infraestructura de la EUIPO está disponible en:

<https://www.euipo.europa.eu/es/observatory/enforcement/blockathon>

¹⁵ <https://euipo.europa.eu/ohimportal/es/web/observatory/blockathon-2018>

¹⁶ <https://euipo.europa.eu/ohimportal/es/web/observatory/blockathon>

¹⁷ https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Blockathon/Blockathon-Forum_Blockchain-Use-Case.pdf

¹⁸ https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/contentPdfs/Strategic_Plan_2025/project_cards/SD1_Anti-counterfeiting_Blockathon_Infrastructure_PC_en.pdf

¹⁹ Los resultados del proyecto pueden consultarse en: <https://www.euipo.europa.eu/de/news/observatory/euipo-unveils-ebsi-elsa-a-ground-breaking-step-in-global-supply-chain-product-authentication>

- a) Un servicio manual de emisión de credenciales de marca: una firma digital que proporciona a los representantes de los activos de PI credenciales de su marca registradas en una cadena de bloques, verificables en cualquier momento por terceros. Este servicio fue sustituido posteriormente por una herramienta automática internacional (un monedero electrónico) integrada en el Registro de PI de la EUIPO, en una cadena de bloques.²⁰
- b) El módulo de autenticación, un generador de etiquetas digitales que contiene la información del producto y las credenciales de marca registradas basadas en la cadena de bloques, el cual permite a los representantes de los activos de PI vincular la información de su marca, producto y empresa en un único documento autoverificable que puede vincularse a los productos físicos.
- c) El visualizador de objetos digitales no fungibles (NFT): una herramienta de lectura de la serialización que verifica automáticamente la información contenida en las etiquetas digitales producidas con el módulo de autenticación, lo que permite comprobar la autenticidad de un producto a cualquier persona que lo posea.
- d) El módulo logístico: una red entre pares que permite a las partes de la cadena de suministro compartir información digital para hacer un seguimiento de los envíos y los productos desde el lugar de fabricación hasta el destino final. Ello permite que los responsables del control fronterizo de la Unión Europea hagan una mejor evaluación de los envíos y agilicen su despacho.

²⁰

<https://euipo.europa.eu/ohimportal/es/news/-/action/view/8662923>



C. APLICACIONES DE LA INFRAESTRUCTURA

11. El registro en la cadena de bloques consiste en un objeto único e inmutable. A medida que los bienes pasan de manos de una parte a otra, estas intercambian el objeto por medio de monederos digitales. La combinación de una identidad única para cada producto y la

transferencia continua de la identidad digital entre los monederos genera una prueba de la autenticidad de los productos. A lo largo del trayecto del producto, las autoridades aduaneras y otras autoridades encargadas del cumplimiento de la ley pueden acceder a información, como los registros de envío auténticos, que puede servir de apoyo a la evaluación de riesgos.

12. Desde la perspectiva del transportista, la información de envío se almacena en la cadena de bloques. Si bien la solución se centra en el nivel de producto, un contenedor también puede ser digitalizado y vinculado mediante algoritmos a las mercancías que contiene. Esto evita la necesidad de abrir un contenedor sellado para comprobar la autenticidad de las mercancías que contiene cada vez que se transfiere entre las partes de la cadena de suministro. Además, las mercancías digitalizadas cuya autenticidad esté probada podrían pasar con rapidez los controles aduaneros.

13. Desde la perspectiva de la observancia, la cadena de bloques puede generar alertas de manera automática sobre la integridad de los productos si se detecta alguna anomalía cuando cambian de manos en la cadena de suministro. Las aplicaciones autorizadas pueden supervisar esas incidencias y enviar notificaciones a los titulares de los derechos y a las autoridades encargadas de hacer cumplir la ley. Opcionalmente, la cadena de bloques puede registrar las actuaciones realizadas por las aduanas para mantener a las partes informadas del estado de un envío.

14. Desde el punto de vista del usuario final, la solución ofrece la posibilidad de mejorar la información contenida en la cadena de bloques, añadiendo registros de forma manual o automática a través de sensores. Para un minorista o un consumidor, esto significa que se pueden aprovechar esos registros para obtener información, como el establecimiento de producción, los movimientos de la cadena de suministro y la procedencia de las materias primas.

15. Por último, esta infraestructura, mediante el uso de interfaces de programación de aplicaciones (API) adicionales o datos definidos, ofrecerá las siguientes funciones complementarias:

- a) Mediante el uso de datos definidos en el gemelo digital (versión digital del artículo físico) y la creación de alertas específicas en sus sistemas, los titulares de derechos también podrían aprovechar la infraestructura para crear servicios adicionales, como la retirada o la desviación de productos del mercado (por ejemplo, cuando los productos farmacéuticos han caducado o se reenvían a países con mayor demanda).
- b) Los titulares de derechos y los consumidores podrían beneficiarse de posibilidades adicionales de negocio a consumidor en el ámbito de la compra posventa de subcomponentes de productos, o el uso del certificado de autenticidad para la reventa en el mercado secundario. Dado que el titular del derecho define qué tipo de datos se incluyen en el gemelo digital, también podría dar lugar a un programa de fidelización específico basado en las características del producto.
- c) Como parte de una solución más amplia integrada en la infraestructura europea de servicios de cadena de bloques,²¹ los consumidores podrían beneficiarse de un monedero único a nivel de la Unión Europea capaz de almacenar todos sus NFT y otros certificados digitales en una única ubicación.

²¹ <https://ec.europa.eu/digital-building-blocks/wikis/display/ebsi>

III. CONCLUSIÓN

16. En el último trimestre de 2024 se introdujeron mejoras en el sistema, en el marco de proyectos específicos, junto con dos marcas, un operador logístico y dos autoridades aduaneras, a fin de probar la idoneidad de la infraestructura en un entorno real.

17. La infraestructura utilizará una versión de producción de la infraestructura europea de servicios basados en cadenas de bloques (EBSI),²² gestionada por EUROPEUM, un consorcio europeo de infraestructuras digitales²³ creado en mayo de 2024 por diez Estados miembros de la Unión Europea. La emisión de estas credenciales verificables está vinculada al Registro de PI de la EUIPO en la cadena de bloques. La infraestructura también se verá afectada por los próximos reglamentos de la Unión Europea y proyectos internacionales, como:

- a) Identidad digital para personas jurídicas y físicas en el marco de la revisión del Reglamento Europeo de Identidad Digital 2.0,²⁴ ya que el proyecto identifica a los titulares de derechos de PI mediante credenciales digitales verificables basadas en una cadena de bloques;
- b) El futuro reglamento por el que se establece el Código Aduanero de la Unión y la Autoridad Aduanera de la Unión Europea,²⁵ ya que el proyecto facilita el intercambio de información sobre la cadena logística y de suministro entre los titulares de derechos de PI, los intermediarios y las autoridades aduaneras;
- c) Pasaporte digital de productos, ya que el proyecto proporciona información adicional sobre la identificación del proyecto;²⁶
- d) El proyecto de identificador mundial de la OMPI podría servir en el futuro para la emisión de credenciales verificables de titulares de marcas a escala mundial y de manera eficaz;
- e) La estructura de datos del Protocolo de Transparencia de la Comisión Económica de las Naciones Unidas para Europa (CEPE), ya que pueden establecerse colaboraciones y sinergias en relación con el intercambio de información y la lucha contra la falsificación.²⁷

18. En 2025 se presentará la infraestructura junto con los resultados de los proyectos piloto y, tras el anuncio de una nueva imagen de marca, se fomentará su adopción por parte de los titulares de derechos de PI, los operadores de transporte y logística y las autoridades aduaneras, con el apoyo de la EUIPO.

[Fin de la contribución]

²² Toda la información sobre EUROPEUM, incluidos los estatutos y la información más reciente, está disponible en: <https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/The+EUROPEUM-EDICs+latest+updates>

²³ La normativa de base está disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=OJ:L_202401432

²⁴ Reglamento 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, versión consolidada de 2024 disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A02014R0910-20241018>

²⁵ Reglamento 2023/0156 por el que se derogan los Reglamentos 2013/952 y 2012/007. Primera lectura en el Consejo. Procedimiento y texto disponibles en: [https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2023/0156\(COD\)&l=en](https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2023/0156(COD)&l=en)

²⁶ Reglamento 2024/1781 por el que se instaure un marco para el establecimiento de requisitos de diseño ecológico aplicables a los productos sostenibles, disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32024R1781>

²⁷ La información sobre el protocolo figura en: <https://uncefact.github.io/spec-unt/>

POR QUÉ LA TECNOLOGÍA AVANZADA ES ESENCIAL PARA COMBATIR LAS INFRACCIONES DE LA PROPIEDAD INTELECTUAL EN TIEMPO REAL

*Contribución preparada por el Sr. Pedro Bravo, jefe de Protección de Contenidos, NOS Technology, Lisboa (Portugal)**

RESUMEN

En la era digital, es vital que los titulares de derechos se protejan contra los métodos modernos de piratería. La piratería es un problema mundial y complejo, y el contenido no autorizado puede aparecer en plataformas de transmisión en continuo (*streaming*), redes de *torrents* y foros de la web oscura a los pocos segundos de su publicación. El crecimiento de Internet y el rápido avance de la tecnología han propiciado que sea más fácil hacer copias de obras protegidas, que a menudo son indistinguibles de los originales, y difundirlas rápidamente, dando así lugar a costosas infracciones y daños irreparables para los titulares de derechos. El conjunto de instrumentos contra la piratería creado por NOS Technology aprovecha la inteligencia artificial (IA), la IA generativa, el aprendizaje automático, la cadena de bloques y la automatización para detectar y confirmar incidentes de piratería en tiempo real y actuar en consonancia, lo que permite a los titulares de derechos identificar y eliminar infracciones en todas las jurisdicciones y garantizar la protección incluso en casos en que los regímenes de observancia no son sólidos. La función automatizada de observancia puede emitir solicitudes de eliminación, bloquear transmisiones ilegales en *streaming* y rastrear a los infractores reincidentes, de manera que se reducen al mínimo la exposición y las pérdidas económicas. Estos recursos son fundamentales para asegurar el futuro de la innovación, la creatividad y la competencia leal en la economía digital.

I. INTRODUCCIÓN

1. En la era digital actual, la propiedad intelectual (PI) es uno de los activos más valiosos para las empresas, los creadores y las organizaciones. La PI impulsa sectores y fomenta la innovación, desde películas, programas de televisión y música hasta publicaciones, juegos, programas informáticos y acontecimientos deportivos en vivo. Sin embargo, ese valor también convierte a la PI en un objetivo prioritario para la piratería, lo que cuesta a las empresas miles de millones en pérdidas de ingresos anualmente y erosiona la confianza de los consumidores. El acceso a Internet ha propiciado que sea más fácil hacer copias de obras protegidas, que a menudo son indistinguibles de los originales, y difundirlas rápidamente, dando así lugar a costosas infracciones.

II. EL RETO

2. Los métodos tradicionales para detectar y combatir la piratería ya no son suficientes. El alcance, la velocidad y la complejidad de la piratería actual han superado la vigilancia y la observancia que se efectúan mediante métodos convencionales. Los piratas ahora operan en redes mundiales, utilizando plataformas cifradas, sistemas descentralizados y tecnologías emergentes para sortear la detección.

* Las opiniones expresadas en este documento son las del autor y no necesariamente las de la Secretaría o los Estados miembros de la OMPI.

3. La PI es la columna vertebral de la innovación, la creatividad y el crecimiento de las industrias en un mundo cada vez más digital. Los activos de PI pueden generar miles de millones de dólares en valor, desde películas y música hasta programas informáticos y emisiones en directo. Sin embargo, ese auge digital también ha hecho que los activos de PI sean más vulnerables que nunca a la explotación ilegal.

4. La piratería moderna es una actividad compleja y mundial. El contenido no autorizado puede aparecer en plataformas de transmisión en continuo, redes de *torrents* y foros de la web oscura a los pocos segundos de su publicación. Cabe pensar que los métodos clásicos de observancia de los derechos de PI no sean eficaces frente a los niveles de velocidad, alcance y complejidad de los métodos de piratería modernos. Sin una intervención en tiempo real, el contenido pirateado puede propagarse por todo el mundo en cuestión de segundos y causar daños irreparables. Esos daños pueden adoptar muchas formas. Por ejemplo, la piratería digital cuesta a las empresas más de 50 000 millones de dólares de los Estados Unidos al año,²⁸ lo que reduce drásticamente los ingresos y socava la rentabilidad. Cada infracción es un duro golpe para quienes trabajan incansablemente en la creación de contenidos valiosos, y desalienta la innovación y la creatividad. La piratería también diluye la reputación de la marca, al crear experiencias negativas para los consumidores que acceden a versiones de productos falsificados o de baja calidad. Por tanto, es fundamental utilizar tecnología en tiempo real para combatir las infracciones de la PI.

III. LA SOLUCIÓN

5. En este punto es donde entran en juego los recursos de vanguardia, como el conjunto de instrumentos contra la piratería creado por NOS Technology, en colaboración con un asociado tecnológico de confianza. Estas soluciones aprovechan la IA, la IA generativa, el aprendizaje automático, la cadena de bloques y la automatización para detectar y confirmar incidentes de piratería en tiempo real y actuar en consonancia, lo que permite proteger a la PI en todo momento.

A. CONJUNTO DE INSTRUMENTOS CONTRA LA PIRATERÍA DE NOS TECHNOLOGY: FUNCIONAMIENTO

6. Se trata de una combinación de tecnología e inteligencia de código abierto recopilada por agentes automatizados. Detecta casos en tiempo real y con alta precisión (más del 99 %) y proporciona todos los detalles de la red en un gráfico,²⁹ para lo que utiliza:

- a) Rastreo web inteligente: con la capacidad de reforzar el aprendizaje para que el rastreo sea eficiente.
- b) Reconocimiento de imágenes y videos: se detectan logotipos, marcas de agua, marcadores y publicidad (anuncios) para confirmar y puntuar la infracción.

²⁸ En un informe de 2019 del Centro Mundial de Políticas de Innovación de la Cámara de Comercio de los Estados Unidos y NERA Economic Consulting, titulado *"Impacts of Digital Piracy on the U.S. Economy"*, se ponen de relieve pérdidas económicas notables como resultado de la piratería de videos digitales, cuyas estimaciones oscilan entre los 29 200 y los 71 000 millones de dólares al año solo para la economía de los Estados Unidos. A nivel mundial, las pérdidas en las industrias del cine y la televisión a causa de la piratería digital oscilan entre los 40 000 y los 97 000 millones de dólares al año, según las hipótesis sobre las tasas de sustitución. Véase <https://www.uschamber.com/technology/data-privacy/impacts-of-digital-piracy-on-the-u-s-economy>.

²⁹ La tecnología NOS emplea un programa informático de bases de datos orientadas a grafos que ayuda a inventariar redes piratas mediante datos recopilados a través de análisis e investigaciones en la web, herramientas de código abierto, redes sociales, pruebas de compra, etc.

- c) Procesamiento del lenguaje natural: identificación de contexto, los servicios, los canales y la tecnología, lo que permite “emular” a un analista humano y mejorar así los resultados con menor inversión (tiempo, recursos y costo).
- d) Puntuación de detección de piratería: a partir de un enfoque híbrido con modelos de aprendizaje automático supervisados y no supervisados.
- e) Aprendizaje activo: en relación con la clasificación de casos para un aprendizaje continuo.

B. BENEFICIOS DE LA DETECCIÓN EN TIEMPO REAL

7. La detección de la piratería en tiempo real puede ofrecer varios beneficios a los titulares de derechos.

- a) Reducción al mínimo de las pérdidas de ingresos y la exposición: la detección en tiempo real garantiza que la transmisión en continuo, la descarga y distribución no autorizadas sean interceptadas antes de que incidan significativamente en los ingresos, lo que permite a las organizaciones identificar y detener las infracciones a medida que ocurren y reducir al mínimo la exposición y las pérdidas financieras.
- b) Proteger la integridad de la marca: una detección y eliminación rápidas refuerzan el compromiso de la marca con la calidad y la exclusividad.
- c) Eficiencia operativa mejorada: las soluciones automatizadas reducen la dependencia de las intervenciones manuales, lo que permite a las empresas centrarse en la innovación en lugar de lidiar constantemente con las amenazas de la piratería.
- d) Cumplimiento y precisión: muchos sectores lidian con estrictas leyes de protección de la PI. Este instrumento permite cumplir plenamente los requisitos vigentes al documentar las infracciones y facilitar acciones legales rápidas. Emplea algoritmos avanzados para distinguir entre contenido legítimo y pirateado, lo que reduce los falsos positivos y garantiza una observancia precisa.
- e) Alcance mundial y cobertura integral: el instrumento vigila ecosistemas digitales abiertos y ocultos, incluidos servicios de transmisión por *streaming* (de pago, gratuitos o compartidos), plataformas sociales, grupos de mensajería (Telegram, WhatsApp), redes entre particulares (P2P) y la web oscura. Opera en jurisdicciones de todo el mundo, inclusión hecha de regiones difíciles de vigilar y la web oscura, lo que garantiza la protección en regiones donde la observancia del derecho de autor suele ser deficiente.
- f) Observancia automatizada: el instrumento emite solicitudes de eliminación, bloquea transmisiones ilegales por *streaming*³⁰ y rastrea a los infractores reincidentes, lo que ahorra tiempo y recursos.
- g) Escalabilidad y proactividad: el instrumento es capaz de vigilar miles de plataformas, redes y usuarios simultáneamente. El análisis predictivo garantiza que se pueda prevenir la piratería antes de que se produzca.

³⁰ Los procedimientos administrativos y jurídicos vigentes en Portugal permiten a los titulares de derechos de PI solicitar eliminaciones en tiempo real o de forma permanente por dominio o por IP. El instrumento contra la piratería detecta, valida y envía una solicitud a una puerta de enlace de bloqueo que se conecta mediante API al proveedor de servicios de Internet.

C. REPERCUSIÓN EN EL MUNDO REAL

8. Las empresas o los organismos encargados del cumplimiento de la ley que investigan delitos contra la PI e invierten en tecnología antipiratería han obtenido resultados mensurables:

- a) Una reducción significativa de las pérdidas de ingresos debidas a la piratería.
- b) Mejores resultados en materia de observancia, al eliminarse el contenido pirateado de forma más rápida y eficaz.
- c) Relaciones fortalecidas con las partes interesadas, incluidos los creadores de contenido y los asociados del ámbito de la distribución.
- d) Resultados mejorados y pruebas fehacientes con más claridad, un alcance más amplio y plazos reducidos.

D. EL VALOR DE LA OBSERVANCIA DE LOS DERECHOS DE PI EN TIEMPO REAL

- a) Protección de las fuentes de ingresos: cada transmisión o descarga pirateada representa una pérdida de ingresos. La tecnología en tiempo real ayuda a mantener el valor al detener rápidamente las infracciones.
- b) Protege la labor creativa: los creadores y las empresas pueden centrarse en la innovación en lugar de luchar contra la piratería, lo que garantiza un crecimiento sostenido y la confianza de los consumidores.
- c) Promueve la competencia leal: velar por la observancia de los derechos de PI con prontitud garantiza que los actores legítimos del mercado sean recompensados por su trabajo, lo que fomenta una economía digital más sana y equitativa.
- d) Aumenta la confianza del consumidor: las empresas fortalecen las relaciones con sus audiencias y consumidores al garantizar que solo esté disponible contenido autorizado y de alta calidad.

IV. CONCLUSIÓN

9. Los instrumentos contra la piratería en tiempo real son el futuro de la observancia de los derechos de PI. Pueden proteger el futuro de la innovación y la creatividad, al permitir que las empresas aseguren sus activos, que los creadores conserven el control de su trabajo y que los consumidores disfruten del contenido según lo previsto. Utilizar la tecnología adecuada hoy garantizará un futuro sostenible, justo e innovador para todos. En un mundo donde los segundos cuentan, la detección y confirmación en tiempo real de las infracciones de los derechos de PI empoderan a las empresas, al permitirles recuperar el control de su contenido, reputación y flujos de ingresos.

[Fin del documento]