



WIPO/ACE/15/8
ORIGINAL: INGLÉS
FECHA: 3 DE AGOSTO DE 2022

Comité Asesor sobre Observancia

Decimoquinta sesión
Ginebra, 31 de agosto a 2 de septiembre, 2022

EL PAPEL DE LOS INTERMEDIARIOS EN LA OBSERVANCIA DE LA PI

Contribuciones preparadas por el Reino Unido, la European Brands Association (AIM), la Federación Internacional de la Industria Fonográfica, DHL Express y Mastercard

1. En su decimocuarta sesión, celebrada del 2 al 4 de septiembre de 2019, el Comité Asesor sobre Observancia (ACE) acordó que en su decimoquinta sesión se examinaría, 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 ese sentido, en el presente documento se exponen las contribuciones de un Estado miembro (el Reino Unido), dos observadores (la *European Brands Association* –AIM– y la Federación Internacional de la Industria Fonográfica –IFPI–) y dos entidades privadas (DHL Express y Mastercard).
2. La contribución del Reino Unido ofrece un panorama general de la campaña *Real Deal Campaign for Fake-Free Markets*, una iniciativa nacional para combatir la venta de productos falsificados y pirata, cuyo éxito radica en alianzas intersectoriales integradas por organizaciones británicas clave, tanto privadas como públicas, que aspiran a reducir el comercio de mercancías infractoras.

3. Las contribuciones de la AIM y la IFPI analizan el papel esencial que desempeñan los distintos tipos de intermediarios en la lucha contra la piratería y la falsificación en Internet y recomiendan la adopción de varias medidas a tal efecto. En concreto, las contribuciones alientan a los intermediarios, a adoptar diligencia debida a la hora de establecer una relación comercial con clientes, a tomar medidas de “notificación y retirada definitiva”, a poner en marcha políticas en contra de los infractores reincidentes, así como a colaborar de forma proactiva con los titulares de los derechos y las autoridades encargadas del cumplimiento de la ley. Asimismo, se identifican tanto ejemplos concretos de acciones que los intermediarios pueden llevar a cabo para poner en práctica esas medidas, así como áreas en los que podrían fortalecerse o complementarse las medidas vigentes.

4. Las contribuciones de DHL Express y Mastercard enriquecen este documento al aportar las perspectivas de otros intermediarios en la lucha contra las infracciones de la PI. En ambas contribuciones se analizan las iniciativas que actualmente los intermediarios, tanto físicos como digitales, han puesto en marcha para combatir las infracciones de la PI. Entre las iniciativas cabe destacar el fomento de la sensibilización del público respecto a las infracciones de la PI, la adopción de medidas proactivas para frenar el comercio de mercancías infractoras de la PI y la colaboración activa con los titulares de los derechos y las autoridades públicas. Tanto DHL Express como Mastercard han adoptado políticas y emprendido diversas acciones encaminadas a la lucha activa contra las infracciones de la PI, tanto en el ámbito digital como en el entorno material.

5. Las contribuciones se presentan en el siguiente orden:

“Real Deal” (La verdad de las cosas): Un enfoque colaborativo para hacer frente a los delitos contra la propiedad intelectual en los mercados en el Reino Unido	3
La perspectiva de la AIM (<i>European Brands Association</i>) acerca del papel de los intermediarios en línea en la lucha contra la falsificación	8
La perspectiva de la industria de las grabaciones musicales acerca del papel de los intermediarios en línea en la lucha contra la piratería.....	14
El cumplimiento de la normativa aduanera en la industria del transporte urgente: el enfoque de DHL Express	21
Iniciativas de Mastercard para prevenir las infracciones de la propiedad intelectual.....	28

[Siguen las contribuciones]

“REAL DEAL” (LA VERDAD DE LAS COSAS): UN ENFOQUE COLABORATIVO PARA HACER FRENTE EN EL REINO UNIDO A LOS DELITOS CONTRA LA PROPIEDAD INTELECTUAL EN LOS MERCADOS

*Contribución preparada por la Sra. Patricia Lennon, directora de campaña, Real Deal Campaign for Fake-free Markets, National Markets Group for Intellectual Property Protection, Londres (Reino Unido)**

RESUMEN

En el presente documento se proporciona un resumen de la campaña *Real Deal*, emprendida en 2009 como iniciativa nacional para hacer frente a la venta de productos falsificados y pirata en los mercados del Reino Unido. El éxito de la iniciativa, financiada por la industria, radica en las alianzas intersectoriales que involucran a todas las organizaciones clave en el Reino Unido (tanto en el sector público como privado) centradas en reducir el comercio de productos falsificados en los mercados. La base de la iniciativa es su Carta voluntaria, mediante la cual los operadores del mercado se comprometen públicamente a mantener sus mercados exentos de productos falsificados. Hasta la fecha, más de 500 mercados en el Reino Unido se han adherido a este compromiso. Como consecuencia del éxito del programa *Real Deal* en los mercados físicos, se reprodujo el modelo básico en 2018 para hacer frente a la venta de productos falsificados en línea y en los grupos de venta en las redes sociales.

I. INTRODUCCIÓN

1. La campaña *Real Deal* para mercados sin venta de productos falsificados¹ es una iniciativa de sensibilización y educación, lanzada en 2009 por el *National Markets Group for Intellectual Property Protection* (NMG) en el Reino Unido, que complementa la labor de observancia del NMG basada en la información. Esta combinación de observancia selectiva y programa de prevención constituye una estrategia de 360 grados para hacer frente a la venta de productos que infringen la propiedad intelectual (PI), entre ellos, los productos falsificados, los productos pirateados o los productos que infringen los derechos sobre diseños registrados, tanto en los mercados físicos del Reino Unido como, más recientemente, en línea y a través de grupos de venta en las redes sociales. En esta presentación se analizará en detalle el programa *Real Deal* y la forma en que ha evolucionado a lo largo de los últimos 13 años.

II. UN ENFOQUE COLABORATIVO FINANCIADO POR LA INDUSTRIA

2. La clave del éxito de la iniciativa *Real Deal* es la colaboración de una amplia gama de partes interesadas. En primer lugar, la iniciativa sólo es posible gracias al compromiso financiero de la industria: su contribución total al proyecto, hasta la fecha, rebasa las 500.000 libras esterlinas, además de la financiación proporcionada por la Oficina de Propiedad Intelectual de la Unión Europea (EUIPO) desde 2015 hasta 2016. Los patrocinadores actuales del proyecto abarcan un amplio espectro de sectores afectados por las infracciones de PI, entre ellos: el organismo *British Phonographic Industry*, *Palmer Biggs IP Solicitors* (estudio de abogados de PI Palmer Biggs), la

* 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.

¹ Más información en www.realdealmarkets.co.uk.

Premier League, Procter & Gamble, React, Superdry, Surelock, el Grupo WRI y otras marcas asociadas que integran el Grupo de Lucha contra la Falsificación. Gracias a su apoyo financiero, la campaña ha podido mantenerse y es sostenible de cara al futuro.

3. Asimismo, el programa es refrendado por todas las partes interesadas clave que desean garantizar un comercio sin productos falsificados, a saber, el *Chartered Trading Standards Institute* (CTSI), *Trading Standards Scotland*, el *National Trading Standards e-Crime Team* (NTSeCT) y la Oficina de Propiedad Intelectual del Reino Unido. El programa es referido como ejemplo de mejores prácticas por Ministros competentes en materia de PI del Reino Unido, la EUIPO y organizaciones que representan los intereses de titulares de derechos de PI, así como la *National Association of British Market Authorities* (NABMA) y la *National Market Traders' Federation*.

III. ¿CÓMO FUNCIONA LA INICIATIVA REAL DEAL?

4. La iniciativa Real Deal proporciona a las autoridades del Reino Unido un mecanismo voluntario, autorregulador y local para hacer frente al problema de los productos falsificados que se venden en los mercados locales. La clave de su éxito radica en que se centra en promover una colaboración más estrecha entre las personas o las organizaciones encargadas de los mercados y las autoridades locales pertinentes encargadas de fijar las normas en materia de comercio. El servicio encargado de fijar las normas en materia de comercio es quien supervisa del mercado y le incumbe también la defensa del consumidor y la inspección de los mercados en el Reino Unido. El objetivo de la iniciativa es aumentar la toma de conciencia entre los organizadores de los mercados sobre sus responsabilidades de garantizar que en sus mercados no se vendan productos falsificados y proporcionarles información práctica, recursos, directrices y contactos para ayudarlos a ello.

IV. MERCADOS FÍSICOS Y RASTRILLOS

5. La iniciativa se desarrolló inicialmente como respuesta directa al creciente problema de las infracciones de PI, la falsificación y la piratería en los mercados físicos y rastrillos. La base del proyecto es la "Carta Real Deal"², firmada tanto por los operadores de los mercados como por los servicios locales encargados de fijar las normas en materia de comercio para confirmar el compromiso conjunto de colaborar para velar por un comercio sin productos falsificados. En la Carta se hace hincapié en un código de prácticas pormenorizado en el que se establecen procedimientos que los operadores de los mercados deben aplicar y a los que deben ceñirse a fin de poder exhibir el logotipo de *Real Deal*.

² Encontrará más información sobre los contenidos de la *Real Deal Charter* y el código de prácticas en <http://www.realdealmarkets.co.uk/resources/>.

6. A través de *Real Deal* se proporciona a los mercados una serie de recursos prácticos, incluido el folleto informativo para comerciantes *How to Stay IP Legal*, afiches y el logotipo de *Real Deal*. El enfoque de *Real Deal* y la importancia de la protección de las marcas y de los derechos de autor también se incluyen como uno de los módulos de aprendizaje clave en el Diploma en Administración de Mercados de la NABMA. Para los funcionarios encargados de la observancia existe otro recurso informativo – *Practical Guide to IP Protection at Markets and Car Boot Fairs* – que es un compendio detallado de estudios de casos, enfoques jurídicos, mejores prácticas y modelos de documentos.



7. La aceptación de la Carta de *Real Deal* ha aumentado año tras año desde su lanzamiento en 2009, y actualmente el programa es utilizado por las autoridades locales de todo el Reino Unido. Más de 500 mercados se han adherido a la Carta y con ello se beneficia a miles de comerciantes y se protege a cientos de miles de compradores.

V. REAL DEAL EN LÍNEA

8. En 2018, *Real Deal* lanzó un programa paralelo, *Real Deal Online*, dirigido a los mercados digitales, en particular al creciente comercio de productos que infringen los derechos de PI en grupos de compra y venta en las redes sociales. La nueva iniciativa en línea, ideada por el NMG y el NTSeCT, es una extensión natural de la campaña *Real Deal*, dado que el modelo – conocido y aplicado en mercados físicos – es sumamente transferible al ámbito en línea y de las redes sociales. La atención se centra en lo mismo:

- sensibilizar a los operadores de los mercados o los administradores de los grupos de venta en las redes sociales de su responsabilidad profesional y obligaciones en virtud de la legislación sobre PI;
- facilitar la interacción de los operadores de los mercados/los administradores de los grupos de venta y sus servicios locales encargados de fijar las normas en materia de comercio; y
- alentar a los operadores de los mercados/los administradores de los grupos de venta a acordar un código de prácticas y a exhibirlo como mensaje para los compradores, vendedores y visitantes.

9. El código de comportamiento de *Real Deal Online* requiere que los administradores de grupos acepten como miembros a los funcionarios de la autoridad local encargada de fijar las normas en materia de comercio y accedan aplicar cinco medidas sencillas:

- prohibir la venta de productos que infringen derechos de PI y otros productos ilícitos;³
- tomar medidas sobre la base de la información que reciban de titulares de derechos de PI y sus representantes en cuanto a la venta de productos ilegales;

³ Entre los que se cuentan los productos grises ilegales, productos robados, productos supuestamente robados, mercancías peligrosas, productos de tabaco (no despachados en aduana), productos alcohólicos (sin licencia), fuegos de artificio (vendidos de forma distinta a la establecida en el código y la normativa), armas ofensivas y artículos de carácter pornográfico.

- notificar a las autoridades encargadas de fijar las normas en materia de comercio si los administradores de grupos creen que se venden productos ilegales en el grupo y excluir a los vendedores de esos productos;
- difundir las advertencias y los avisos publicados por las autoridades encargadas de fijar las normas en materia de comercio, y
- asegurarse de que todos los miembros del grupo estén al tanto de su política de prohibición de productos falsificados.

10. En el lanzamiento del programa *Real Deal Online* en septiembre de 2018, el Ministro de Propiedad Intelectual, Sam Gyimah, reconoció su valor y señaló: *“El Reino Unido es rico en creadores e innovadores talentosos y debemos proteger sus derechos de propiedad intelectual tanto en Internet como en otros ámbitos. Las redes sociales pueden ser una fuerza positiva y facilitar a los usuarios la compra y venta de productos. Sin embargo, esto puede traer aparejado un aumento en el número de productos falsificados y otros productos ilegales. Por este motivo acojo con satisfacción esta iniciativa que reúne al sector, las autoridades encargadas de fijar las normas en materia de comercio y el gobierno local para ayudar a proteger a los negocios legítimos y permitir que los titulares de derechos aprovechen los beneficios de sus propias creaciones”*.

11. Se ha elaborado una Guía práctica sobre *Real Deal* para funcionarios encargados de hacer cumplir la Ley, y han contribuido a su elaboración el NMG, el NTSeCT y funcionarios encargados de coordinar la labor de observancia de la PI del CTSI. Dicha guía contiene un paquete de orientaciones y recursos listos para usar a fin de ayudar a los servicios encargados de fijar las normas en materia de comercio a hacer frente al comercio de productos que infringen la PI en grupos de las redes sociales de su zona. Asimismo, se está poniendo en práctica un programa complementario de capacitación y actividades de difusión de conocimientos, que cuenta con apoyo del *National Tasking Group*, perteneciente a *National Trading*, y con financiación de los asociados sectoriales del proyecto *Real Deal*.

12. Desde el lanzamiento de la guía práctica, más de 100 servicios locales encargados de fijar normas en materia de comercio la han solicitado y más de 200 funcionarios han participado en el programa de capacitación, lo cual demuestra la demanda de aprendizaje y asistencia práctica de los funcionarios encargados de velar por las normas en materia de comercio para hacer frente a este creciente problema.

13. Los servicios encargados de fijar las normas en materia de comercio en todo el país han comenzado a aplicar el programa a escala local dirigido a cientos de grupos de administradores y han alcanzado a cientos de miles de usuarios de grupos de venta en las redes sociales. A medida que más servicios de normas comerciales adopten el programa, el mensaje de *Real Deal* se extenderá exponencialmente, y cada vez más grupos de compra-venta se convertirán en espacios libres de falsificaciones.

VI. RESULTADOS POSITIVOS PARA UNA SERIE DE PARTES INTERESADAS

14. En los mercados físicos y digitales, el programa *Real Deal* brinda beneficios a varias partes interesadas:

- Proporciona a **las autoridades locales** una estrategia preventiva y eficaz en función de los costos para reconocer y premiar a organizadores de mercados comprometidos con mantener unos mercados en los que no se vendan productos que infringen derechos de PI y otros productos ilícitos.
- Ofrece a **los operadores del mercado y los administradores de grupos de venta** un marco práctico y un conjunto de procedimientos para garantizar que los posibles

- comerciantes de productos ilícitos no puedan afianzarse.
- Permite a **los titulares de derechos de PI y a los servicios locales encargados de fijar las normas en materia de comercio** canalizar sus recursos de forma más eficaz hacia los mercados y grupos de venta en los que se producen problemas de falsificación.
 - Garantiza la igualdad de condiciones a **los comerciantes legítimos y los negocios locales** para que no compitan con comerciantes de productos falsificados.
 - Ofrece a **los consumidores** un símbolo reconocible de comercio justo y de compra en mercados sin productos falsificados.

[Fin de la contribución]

LA PERSPECTIVA DE LA AIM (EUROPEAN BRANDS ASSOCIATION) ACERCA DEL PAPEL DE LOS INTERMEDIARIOS EN LÍNEA EN LA LUCHA CONTRA LA FALSIFICACIÓN

*Contribución preparada por la Sra. Marie Pattullo, administradora principal de protección de marcas e imagen de marcas, AIM (European Brands Association), Bruselas (Bélgica)**

RESUMEN

Para garantizar un ecosistema digital limpio y justo para todos los usuarios, y para proteger a los consumidores de las ofertas en Internet de productos falsificados y otros productos ilícitos, de mala calidad y productos infractores, todos los interlocutores de las cadenas de suministro, incluidos los titulares de registros de marcas y los intermediarios en línea, deben cumplir su papel. En esta contribución se describe cómo los intermediarios en línea pueden contribuir ejerciendo un control adecuado en las partes de la cadena de valor que son de su competencia, mediante medidas como, por ejemplo:

- establecer un sistema razonable de diligencia debida para identificar a sus clientes;
- establecer, y hacer cumplir, disposiciones pertinentes de protección de los derechos de PI en sus términos y condiciones y procedimientos eficaces de notificación y retirada;
- aplicar medidas proactivas, incluidas medidas técnicas, para impedir que en sus servicios aparezcan ofertas de productos ilícitos;
- retirar rápidamente (y de forma permanente) ese tipo de ofertas una vez detectadas y prohibir que los reincidentes accedan a sus servicios, y
- proporcionar información de forma proactiva sobre las infracciones a las autoridades encargadas de la aplicación de la ley, incluidas las autoridades aduaneras y de vigilancia del mercado, lo que permite analizar riesgos y determinar objetivos eficazmente.

También se señalan ejemplos concretos de lo que los intermediarios pueden hacer para poner en práctica esas medidas, y también se determinan las esferas en que podrían intensificarse o complementarse las medidas vigentes. Por último, en esta contribución se insta a todos los actores interesados a que tomen medidas en la lucha contra la falsificación.

I. PANORAMA GENERAL

1. Considerando el aumento que está experimentando el comercio mundial de mercancías falsificadas y su incidencia en todas las esferas, desde las medidas de protección de los consumidores y otros sectores de la población hasta las economías nacionales, la obtención de empleo, las industrias de medio ambiente e industrias de la innovación, se señala a menudo que lo que es ilegal en el entorno físico también debería serlo en Internet. La *European Brands Association* opina que es necesario dar un paso más: necesitamos que esa retórica cristalice en medidas reales, prácticas y eficaces.

2. La *European Brands Association* representa a más de 2.500 fabricantes de productos de marca, desde pequeñas y medianas empresas hasta empresas multinacionales. Ninguna de estas

* 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.

empresas elabora mercancías falsificadas ni las transporta, exporta, importa, vende u obtiene algún tipo de beneficio de su comercio. Aunque los titulares de derechos hacen todo lo posible para proteger sus derechos de PI en todo el proceso, desde el registro de la marca hasta llegar a un litigio, no les resulta posible supervisar o controlar la existencia de cadenas de suministro ilegales que pueden perturbar gravemente ese comercio.

3. Así, todos los actores que participan en la cadena de suministro deben cumplir un papel en esta lucha. Si bien en esta contribución la atención se centra en los intermediarios en línea, no podemos ni debemos olvidar el papel que ejercen los intermediarios en el entorno físico, como los operadores de transporte marítimo y otro tipo de operadores de transporte y de logística; los agentes de la exportación, la importación y el despacho aduanero; los intermediarios aduaneros y los operadores de correo y mensajería. Este asunto nos incumbe, o debería incumbirnos, a todos por igual.

II. EL ENTORNO DIGITAL

4. La transformación digital ha traído consigo muchas ventajas, pero también muchos riesgos y retos, como el aumento exponencial de la oferta en Internet de productos falsificados y otros productos ilícitos, productos de mala calidad y productos infractores. Proteger a los consumidores y suministrarles productos de confianza, seguros e innovadores está en la esencia de la labor de todo fabricante de productos de marca, y también debería ser así en la labor que cumple todo intermediario y minorista, tanto en Internet como en el entorno físico.

5. La pandemia nos cambió la conducta casi de la noche a la mañana, y la comunicación y el comercio por Internet pasaron a ser la tendencia principal, y podría decirse que esencial, en muchos lugares. Comprar productos por Internet, ya fueran comestibles y otros productos esenciales, o efectuar compras impulsivas guiadas por el aburrimiento de estar encerrado, se convirtió en lo habitual para millones de personas que antes preferían salir a la calle. También se observó un enorme crecimiento y dependencia del comercio electrónico entre empresas, ya que los intermediarios en línea no solo atienden al mercado entre empresas y consumidores. Mientras que las empresas legales y las autoridades públicas se esforzaban por equilibrar la accesibilidad mediante el establecimiento de salvaguardias en el comercio electrónico, y los organismos encargados del cumplimiento de la ley luchaban por mantener el flujo del comercio esencial, los falsificadores dirigían su atención hacia los equipos de protección personal y los medicamentos falsos, o marcaban incorrectamente sus documentos de envío y embalajes, y proliferaban en línea las ofertas de mercancías falsificadas y fraudes que utilizaban nombres comerciales.

6. Sí, todos estamos agradecidos de que existan estos canales comerciales en Internet. Sí, probablemente, su único destino es crecer. Y sí, todas las marcas, todos los proveedores de servicios necesitan y valoran la relación con los intermediarios en línea para conectar con sus socios comerciales y con los consumidores. Esa es la razón por la que también nosotros necesitamos confiar en ellos para que cumplan su papel a la hora de mantener la seguridad del entorno digital.

III. QUÉ SE NECESITA

7. Desde la perspectiva de los titulares de registros de marcas, los intermediarios en línea pueden contribuir a mantener un ecosistema de Internet limpio y justo ejerciendo un control apropiado sobre las partes de la cadena de valor que son de su competencia mediante medidas como, por ejemplo:

- establecer un sistema razonable de diligencia debida para identificar a sus clientes (“Conoce a tu Cliente Corporativo”);
- establecer, y hacer cumplir, disposiciones pertinentes de protección de la PI en sus términos y condiciones y procedimientos eficaces de notificación y retirada;
- aplicar medidas proactivas, incluidas medidas técnicas, para impedir que en sus servicios aparezcan ofertas de productos ilícitos;
- retirar rápidamente (y de forma permanente) ese tipo de ofertas una vez detectadas y prohibir que los reincidentes accedan a sus servicios, y
- proporcionar información sobre las infracciones de forma proactiva a las autoridades encargadas del cumplimiento de la ley, incluidas las autoridades aduaneras y de vigilancia del mercado, lo que permite analizar los riesgos y establecer objetivos eficazmente.

8. No se pide a los intermediarios en línea que se dediquen a efectuar un monitoreo general, pero, como cualquier empresa, deberían aplicar la diligencia debida. La aplicación de medidas impulsadas por propia iniciativa encaminadas a impedir que los delincuentes exploten sus redes y servicios debería formar parte de las prácticas empresariales, y la cooperación voluntaria y activa con los socios afectados del sector privado, y especialmente los titulares de derechos, debería ser la norma. La verificación de la identidad de los clientes es una medida obvia en una relación comercial, tanto en el entorno físico como en Internet. En una economía responsable y madura, está fuera de toda duda que las empresas no puedan operar y tener acceso a una infraestructura moderna y necesaria si no se identifican con precisión.

9. Se debería aplicar un procedimiento eficaz de notificación y acción que permita tanto a los usuarios como a los titulares de derechos señalar los contenidos ilícitos (que incluya un mecanismo de señalización fiable) para suministrar datos a algoritmos que permitan su revisión automática o, cuando sea necesario, humana y la adopción de medidas apropiadas. Tras la confirmación del contenido ilícito, no solo debe retirarse dicho material rápidamente (cuánto más tiempo permanezca en Internet, más tiempo se defraudará a los titulares de derechos y a los consumidores), sino que en ningún momento debe permitirse que se vuelva a alojar. Debe tenerse en cuenta que se trata de productos falsificados, no de opiniones u otro tipo de contenidos generados por los usuarios que tal vez habría que considerar en el marco de las normas de libertad de expresión. Nadie esperaría que un producto falsificado que se hubiera retirado de las estanterías de un supermercado un martes volviera a estar en ellas el miércoles siguiente. ¿Por qué es diferente en Internet?

10. A los titulares de derechos se les dice con frecuencia que deberían adherirse a los programas de protección de marcas establecidos por los intermediarios. Y lo hacen, y algunos de estos programas pueden resultar eficaces. Sin embargo, los intermediarios en línea piden seguidamente información más detallada sobre sus productos y sobre cómo autenticarlos. Solo un titular de derechos puede autenticar su propia marca, y pocos, de haber alguno, revelarán sus métodos ocultos de protección de marca a otro agente comercial, en particular si se trata de un posible competidor. También se pide frecuentemente a los titulares de derechos que aporten (repetidamente) pruebas y traducciones, incluso en relación con infractores reincidentes, como sucede, lamentablemente, demasiado a menudo.

11. Esta vía de intercambio de información es más bien unidireccional. Los titulares de derechos no les piden a los agentes de Internet que revelen sus algoritmos, pero sería conveniente disponer de algunos comentarios e información útiles. Por ejemplo, en virtud del Memorando de entendimiento de la Unión Europea sobre la venta de productos falsificados a través de Internet,⁴ las plataformas signatarias citan millones de retiradas impulsadas por propia iniciativa por cada

⁴ https://ec.europa.eu/growth/industry/strategy/intellectual-property/enforcement-intellectual-property-rights/memorandum-understanding-sale-counterfeit-goods-internet_en.

período objeto de informe, lo cual está muy bien, salvo por el hecho de que los titulares de derechos no saben a qué se refieren, por qué se retiraron (ni siquiera se sabe cuántas retiradas se deben a infracciones de PI) o incluso qué marcas y qué vendedores están implicados, lo que dificulta las acciones legales posteriores. ¿No sería sin duda más eficaz que todos los actores apuntaran a los mismos comerciantes deshonestos?

12. Por otra parte, los titulares de registros de marcas reciben constantemente peticiones de abundante información por parte de las autoridades que velan por la observancia de los derechos de PI, pero no les es posible suministrar información que no tienen. Los titulares de registros de marca no tienen visibilidad de los canales de suministro y de comercio ilícitos. Si bien gran parte de esos datos pertenecen a las empresas de transporte y otras empresas de logística de transporte, o esas empresas tienen acceso a los mismos, los intermediarios en línea también podrían suministrar gran parte de esos datos, en particular, a las aduanas, que podrían adoptar medidas en la frontera contra el transporte marítimo de grandes cargamentos, antes de que estos se dividan en múltiples envíos pequeños y se propaguen por el mercado. Así, las aduanas deberían registrar y almacenar los datos relativos a todas las retenciones efectuadas, incluidas las de pequeños envíos. En un marco realista, los funcionarios de aduanas no pueden controlar materialmente más de un 1% o 2% de los envíos, de manera que resulta esencial disponer de información y datos sólidos antes de la llegada de los envíos para poder efectuar una evaluación y determinar objetivos eficazmente.

13. El comercio entre empresas y consumidores ha dado lugar a una gran abundancia de pequeños paquetes, pero no debemos engañarnos creyendo que esa es la vía de todos los productos falsificados, es decir que ese no debería ser el único canal que las aduanas deben controlar. Los contenedores de transporte marítimo pueden llenarse de pequeños artículos y paquetes que se envían una vez que el contenedor llega a puerto, y a menudo sirven para transportar las existencias que se almacenan en los centros de distribución. Si las aduanas dispusieran de datos previos a la llegada de los productos que les permitieran detectar envíos sospechosos de gran envergadura, se reduciría el lastre de sus restringidos recursos, maximizando al mismo tiempo las posibilidades de éxito a la hora de detectar envíos ilícitos. Ello debería asimismo reducir en consecuencia los índices de fraude y evasión fiscales, dando así apoyo a las principales funciones aduaneras en cuanto que organismos de protección y recaudación de los ingresos públicos.

14. El intercambio proactivo de datos de los envíos y del cliente con los organismos encargados del cumplimiento de la ley debería ser una práctica comercial habitual. En las plataformas, las redes sociales, los proveedores de pago en línea, los servicios de mensajería y los de correo y postales saben, o deberían saber, quiénes son sus clientes. Deberían disponer de información detallada de los delincuentes reincidentes y tener acceso a cuentas vinculadas (por ejemplo, aquellas en que se utilizan las mismas direcciones de protocolo de Internet o información bancaria). Los encargados de la gestión de centros de almacenaje y redes de distribución propios cuentan con diferentes tipos de datos comerciales, por ejemplo, manifiestos de carga y listas de pedidos, información que debería intercambiarse de forma proactiva con los organismos encargados del cumplimiento de la ley, en el marco de los parámetros legales pertinentes. Estos intermediarios están en perfecta situación no solo para redactar los términos y condiciones comerciales apropiados de sus clientes de pago, sino también para aplicarlos, inclusión hecha, en su caso, de disposiciones contractuales o incluso de contratos de seguros para cubrir posibles retrasos o costos, como puedan ser de almacenamiento y destrucción.

15. Los actores en el sistema de nombres de dominio (proveedores de alojamiento web, registros, registradores, proveedores de servidores proxy, revendedores, etcétera) también cumplen su papel. El acceso y la divulgación de datos WHOIS exactos y verificados son de interés público y necesarios para el cumplimiento de las obligaciones legales. Como consecuencia lamentable pero inevitable de los métodos elegidos por la Corporación para la Asignación de Nombres y Números de Internet (ICANN) para aplicar el Reglamento General de Protección de

Datos (RGPD) de la Unión Europea, nos topamos con una expurgación casi total de los datos de los titulares de nombres de dominio que va mucho más allá de lo necesario. Por ejemplo, no hay ninguna razón para que no se recojan y divulguen los datos de las personas jurídicas, a los que no se aplica el RGPD. Se ha suprimido así la principal información para la investigación de delitos contra la PI, la ciberseguridad y la protección del consumidor en el marco de la lucha contra nombres de dominio infractores, utilizados para vender mercancías falsificadas y cometer muchos otros fraudes cibernéticos en que se hace un uso indebido de las marcas.

16. Algunos datos de las personas jurídicas deberían ser públicos (¿por qué un usuario no debe saber a quién le da los datos de su tarjeta de crédito y otros datos personales?) y otros datos de los titulares de nombres de dominio deberían ser divulgados sin dilación en atención a una petición legítima. Aunque el proyecto de Directiva de la Unión Europea sobre seguridad de las redes y sistemas de información⁵ está orientado hacia la ciberseguridad y no hacia la PI, la *European Brands Association* espera que dicha Directiva contribuya a restablecer ese equilibrio, sobre todo teniendo en cuenta el uso de nombres de marca en tantos ciberdelitos, como, por ejemplo, la suplantación de la identidad y otros fraudes de Internet.

17. Un latiguillo habitual que se obtiene cuando se pregunta por un dato es “bloqueo de datos: RGPD”. El RGPD no se aplica a los datos de las personas jurídicas ni su objeto era servir de escudo de las actividades delictivas. No debería haber ningún impedimento para que los intermediarios en línea (o los intermediarios en el entorno físico) compartan los datos de las personas jurídicas con los organismos de la Unión Europea encargados del cumplimiento de la ley, y también debería ser posible efectuar ese tipo de intercambios en otras jurisdicciones. Es muy necesario que exista algún tipo de orientación oficial sobre el intercambio de datos personales necesarios para las investigaciones de delitos de PI y las consiguientes acciones legales, y no debería resultar polémico que se permita que los investigadores accedan a los datos de personas que han sido designadas como responsables de actividades ilegales.

18. Para llevar a la realidad gran parte de lo que se expone más arriba, no es necesario contar con legislación. Sin embargo, la experiencia demuestra que las medidas de carácter voluntario no bastan por sí solas. La Ley de Servicios Digitales de la Unión Europea⁶ aporta algunas medidas útiles, pero al ser horizontal, es decir que se aplica a todas las formas de contenido ilícito en Internet, y no únicamente a las mercancías, no es una ley preparada para el futuro si se considera desde el punto de vista de la lucha contra la falsificación.

19. Los propietarios de marcas acogen con satisfacción, en cuanto que medidas de mitigación de riesgos, las disposiciones de la Ley de Servicios Digitales que ayudarán a frenar la venta de productos ilícitos por Internet, así como el mecanismo armonizado de la Unión Europea de notificación y acción para detectar y suprimir las ofertas en línea de productos ilícitos y las obligaciones adicionales para plataformas de gran envergadura. No obstante, la *European Brands Association* lamenta que esas nuevas obligaciones no se apliquen a todos los intermediarios en línea que participan en la venta o la promoción de productos ilícitos en Internet, en particular, en redes sociales, aplicaciones móviles y plataformas publicitarias, así como el hecho de no haber introducido una obligación de retirada definitiva en relación con los proveedores de servicios de alojamiento web que impida que contenidos señalados previamente y retirados o desactivados o contenidos similares vuelvan a alojarse en sus servicios. La *European Brands Association* confía en que el próximo instrumento de la Unión Europea, a saber, el Conjunto de herramientas de la Unión Europea contra la falsificación⁷, aportará las herramientas y medidas prácticas necesarias para colmar estas lagunas.

⁵ Para obtener más información sobre la Directiva, véase:

[https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI\(2021\)689333_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf).

⁶ <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>.

⁷ https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12915-EU-toolbox-against-counterfeiting_es.

IV. SIGUIENTES PASOS

20. La lucha contra la falsificación no se limita a proteger derechos privados. Debido a la demostrada vinculación de los delitos de PI con la delincuencia organizada, la Agencia de la Unión Europea para la Cooperación Policial (Europol), con el apoyo de la Oficina de Propiedad Intelectual de la Unión Europea (EUIPO), ha creado la Coalición Coordinada para Delitos contra la PI. Dicho instrumento se ha visto reforzado tras la reinstauración de los delitos de PI como prioridad en el marco de la Plataforma Multidisciplinar Europea contra las Amenazas Delictivas (EMPACT) durante el período comprendido entre 2022 y 2025. En los estudios y la información disponible de órganos públicos como la Organización de Cooperación y Desarrollo Económicos (OCDE) y el Observatorio de la EUIPO sobre infracciones de derechos de PI se destaca reiteradamente el daño, incluido el daño físico, que el comercio de las mercancías falsificadas causa a los consumidores. Las recaudaciones públicas en forma de impuestos y derechos se agotan. Se pierden puestos de trabajo. Las empresas quiebran. El mismo medio ambiente se pone en peligro con la producción y el transporte de mercancías que nunca deberían haberse fabricado y que no pueden destruirse o reciclarse de forma sostenible, al desconocerse las materias primas con que están hechas.

21. Es esta una batalla conjunta en la cual corresponde a los intermediarios en línea cumplir un papel fundamental en la medida en que los delincuentes, más interesados en obtener ganancias ilícitas que en respetar las leyes, las normas y la seguridad, sigan abusando de sus infraestructuras y servicios. Ninguno de nosotros, ni en línea ni en el entorno físico, podemos ganarla solos. La estrategia de división no tiene cabida aquí; debemos trabajar juntos.

[Fin de la contribución]

LA PERSPECTIVA DE LA INDUSTRIA DE LAS GRABACIONES MUSICALES ACERCA DEL PAPEL DE LOS INTERMEDIARIOS EN LA LUCHA CONTRA LA PIRATERÍA

*Contribución preparada por el Sr. Lauri Rechartt, jefe de asuntos jurídicos, Federación Internacional de la Industria fonográfica (IFPI), Londres (Reino Unido)**

RESUMEN

La piratería en línea todavía representa una grave amenaza para la industria musical. El estudio de los consumidores de música de 2021, efectuado por la Federación Internacional de la Industria Fonográfica (IFPI) y que es el mayor estudio de mercado centrado en la música en todo el mundo¹, puso en evidencia que el 30% de las personas encuestadas utiliza medios no autorizados para la escucha o descarga de música. Esta proporción se eleva al 38% entre los jóvenes de 16 a 24 años.

Habida cuenta de la ingente cantidad de contenidos disponibles, el *stream ripping*, una forma de piratería que consiste en la copia o “ripeo” de contenidos transmitidos por flujo continuo, y la creación de copias digitales permanentes de estos contenidos, es uno de los principales motivos de gran preocupación.

La piratería antes de la difusión, es decir, la puesta a disposición no autorizada de grabaciones antes de su fecha de lanzamiento, es otra actividad particularmente perjudicial para los titulares de derechos en la industria musical, debido a las repercusiones comerciales tan negativas que tiene en las ventas legales. Los contenidos que todavía no se han difundido suelen estar disponibles a través de las plataformas de las redes sociales, mientras que el contenido original se almacena en los denominados *cyberlockers*. Estos *cyberlockers* no suelen exigir, menos aún verificar, los datos de identificación de sus usuarios, circunstancia que dificulta que los titulares de derechos puedan emprender acciones directas contra la persona o personas que hayan cometido la infracción primaria.

Los intermediarios en línea, a cuyos medios recurren los servicios en línea infractores, desempeñan un papel fundamental a la hora de abordar con eficacia los usos no autorizados. El presente documento determina las principales medidas y procedimientos que deben aplicar con diligencia los intermediarios en línea, al objeto de reforzar la observancia de los derechos en la red.

Entre estas acciones figuran la definición del ámbito y las condiciones de la cláusula de exención de responsabilidad, la implantación de políticas rigurosas de “Conoce a tu Cliente Corporativo” (KYBC, por su sigla en inglés), la mejora de la transparencia y la implantación de políticas estrictas para hacer frente a los infractores reincidentes.

Asimismo, la IFPI respalda la ampliación de la base de datos WIPO ALERT como centro fiable para la recopilación y el intercambio de información sobre sitios problemáticos facilitada por las administraciones competentes de los Estados miembros de la OMPI al servicio de la industria publicitaria.

* 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.

¹ El estudio se llevó a cabo en 21 países y recogió las opiniones de 43.000 personas.

I. UN MERCADO MUSICAL PRÓSPERO QUE LIDIA CON EL PROBLEMA DE LA PIRATERÍA EN LÍNEA

2. La Federación Internacional de la Industria Fonográfica (IFPI) es la asociación internacional que se ocupa de la defensa de los intereses de la industria discográfica en todo el mundo. La IFPI y su red de asociaciones profesionales afiliadas cuentan entre sus miembros con 8.000 destacadas compañías discográficas independientes, dedicadas a la creación, producción y distribución de grabaciones sonoras en más de 70 países.

3. La industria musical fue una de las primeras en reaccionar ante el desafío de la digitalización. Durante más de 15 años sufrió una caída considerable de los ingresos a causa, sobre todo, del uso masivo no autorizado de música en Internet, hasta que, en 2015, recuperó la tendencia de crecimiento. Durante esa época tan complicada, las discográficas no dejaron de invertir en artistas y sistemas e infraestructuras mundiales, lo cual les permitió otorgar licencias a más de 60 millones de canciones y cientos de servicios digitales en todo el planeta. Gracias a ese tesón, los aficionados a la música gozan hoy en día de un acceso prácticamente ilimitado a un volumen sin precedentes de música de diversa índole, mientras que los artistas pueden acceder a los mercados mundiales y a la oportunidad de establecer vínculos con seguidores de cualquier lugar del planeta.

4. No obstante, los usos no autorizados de música en Internet suponen un grave problema para la industria discográfica y, en particular, los servicios de *stream ripping*, con los que los usuarios pueden hacer copias permanentes de las grabaciones de los servicios en línea de transmisión por flujo continuo. En los últimos tiempos, las infracciones se han trasladado de los servicios en la web a las aplicaciones móviles. La IFPI calcula que cada mes se descargan 515 millones de canciones de sitios de *stream ripping*². Los servicios de *cyberlocker* (servicios de almacenamiento de archivos en línea) plantean un problema similar para los titulares de derechos, ya que en ellos los usuarios pueden cargar y distribuir archivos digitales en una plataforma de almacenamiento cuyo control, gestión y mantenimiento corre a cargo del operador del sitio web. A menudo, estos servicios distribuyen contenidos que todavía no se han difundido, una práctica que perjudica de manera particular a los resultados comerciales de los titulares de derechos. Otros servicios problemáticos son algunas plataformas de redes sociales, foros en Internet y servicios de mensajería que se utilizan para compartir a gran escala material que infringe el derecho de autor.

II. DEBER DE DILIGENCIA Y RESPONSABILIDADES DE LOS INTERMEDIARIOS EN LÍNEA

4. Los intermediarios de uno u otro tipo desempeñan un papel esencial en la lucha contra las infracciones en Internet. Gracias a su rol primordial en el entorno de red digital, suelen ser los más indicados para evitar las actividades infractoras.

5. Los proveedores de acceso a Internet, las redes de distribución de contenidos (por ejemplo, Cloudflare), los proveedores de servicios de alojamiento, los motores de búsqueda, los registradores y registros de nombres de dominio, las tiendas de aplicaciones, los mercados de comercio electrónico, los procesadores de pagos y los anunciantes pueden contribuir a que el Internet sea un lugar más seguro y a que el mercado de contenidos digitales funcione mejor.

² La IFPI compila datos sobre visitas a sitios de copia de contenidos transmitidos por flujo continuo de otros sitios similares y calcula la proporción de esas visitas, cuyo resultado es la descarga eficaz de contenidos musicales protegidos por derecho de autor.

6. Las autoridades legislativas han reconocido la necesidad de fortalecer las responsabilidades y la rendición de cuentas de los intermediarios en línea³, y así lo demuestran el reciente proyecto de ley sobre seguridad en Internet del Reino Unido y la propuesta de Ley de Servicios Digitales⁴ de la Unión Europea (UE). La forma y el ámbito de aplicación de las medidas que cabe esperar de los intermediarios dependerán de la actividad que desempeñe cada uno de ellos. En el apartado siguiente se describen varias medidas razonables y eficaces que pueden contribuir a la creación de un entorno de Internet más seguro y un mercado de contenidos digitales sostenible.

A. MEDIDAS PROACTIVAS PARA EVITAR LAS INFRACCIONES DEL DERECHO DE AUTOR

7. Los servicios de alojamiento, como las plataformas en línea que almacenan los contenidos cargados por sus usuarios, desempeñan un papel de creciente importancia en la distribución de contenidos por Internet.

8. En muchas jurisdicciones, los proveedores de estos servicios de alojamiento gozan de limitaciones de la responsabilidad a condición de que retiren con prontitud los contenidos infractores en cuanto tengan conocimiento, real o presunto, de su existencia. No obstante, con la evolución del ecosistema de Internet (la web 2.0), estas cláusulas de exención de responsabilidad se han tornado problemáticas en un gran número de casos. Por un lado, no queda claro qué tipo de plataformas tienen derecho a estos privilegios. Por otro lado, en vista del volumen de contenidos y de la celeridad con la que se cargan en estas plataformas, se ha demostrado la ineficacia de las sencillas medidas de “retirada”, pues se puede volver a cargar los mismos contenidos inmediatamente después en el mismo servicio.

9. Con respecto al primer punto, las autoridades de la UE y el Tribunal de Justicia de la UE han tratado de precisar el ámbito de aplicación de las cláusulas de exención de responsabilidad. En esencia, las cláusulas de exención de responsabilidad deben circunscribirse a los intermediarios técnicos, automáticos y pasivos. Del mismo modo, en su informe de 2020 sobre el Artículo 512 del Título 17 de la Ley de Derecho de Autor de los Estados Unidos relativo a las cláusulas de exención de responsabilidad, la Oficina de Derecho de Autor de los EE.UU. cuestionó la aplicación de las cláusulas de exención de responsabilidad a los servicios que van más allá del mero almacenamiento de contenidos⁵.

10. En lo referente al segundo punto, según los datos de la IFPI, un número elevado de notificaciones de infracción enviadas por la IFPI estaban relacionadas con los mismos contenidos y el mismo sitio. Por ejemplo, en el marco de Twitter en el año 2020, el tema *Blinding Lights* de The Weeknd fue notificado más de 3.700 veces y *Watermelon Sugar* de Harry Styles lo fue más de 2.900 veces tras la primera notificación. Estos datos ponen de manifiesto que el sistema vigente de “notificación y retirada” ha resultado ser un instrumento ineficaz para hacer frente al enorme volumen de contenidos en línea que infringen el derecho de autor.

11. Para resolver este problema, los proveedores de servicios de alojamiento deben garantizar medidas de “retirada definitiva” para poder acogerse a los privilegios de las cláusulas de exención de responsabilidad. Esto implica que, en el momento mismo en que tenga conocimiento de una infracción, el proveedor de servicios de alojamiento debe i) eliminar todas las copias de la obra o la grabación sonora y ii) garantizar que esa misma obra o grabación (o una copia) no se vuelva a publicar o a cargar en el futuro (es decir, la obligación de retirarla de forma definitiva), o correrá el riesgo de tener que asumir responsabilidades.

³ <https://bills.parliament.uk/bills/3137/publications>.

⁴ <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM%3A2020%3A825%3AFIN>

⁵ <https://www.copyright.gov/policy/section512/section-512-full-report.pdf>

12. Las medidas de “notificación y retirada definitiva” son una obligación eficaz y proporcionada, habida cuenta también de que se pueden llevar a la práctica a través de tecnologías disponibles en el mercado, como las aplicaciones de reconocimiento automático de contenido.

B. POLÍTICAS PARA INFRACTORES REINCIDENTES

13. Todos los intermediarios también deben poner en marcha políticas eficaces contra los infractores reincidentes. Ello supone que cuando un intermediario sepa o tenga conocimiento de que un destinatario de sus servicios (ya sea un revendedor o un usuario final) ha utilizado sus servicios de forma reiterada para vulnerar sus derechos de propiedad intelectual (PI), el intermediario deberá (en las circunstancias adecuadas) interrumpir la prestación de sus servicios a dicho destinatario. Esta obligación ya forma parte de las condiciones de exención de responsabilidad previstas en la Ley de Derecho de Autor de los Estados Unidos de América.

14. La política para infractores reincidentes debe aplicarse en aras de la prevención y disuasión del uso de los servicios de los intermediarios para llevar a cabo actividades ilegales de manera reiterada y sistemática. Asimismo, la política debe garantizar que los infractores reincidentes a quienes se haya suspendido la prestación de servicios no puedan utilizar el servicio con otro nombre. La aplicación de esta política debe ir acompañada de otra política eficaz de “Conoce a tu Cliente Corporativo” (KYBC, por su sigla en inglés)⁶.

15. Las condiciones de servicio planteadas por los intermediarios en línea deben indicar de manera clara y transparente el derecho y la facultad de los intermediarios de suspender y poner fin a la prestación de sus servicios a los infractores reincidentes, de conformidad con los principios expuestos anteriormente.

III. TRANSPARENCIA Y ACCESO A LA INFORMACIÓN

16. La falta de transparencia, en particular el hecho de que los operadores de servicios ilegales en línea puedan ocultar fácilmente su identidad, es uno de los principales obstáculos que impiden la observancia efectiva de los derechos de PI en la red. Hoy en día, los operadores pueden actuar en el más absoluto anonimato, al amparo de servicios de privacidad de dominios o empresas ficticias, y los intermediarios no suelen exigir a sus clientes que acrediten su auténtica identidad y sus datos de contacto reales. Esta situación socava en gran medida la labor de observancia de la legislación en Internet, así como los intentos de contactar con los presuntos infractores o de emprender acciones contra ellos.

17. Los gobiernos de todo el mundo han de plantearse una serie de medidas para hacer frente a la falta de transparencia en línea.

A. “CONOCE A TU CLIENTE CORPORATIVO” Y NORMAS DE ACCESO

18. La legislación debe exigir a los intermediarios en línea que pongan en marcha políticas eficaces en materia de KYBC, es decir, que garanticen la disponibilidad de información precisa sobre sus clientes, incluidos sus datos de contacto. Tales obligaciones ya existen en otros sectores, como los sectores de servicios financieros o bancarios y de servicios jurídicos. Además, la Ley de Servicios Digitales, que actualmente se está finalizando en el ámbito de la Unión Europea, propone imponer una obligación sobre los mercados en Internet para verificar la identidad de los comerciantes que hacen negocios en sus plataformas. El concepto de “cliente

⁶ Véase la sección IV.

con propósitos comerciales” debe interpretarse de manera que englobe a las personas jurídicas y físicas que actúan con ánimo de lucro directo o indirecto. Deben imponerse las sanciones penales pertinentes por incumplimiento de la obligación y los intermediarios deben interrumpir los servicios que prestan a los clientes con propósitos comerciales que no faciliten la información necesaria. Esta obligación también debe extenderse a los revendedores de los servicios del intermediario original.

19. Además de la obligación de aplicar una política de KYBC, debe preverse un fundamento jurídico claro para que las personas que tengan un interés legítimo en acceder a la información en manos de los intermediarios puedan hacerlo de manera oportuna. Los titulares de derechos que investiguen las infracciones de los derechos de PI, con arreglo a la legislación aplicable, tienen ese interés legítimo y, por ende, se les debe permitir el acceso a esa información.

B. PUBLICACIÓN DE DATOS DE CONTACTO PRECISOS

20. Debe establecerse el requisito básico de que todos los servicios de la sociedad de la información publiquen en sus sitios web los datos precisos de contacto y de los operadores. Por ejemplo, el artículo 5 de la Directiva sobre el comercio electrónico de la UE⁷ establece esta obligación a los proveedores de servicios de Internet. Por desgracia, hasta la fecha, el cumplimiento en la práctica de esa obligación por parte de las autoridades de los Estados miembros de la UE ha brillado por su ausencia y apenas se prevén sanciones disuasorias en caso de incumplimiento. Es fundamental contar con este tipo de disposiciones estrictas en materia de transparencia y velar por su observancia efectiva, no solo en beneficio de los titulares de los derechos de PI, sino también desde el punto de vista más general de la protección del consumidor.

C. ACCESO A REGISTROS COMO LAS BASES DE DATOS WHOIS

21. A raíz de los cambios introducidos en las leyes de protección de datos en Europa, la Corporación de Internet para la Asignación de Nombres y Números (ICANN)⁸ introdujo una especificación temporal para las bases de datos WHOIS⁹ que exigía a los registradores y a los registros que redactaran la gran mayoría de los datos WHOIS relativos a los registradores de dominios europeos (con independencia de que fueran personas físicas o jurídicas). El resultado ha sido una retirada casi total y en muchos casos injustificada del registro público WHOIS, que rebasa con creces todos los requisitos previstos en el Reglamento General de Protección de Datos (RGPD)¹⁰ (que ha sido utilizado para justificar la retirada del acceso a WHOIS) y que ha tenido una incidencia considerable en la capacidad de los titulares de derechos a la hora de obtener los datos necesarios para la observancia efectiva de sus derechos. Urge intervenir al objeto de restablecer el acceso de los titulares de derechos al registro WHOIS con el fin legítimo de investigar y velar por el respeto de sus derechos de PI. Si bien se han emprendido algunas iniciativas legislativas destinadas a resolver el problema de la inaccesibilidad a la información de las bases de datos WHOIS, como la propuesta de Directiva SRI 2¹¹ en la UE, hasta ahora han

⁷ Directiva 2000/31/CE relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior, disponible en <https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX%3A32000L0031>

⁸ La ICANN es un grupo formado por múltiples partes interesadas que coordina varias bases de datos relacionadas con Internet.

⁹ WHOIS es un protocolo que se vincula a bases de datos mantenidas por los registradores y registros de nombres de dominio en relación con información de sus clientes.

¹⁰ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, DO L 119 (<https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679>).

¹¹ <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM%3A2020%3A823%3AFIN>.

demostrado ser inadecuadas. Es urgente intervenir de manera integral con miras a precisar el interés que reviste un registro público WHOIS para los titulares de derechos, de modo que estos puedan investigar y hacer valer sus derechos.

IV. LA LUCHA CONTRA LA PIRATERÍA TRANSFRONTERIZA

22. Los servicios que lucran a costa de la distribución no autorizada de música en Internet pueden establecerse en prácticamente cualquier lugar, y las infracciones del derecho de autor en línea pueden darse de manera simultánea más allá de las fronteras en un número ilimitado de territorios. No obstante, a la hora de intentar poner fin a las operaciones de estos negocios ilegales, ya sea mediante la adopción de medidas directas contra los infractores o la búsqueda de medidas cautelares contra los servicios intermediarios utilizados por los infractores, los titulares de derechos se ven abocados a emprender acciones judiciales en todas y cada una de las jurisdicciones en las que el servicio está disponible. Este proceso conlleva una ralentización y un encarecimiento considerables de la lucha contra las infracciones en línea y limita la eficacia de las acciones emprendidas por los titulares de derechos con el fin de protegerlos.

23. Por ejemplo, desde hace más de 15 años, los titulares de derechos intentan frenar las infracciones de la PI en el famoso sitio web denominado "The Pirate Bay". Los operadores del sitio se han enfrentado a procesos civiles y penales y los casos se han trasladado al Tribunal de Justicia de la UE, así como al Tribunal Europeo de Derechos Humanos¹². Todos los casos confirmaron el carácter infractor del derecho de autor del servicio y, pese a ello, el sitio se mantiene accesible en muchas jurisdicciones de todo el mundo.

24. Las autoridades legislativas pueden adoptar más medidas para facilitar y mejorar la observancia transfronteriza de los derechos de PI. Los derechos sustantivos, las medidas de observancia y los procedimientos están ampliamente armonizados a nivel internacional en virtud de los Tratados Internet de la Organización Mundial de la Propiedad Intelectual (OMPI) y del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio de la Organización Mundial del Comercio (OMC). En los casos pertinentes, estos elementos comunes deben permitir que los tribunales nacionales acepten las constataciones de las autoridades judiciales o administrativas competentes de otros países como prueba suficiente de las reclamaciones del mismo tipo (por ejemplo, reclamaciones relativas al carácter infractor de un sitio web). Este avance puede revestir suma importancia, por ejemplo, en los casos de medidas cautelares de bloqueo no basadas en la culpa contra intermediarios en línea que estén relacionados con un mismo servicio que opere en varias jurisdicciones, así como en los casos de infracción directa relativos al mismo contenido, los mismos titulares de derechos y el mismo servicio en línea que opera en varios territorios. Asimismo, los tribunales deben estar facultados para evaluar los daños a nivel mundial, es decir, no deben limitarse al territorio de su jurisdicción.

25. En este contexto, la IFPI apoya la labor de la OMPI de promoción de la base de datos WIPO ALERT. La IFPI considera que esta iniciativa puede representar un papel clave en la recopilación y el intercambio de información sobre los sitios problemáticos facilitada por las autoridades de los Estados miembros de la OMPI en beneficio de la industria publicitaria. Asimismo, los gobiernos han de fomentar y facilitar el diálogo entre los titulares de derechos y los intermediarios a nivel local para acordar soluciones voluntarias, similares a los códigos de conducta sobre el bloqueo de sitios web acordados por las partes interesadas en Alemania¹³,

¹² C-610/15 *Stichting Brein v Ziggo BV and XS4ALL Internet BV* (2017), disponible en: <https://curia.europa.eu/juris/liste.jsf?language=en&T,F&num=c-610-15>; *Neij and Sunde Kolmisoppi v Sweden* (2013) Solicitud N.º 40397/12, disponible en: <https://hudoc.echr.coe.int/eng#%7B%22appno%22%3A%2240397%2F12%22%7D>.

¹³ <https://cuii.info/ueber-uns/>.

Dinamarca¹⁴, España¹⁵, los Países Bajos¹⁶, Portugal¹⁷ y Suecia¹⁸, o los memorandos de entendimiento pactados entre anunciantes, intermediarios publicitarios y titulares de derechos.

[Fin de la contribución]

¹⁴ <https://rettighedsalliancen.com/new-code-of-conduct-agreement-between-the-telecommunications-industry-and-the-rights-alliance-ensures-more-effective-enforcement/> and https://rettighedsalliancen.com/wp-content/uploads/2020/11/CoC_ENG.eksl_.Anneks.pdf.

¹⁵ <https://www.culturaydeporte.gob.es/actualidad/2022/01/220121-protocolo-antipirateria.html>

¹⁶ <https://www.acm.nl/en/publications/agreement-among-internet-providers-and-copyright-holders-regarding-blocking-websites-illegal-content>.

¹⁷ <https://edri.org/our-work/portugal-voluntary-agreement-against-copyright-infringements/>.

¹⁸ <https://rattighetsalliansen.se/wp-content/uploads/2022/05/Branschoverenskommelse.pdf>.

EL CUMPLIMIENTO DE LA NORMATIVA ADUANERA EN LA INDUSTRIA DEL TRANSPORTE URGENTE: EL ENFOQUE DE DHL EXPRESS

*Contribución preparada por la Sra. Sandra Fischer, jefa aduanas global; la Sra. Asha Menon, vicepresidenta de cumplimiento aduanero global y asuntos regulatorios; el Sr. Marcelo Godoy Rigobello, vicepresidente de atención al cliente de aduanas global; y el Sr. Gordon Wright, vicepresidente de asuntos normativos y de aduanas en la UE, DHL Express, Diegem (Bélgica)**

RESUMEN

En un mundo cada vez más interconectado, mucho más de lo que las generaciones anteriores podrían haberse imaginado, el comercio mundial ha cobrado una importancia sin precedentes. El rápido crecimiento del comercio electrónico y la pandemia del COVID-19 han aumentado significativamente la cantidad de paquetes internacionales en circulación por el mundo, lo que ha provocado mayores desafíos en lo atinente al cumplimiento de las normas aduaneras y comerciales. Este documento presenta un panorama general de alto nivel acerca del planteamiento de DHL Express para garantizar el cumplimiento de la normativa aduanera en su red, así como propuestas respecto de las esferas de cooperación con las autoridades para hacer frente a las infracciones.

I. PLANTEAMIENTO DE DHL EXPRESS SOBRE EL CUMPLIMIENTO DE LA NORMATIVA ADUANERA

1. DHL Express mantiene un firme compromiso con el cumplimiento de la normativa en materia de comercio. El respeto de la normativa aduanera es un aspecto fundamental de la cultura de DHL Express y de la propuesta de valor que ofrece a sus clientes, así como de su mandato de trabajo ético. La misión del Equipo de Cumplimiento Aduanero de DHL Express consiste en facilitar el crecimiento sostenible de la empresa, al proporcionar a sus clientes una experiencia de comercio transfronterizo eficiente y en cumplimiento de la normativa a través de la colaboración con las autoridades.

2. Desde hace años, DHL Express cuenta con una serie de controles proactivos para evitar que los envíos que no cumplan con la normativa entren en su red global. Los controles son los que figuran a continuación:

- control físico de la seguridad de los envíos de carga aérea antes de la salida de los aviones (por ejemplo, mediante inspecciones por rayos X);
- inspecciones o exámenes físicos de los envíos (por ejemplo, para detectar de forma proactiva las mercancías peligrosas no declaradas); y
- filtrado de entidades no autorizadas en todos los envíos mediante análisis de datos (a partir de la información del consignador y el consignatario).

3. Además de estos controles proactivos, DHL Express ha puesto en marcha el Programa Mundial de Cumplimiento Aduanero con el objetivo de reforzar la integridad de los envíos y la calidad de los datos de las facturas proporcionadas por los expedidores. De este modo, las

* 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.

autoridades aduaneras podrán llevar a cabo una evaluación de riesgos más focalizada y respaldar el cumplimiento de los procesos propios del despacho de aduana.

4. De cara a que las iniciativas de cumplimiento interno sean fructíferas, DHL Express estima que es necesario establecer una estrecha colaboración con las autoridades aduaneras para instruir a los expedidores. En este sentido, es fundamental que las autoridades aduaneras mejoren la comunicación directa con los expedidores (que son quienes suministran las mercancías físicas y los datos o la información) sobre lo importante que es facilitar datos de alta calidad al hacer envíos internacionales, para que sean plenamente conscientes de las responsabilidades inherentes a los envíos transfronterizos.

II. PROGRAMA MUNDIAL DE CUMPLIMIENTO ADUANERO DE DHL EXPRESS

5. DHL Express ha puesto en marcha el Programa Mundial de Cumplimiento Aduanero para dar mayor prioridad a la formación de sus clientes en las cuatro esferas de riesgo que se indican a continuación:

- derechos de propiedad intelectual (DPI): para evitar que los expedidores envíen mercancías infractoras de los DPI a través de DHL Express;
- infravaloración: para evitar que los expedidores subestimen el valor de las mercancías en la factura comercial con el fin de pagar una cantidad menor (o nula) de aranceles o impuestos;
- descripciones de las mercancías: para impedir que los expedidores faciliten descripciones incompletas o inexactas de las mercancías con el fin de burlar los controles de seguridad; y
- autenticidad del expedidor y el destinatario: para evitar que los expedidores aporten información inexacta sobre el expedidor o el destinatario con el fin de sortear el control de seguridad o el filtrado de entidades no autorizadas.

6. El factor esencial que subyace a las cuatro esferas de riesgo mencionadas es la calidad de los datos. Habida cuenta de esta prioridad y del compromiso terminante de DHL Express de informar y sensibilizar a sus clientes acerca de la importancia de facilitar datos completos y precisos con el fin de proteger las mercancías legítimas que se envíen con esta compañía de logística, es fundamental que los expedidores sean conscientes de que el incumplimiento de la normativa acarrea consecuencias graves y tangibles.

7. Además de educar a sus clientes, DHL Express también instruye a sus empleados a través de comunicados y formaciones internas, al tiempo que mejora sus procesos e instrumentos internos de gestión de riesgos para reducir las probabilidades de que entren envíos que no cumplen con la normativa en la red de DHL Express. Entre las iniciativas internas figuran, entre otras, las siguientes:

- reforzar las condiciones para la creación de nuevas cuentas para evitar la entrada de infractores conocidos;
- poner a prueba las herramientas de análisis de datos y aprendizaje automático para identificar e interceptar de forma anticipada los envíos que puedan incumplir la normativa en los países de origen; y
- mejorar los sistemas de reserva de envíos para orientar a los expedidores sobre la forma óptima de crear descripciones de mercancías completas y precisas al hacer envíos con DHL Express.



Imagen 1: Ejemplos de pósters internos de DHL Express para sensibilizar a los empleados acerca de las cuatro esferas de riesgo de incumplimiento de las normativas aduaneras.

III. RESPUESTA PROACTIVA A LAS INFRACCIONES DE LA PROPIEDAD INTELECTUAL EN LA PRÁCTICA

8. DHL Express Hong Kong cuenta con un equipo especializado que inspecciona a diario las mercancías y trabaja en estrecha colaboración con las autoridades aduaneras de Hong Kong en busca de mercancías que vulneren los DPI. Durante 2020 y 2021, DHL Express Hong Kong interceptó más de 28.000 envíos salientes tras la inspección física con el fin de identificar las mercancías que se sospechaba que infringían los DPI.



Imagen 2: Empleados de DHL Express Hong Kong efectuando inspecciones físicas de mercancías sospechosas de infringir los DPI.

9. En octubre de 2021, a través de una “carta de agradecimiento”, las autoridades aduaneras de Hong Kong encomiaron la labor de DHL Express Hong Kong en la lucha contra el contrabando, ya que gracias a sus controles se incautaron mercancías infractoras de los DPI y otros productos ilícitos por valor de 7,6 millones de dólares de Hong Kong durante el tercer trimestre de 2021. Este reconocimiento pone de manifiesto el compromiso sostenido del equipo de DHL Express Hong Kong con el cumplimiento de la normativa de comercio.

10. DHL Express EE. UU., en estrecha colaboración con la Oficina de Aduanas y Protección Fronteriza de los Estados Unidos (CBP, por sus siglas en inglés), trabaja con decisión en la interceptación e inspección de mercancías sospechosas de infringir los DPI y brinda apoyo operativo al programa de abandono voluntario de mercancías presuntamente infractoras de los DPI¹. DHL Express EE. UU. dedica recursos a la identificación y retirada de mercancías

¹ Un programa piloto en el que la aduana retiene los envíos sospechosos de infringir los DPI y DHL presenta al cliente la opción de abandonar la mercancía o impugnar las constataciones de la aduana sobre la vulneración de los DPI. Gracias a este proceso, las autoridades aduaneras pueden retirar inmediatamente de la red los envíos que infringen los DPI sin necesidad de llevar a cabo una prolongada operación de incautación.

infractoras de los DPI de su red y colabora con los equipos del origen en la eliminación de los “expedidores problemáticos” de su red. En 2021, el equipo de DHL Express EE. UU., junto con la CBP, interceptó durante la inspección física más de 3.500 envíos al objeto de identificar mercancías sospechosas de vulnerar los DPI, con lo que contribuyó al bloqueo de muchas cuentas de “expedidores problemáticos”. También en 2021, se remitieron más de 5.000 envíos por valor de 246,3 millones de dólares de los EE. UU. al proceso de la CBP de abandono de mercancías presuntamente infractoras de los DPI, con el consiguiente ahorro de más de 49 millones de dólares de los EE.UU.² para los contribuyentes estadounidenses.

11. La CBP del puerto de Cincinnati ha señalado el inestimable valor que tiene su alianza con DHL y afirma que la colaboración de esta empresa de logística en la detección las mercancías prohibidas e infractoras de los DPI resulta decisiva a la hora de llevar a cabo su cometido. El Centro Nacional de Coordinación de Derechos de Propiedad Intelectual (IPR Center) otorgó a DHL Express EE. UU. un premio en reconocimiento a su labor como entidad más activa en la industria de las entregas urgentes y a su estrecha colaboración con el IPR Center en el suministro de datos y apoyo operativo en materia de mercancías falsificadas.

12. Para garantizar la continuidad de la fructífera labor en la lucha contra las infracciones de los DPI, un posible ámbito de cooperación entre las autoridades reguladoras y los proveedores de servicios de transporte urgente consiste en intensificar el flujo de datos sobre los expedidores que no cumplen con la normativa. La coordinación de todas las partes involucradas en la cadena de suministro podría tener una incidencia considerable. Los infractores de los DPI no cesan de adaptar su *modus operandi* para vender y transportar mercancías que no cumplen con la normativa a través de diferentes mercados en Internet y plataformas de redes sociales, distintas rutas de envío, diversos proveedores de servicios de transporte y formas variadas de transporte. Por ende, es esencial velar por una cooperación férrea y un intercambio de información eficaz entre todas las partes interesadas.

IV. RECOMENDACIÓN DE DHL PARA LAS AUTORIDADES REGULADORAS

13. La recomendación para las autoridades es que, en colaboración con los titulares de los derechos, elaboren y mantengan actualizado un listado único de “infractores de los DPI”, al que puedan tener acceso los bancos, las redes sociales, las plataformas de comercio electrónico y los proveedores de servicios de transporte. Esta base de datos permitiría a cada una de las partes interesadas impedir que los infractores de los DPI lleven a cabo actividades comerciales, a través de un esfuerzo coordinado. Con esta base de datos, por ejemplo, DHL Express podría identificar a los infractores de los DPI en sus sistemas internos y bloquear la opción de crear una cuenta, activar la interceptación de envíos y proporcionar más datos e información a las autoridades competentes (siempre y cuando la legislación lo permita).

V. DESAFÍOS

14. Pese a que ya hay varias iniciativas en curso, todavía quedan muchos desafíos pendientes que pueden abordarse de forma conjunta entre el industria y las autoridades reguladoras relevantes, tales como:

² Esta cifra se basa en el artículo de la CBP de los EE. UU. titulado “*Cincinnati CBP Breaks Records in Fiscal Year 2021*” (“La CBP de Cincinnati bate récords en el año fiscal de 2021”), disponible (en inglés) en el siguiente enlace: <https://www.cbp.gov/newsroom/local-media-release/cincinnati-cbp-breaks-records-fiscal-year-2021>.

- No todos los organismos locales encargados del cumplimiento de la ley participan con rigor en la identificación o detención de las mercancías infractoras de los DPI mediante un planteamiento conjunto con DHL Express.
- No todos los titulares de derechos inician los procedimientos establecidos para iniciar las posibles incautaciones de envíos que infringen los DPI a través de los organismos encargados del cumplimiento de la ley.
- Si el intercambio de información limitado por parte de los organismos encargados del cumplimiento de la ley, DHL Express no puede desarrollar un enfoque basado en riesgos para frenar las infracciones de los DPI. He aquí algunos ejemplos en los que se podría mejorar la colaboración para aumentar el éxito de los esfuerzos conjuntos:
 - la comunicación de las incautaciones de forma puntual, periódica y en formato digital que facilite su posterior procesamiento;
 - la incorporación de los datos de la mercancía y de las diferencias con respecto a la factura del expedidor; y
 - la gestión de las autoridades en relación a las mercancías infractoras de los DPI que hayan sido identificadas por DHL Express. Actualmente, la decisión de destruir o devolver el envío está en manos de DHL.
- La inspección a través de rayos X no sirve para identificar las mercancías infractoras de los DPI. Dicha verificación implica la apertura de cada envío para comprobar si contiene alguna mercancía sospechosa de vulnerar la imagen de marca o el derecho de autor. Esta tarea manual exige recursos adicionales y conlleva mucho tiempo. Con el intercambio de datos y la información sobre los mercados de la que disponen las autoridades reguladoras, esta tarea podría aligerarse.
- Los envíos que contienen mercancías sospechosas de infringir los DPI deben someterse a una inspección por parte de las autoridades que podría desembocar en su incautación. El depósito de estos envíos a la espera de los resultados tiene una incidencia negativa en la capacidad de almacenamiento de DHL y la agilización de los tiempos de respuesta reduciría estas exigencias operacionales.
- DHL no es un organismo encargado del cumplimiento de la ley y, por ende, carece de la información y competencia necesarios para detener los envíos.

VI. CONCLUSIÓN: VENTAJAS DE LA COLABORACIÓN PROACTIVA CON LAS AUTORIDADES REGULADORAS PARA TODAS LAS PARTES

15. La observancia efectiva de las infracciones comerciales exige un planteamiento orientado a los riesgos y a la detección de las posibles amenazas, así como la cooperación y el intercambio de información entre las distintas partes interesadas a lo largo de la cadena de suministro, como las autoridades aduaneras y el sector del transporte urgente. Las empresas de transporte urgente no pueden actuar como organismos responsables del cumplimiento de la ley, pero sí pueden adoptar las medidas oportunas a partir de la información facilitada por las autoridades aduaneras con el fin de evitar el incumplimiento de la normativa.

16. DHL Express mantiene un firme compromiso con el cumplimiento de la normativa de comercio y brinda un apoyo continuo a las autoridades de todo el mundo en la lucha contra el comercio ilícito a través de las siguientes acciones:

- cooperación y suministro de datos electrónicos precisos y oportunos sobre los envíos para que las autoridades aduaneras puedan evaluar los riesgos en las fases más tempranas del proceso;
- interceptación y entrega de los envíos físicos que las autoridades aduaneras identifiquen como infractores;

- adopción de medidas contra los expedidores infractores identificados por las autoridades aduaneras; y
- suministro de apoyo e información adicional a las investigaciones principales de las autoridades aduaneras (por ejemplo, datos sobre los expedidores y destinatarios, en caso de que la legislación lo permita).

17. Conforme se ha expuesto en esta contribución, DHL Express va un paso más allá en su compromiso pleno con la lucha preventiva contra las infracciones a través de las siguientes iniciativas:

- cooperación con las autoridades aduaneras;
- puesta en marcha de controles de envíos en el punto de origen, tanto de las mercancías físicas como de la calidad de los datos de los envíos;
- utilización del análisis de datos y el aprendizaje automático para detectar de modo preventivo los envíos que no cumplen con la normativa;
- detención de envíos sospechosos de infracción en la red; y
- cierre de las cuentas de los expedidores infractores.

18. Habida cuenta de todo lo anterior, para DHL Express es fundamental que las autoridades valoren y reconozcan su labor. DHL Express considera que este reconocimiento representa un impulso para proseguir con su labor y llevarla un paso más allá y, asimismo, estima que su tarea redundará en beneficio de las administraciones aduaneras, de otros organismos gubernamentales, de los clientes y de la propia compañía de logística.

19. Por último, es esencial que las autoridades competentes profundicen y mejoren la comunicación directa con los expedidores para que comprendan cuán importante es facilitar datos de alta calidad en los envíos internacionales, y para que sean conscientes de que el incumplimiento de las normativas acarrea consecuencias graves y tangibles.

20. DHL Express está plenamente comprometido con el cumplimiento de la normativa de comercio y recibe con beneplácito cualquier iniciativa de cooperación o la puesta en marcha de proyectos piloto junto con las autoridades aduaneras, otros organismos gubernamentales y actores de la industria para hacer frente al comercio ilícito.

[Fin de la contribución]

INICIATIVAS DE MASTERCARD PARA PREVENIR LAS INFRACCIONES DE LA PROPIEDAD INTELECTUAL

*Contribución preparada por el Sr. Jonathan Trivelas, vicepresidente, Equipo de Rendimiento de la Marca, Relación con los Clientes y Rendimiento, Mastercard International, Adquisiciones, Nueva York (Estados Unidos de América)**

RESUMEN

Mastercard está comprometido en luchar contra las infracciones de la propiedad intelectual (PI) y no tolera el uso de su marca, su red, sus programas o sus servicios para promover actividades ilegales. Cabe mencionar que Mastercard no guarda una relación directa ni asume ningún tipo de responsabilidad sobre los comerciantes que aceptan pagos con tarjetas Mastercard. Más bien, el comerciante suscribe un contrato con una entidad financiera, a la que se denomina adquirente, que es la entidad que mantiene la relación directa con Mastercard como cliente autorizado. Los clientes de Mastercard, sus comerciantes y el resto de participantes de la red deben respetar la legislación vigente, así como las Reglas y otros Estándares de Mastercard.

Mastercard coopera frecuentemente y mantiene una estrecha colaboración con los organismos encargados del cumplimiento de la ley, los titulares de derechos y otras entidades en materia de actividades presuntas ilegales, como las infracciones de la propiedad intelectual. Asimismo, Mastercard cuenta con varios programas y herramientas para ayudar a los adquirentes a prevenir actividades ilegales, como es la Alerta de Mastercard para Controlar a los Comerciantes de Alto Riesgo (MATCH™) y el Proveedor de Monitoreo de Comerciantes (MMP, por sus siglas en inglés).

I. VISIÓN GENERAL DEL PAPEL DE MASTERCARD EN EL ECOSISTEMA DE PAGOS Y EL MODELO CUATRIpartito

1. Mastercard lleva a cabo varias actividades de procesamiento en distintos ámbitos. La actividad principal de Mastercard consiste en la tramitación de pagos a nombre de sus clientes. En esta actividad básica suelen intervenir cuatro partes: Mastercard, las instituciones financieras, los comerciantes y el titular de la tarjeta. Las entidades financieras emiten tarjetas de pago Mastercard a sus clientes, quines pueden ser particulares o empresas (titulares de tarjetas). El banco que expide estas tarjetas se denomina “emisor” o “banco emisor”. Una vez en su posesión, el titular de la tarjeta Mastercard puede utilizarla para efectuar un pago a un comerciante (por ejemplo, una tienda física o en línea). El banco que facilita el pago del emisor del titular de la tarjeta al comerciante se denomina “adquirente” o “banco adquirente”.

2. El titular de la tarjeta mantiene una relación contractual con su emisor o emisores. El comerciante guarda una relación contractual con su adquirente o adquirentes. Tanto los emisores como los adquirentes tienen un contrato con Mastercard que les permite efectuar transacciones de pago en calidad de clientes de Mastercard. Mastercard no establece una relación directa con los comerciantes ni con los titulares de las tarjetas.

* 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.

3. La parte encargada de facilitar los pagos es el adquirente, que recibe la solicitud de pago del comerciante y la envía al emisor del titular de la tarjeta a través de la red Mastercard. En seguida, el adquirente recibe el pago del emisor a través de la red Mastercard y lo ingresa en la cuenta bancaria del comerciante. Los comerciantes deben firmar un contrato con un adquirente para poder aceptar pagos mediante tarjetas Mastercard y son los adquirentes quienes tienen la responsabilidad de conocer a sus comerciantes y supervisar su actividad.

4. Por otro lado, Mastercard fija y actualiza las Reglas y Estándares que rigen todos los aspectos de la actividad de Mastercard, entre cuyos principios fundamentales se encuentra la legalidad. Mastercard no permite el uso de su marca, red, programas o servicios para promover cualquier tipo de actividad ilegal. Los clientes y comerciantes de Mastercard, así como el resto de participantes de la red, están obligados a cumplir con toda la legislación vigente y con las Reglas y Estándares de Mastercard. Mastercard ha puesto en marcha una serie de programas orientados a la identificación de actividades ilegales que exigen acción inmediata si se detecta algún tipo de infracción.

II. INICIATIVAS DE MASTERCARD EN LA LUCHA CONTRA LAS INFRACCIONES DE LA PROPIEDAD INTELECTUAL

A. POLÍTICA ANTIPIRATERÍA DE MASTERCARD

5. La política de Mastercard relativa al comercio en línea de productos que infringen el derecho de autor y de productos de marcas falsificadas (la “Política antipiratería”)²⁸ respalda y se considera conjuntamente con el programa de Mitigación y Evaluación del Riesgo del Negocio de Mastercard. De acuerdo con esta política, Mastercard acepta e investiga las denuncias de entidades encargadas de aplicar la ley y de otras fuentes (es decir, los titulares de derechos y sus representantes autorizados) relacionadas con la venta en Internet de un producto o servicio presuntamente infractor del derecho de autor o de la marca de un tercero.

B. PROGRAMA DE MITIGACIÓN Y EVALUACIÓN DEL RIESGO DEL NEGOCIO

6. El programa de Mitigación y Evaluación del Riesgo del Negocio (BRAM por sus siglas en inglés) se creó en 2005 con el objetivo de investigar y hacer frente a los clientes que llevan a cabo actividades ilegales. Mastercard puede tener conocimiento de una posible infracción a través de la remisión de las entidades encargadas de aplicar la ley, de los titulares de derechos o bien, a raíz de una investigación interna. El equipo del programa BRAM investiga la actividad sospechosa y, en función de sus averiguaciones, puede efectuar una transacción de “rastreo” en el sitio web infractor con miras a confirmar si se aceptan tarjetas Mastercard para los pagos en este sitio web y a determinar la identidad del adquirente o cliente de Mastercard con el que el comerciante efectúa las transacciones.

7. Si se constata que el comerciante podría ser infractor, se notifica a su adquirente. El adquirente debe investigar el asunto, informar a Mastercard de sus conclusiones y confirmar que se ha puesto fin a toda actividad ilegal. Si el adquirente concluye que el comerciante no participaba en ninguna actividad ilegal, debe aportar a Mastercard pruebas contundentes que así lo demuestren. Si se determina que el comerciante ha participado en una actividad ilegal y el adquirente pone fin a su relación contractual con él, el adquirente debe hacerlo figurar en el sistema MATCH (Alerta de Mastercard para Controlar a los Comerciantes de Alto Riesgo). El sistema MATCH es una base de datos en la que figuran los comerciantes

²⁸ Disponible en: <https://www.mastercard.com.mx/content/dam/mccom/es-mx/About%20MasterCard/What%20We%20Do/pdf/anti-piracy-policySPA.pdf>.

que han sido dados de baja por el adquirente por haber infringido las Reglas y Estándares de Mastercard. Una vez concluida la investigación, Mastercard utiliza las evaluaciones de infracciones para desalentar futuros casos de actividad ilegal y para transmitir el mensaje de que la red Mastercard aplica una política de cero tolerancia a las actividades ilegales.

a) Blanqueo de transacciones y otros desafíos

8. El blanqueo de transacciones (también llamado factorización de transacciones o *factoring*) es una táctica habitual que utilizan los comercios inmersos en actividades ilegales para no ser detectados por su adquirente y por Mastercard y que está prohibida según las Reglas y Estándares de Mastercard. El blanqueo de transacciones se produce cuando un comerciante redirige los pagos de una actividad ilegal a través de la cuenta de un comerciante que fue aprobada para otro sitio web. El adquirente, por ende, no tiene conocimiento del sitio web infractor ni del sitio web que procesa los pagos de la actividad ilegal. Por ejemplo, el adquirente aprueba la cuenta de un comerciante para la venta de zapatos a través del sitio web goodshoes.com. Durante el proceso de admisión del comerciante, el adquirente revisa goodshoes.com, confirma que no se ofrecen productos o servicios ilegales y, a continuación, autoriza al comerciante el procesamiento de pagos con tarjetas Mastercard en calidad de zapatería en Internet. No obstante, el comerciante gestiona otro sitio web que vende relojes de lujo falsificados, denominado fakewatches.com, del que el adquirente no tiene constancia. Cuando el titular de una tarjeta hace una compra en fakewatches.com, la transacción se redirige (o se “blanquea”) a través de la cuenta del comerciante configurada para goodshoes.com.

9. Los adquirentes tienen la obligación de cerciorarse de que sus comerciantes no se dedican al blanqueo de transacciones. Mastercard es consciente de que la detección y mitigación de esta actividad puede ser tarea difícil, pero existen varias medidas eficaces, como la utilización de prácticas estrictas de diligencia debida, el control eficaz de las transacciones y las controversias, así como el uso de la tecnología de rastreo de sitios web para supervisar su contenido.

10. Además, Mastercard debe hacer frente al desafío que supone la falta de especialización en materia de derechos de PI, así como la limitación de no ser los propietarios de la PI que se está infringiendo. Por otro lado, Mastercard carece de una relación directa con el comerciante y no dispone de información sobre su titularidad o sus relaciones contractuales con otras entidades. En consecuencia, muchas veces Mastercard no puede concluir con seguridad que un comerciante venda productos que vulneran los derechos de PI sin la confirmación del titular de los derechos de PI o de las entidades encargadas de aplicar la ley.

b) Programa de Supervisión de Comerciantes

11. Hay varios Proveedores de Servicios de Monitoreo de Comerciantes (MMSP, por sus siglas en inglés) que ayudan a los adquirentes a monitorear las actividades ilegales, incluidos los indicios de blanqueo de transacciones. Mastercard creó el Programa de Monitoreo de Comerciantes (MMP) con carácter opcional. A través de este programa, se alienta a los adquirentes a registrar su MMSP con Mastercard y a presentar informes mensuales que confirmen qué URL de los comerciantes son objeto de supervisión para poder acreditarlo frente a una posible evaluación de infracciones. Si el comerciante objeto del monitoreo como parte del MMP fuese detectado en un futuro por Mastercard por participar en actividades ilegales o en una operación de blanqueo de transacciones y el adquirente hubiese cumplido todos los requisitos previstos en el MMP, Mastercard podría conceder una mitigación parcial en las evaluaciones de infracciones pertinentes. Los requisitos son los siguientes: el adquirente debe

registrar el MMSP con Mastercard, el MMSP debe monitorear de forma constante a dichocomerciante y el adquirente o el MMSP deben presentar informes mensuales a Mastercard que demuestren dicho monitoreo, el adquirente debe tomar medidas inmediatas ante la notificación de detección de actividad sospechosa del programa BRAM y el adquirente o el MMSP deben facilitar un informe de incidencias acerca del comerciante identificado.

c) Alianzas

12. Cada año, Mastercard se ocupa de cientos de casos de infracciones de los derechos de PI en los que o bien, se retira el contenido ilegal del sitio web del comerciante, o bien se pone fin a la capacidad del comerciante para aceptar tarjetas Mastercard. El punto fuerte del programa BRAM reside en las alianzas, ya que las vulneraciones de los derechos de PI no siempre son fáciles de identificar y a menudo requieren la confirmación de los propios titulares de los derechos de PI. Mastercard colabora de manera regular con las entidades encargadas de aplicar la ley, como la Real Policía Montada del Canadá y la Policía de la Ciudad de Londres, que validan las denuncias de los consumidores y derivan los casos a Mastercard para la toma de las medidas oportunas. Además, Mastercard colabora asiduamente con grupos de la industria, como la *International Anticounterfeiting Coalition, Inc.* (IACC) y la *Motion Picture Association* (MPA), cuyos miembros son titulares de derechos. A través de estas alianzas, las marcas asociadas a estas entidades pueden trasladar los casos a Mastercard para que los investigue. Además, según se indica en la política antipiratería de Mastercard, los propios titulares de los derechos pueden remitir los casos a Mastercard de forma directa.

C. MATCH™

13. El Alerta de Mastercard para Controlar a los Comerciantes de Alto Riesgo (MATCH™) tiene por objeto brindar a los adquirentes la oportunidad de elaborar y revisar información mejorada o adicional sobre los posibles riesgos antes de suscribir un acuerdo con un comerciante. MATCH es una herramienta que ayuda a los adquirentes a evaluar a los comerciantes que pueden entrañar un riesgo elevado —o a quienes hayan infringido las Reglas y Estándares— durante el proceso de diligencia debida y antes de iniciar una colaboración con ellos, y tiene carácter obligatorio para los adquirentes con licencia de Mastercard, salvo que lo prohíba la legislación local. Cuando un adquirente está considerando autorizar a un comerciante para que acepte tarjetas Mastercard como forma de pago, MATCH puede ayudar al adquirente a saber si el comerciante ha sido cancelado por otro adquirente debido a circunstancias que se ajustan a los criterios del sistema MATCH Add. Los criterios del sistema MATCH Add constituyen una lista de motivos para añadir a un comerciante al sistema MATCH cuando un adquirente da de baja a ese comerciante por haber cometido una infracción de las Reglas y Estándares de Mastercard. Por ejemplo, si se detecta que un comerciante ha efectuado transacciones ilegales, se cumplirían los criterios para exigir al adquirente que añada al comerciante al sistema MATCH mediante el código de motivo correspondiente. Cada código de motivo designa de forma precisa la razón que llevó al comerciante a ingresar en el sistema MATCH, de modo que todo adquirente que consulte el sistema a partir de ese momento tendrá conocimiento de esa actividad previa. Esta información podría incidir en la decisión del adquirente de contratar a este comerciante o de establecer acciones o condiciones concretas para supervisar y mitigar el posible riesgo. No obstante, conviene señalar que MATCH no es una lista negra, ya que los adquirentes no están obligados a descartar a los comerciantes por el hecho de estar incluidos en el sistema MATCH.

III. CONCLUSIÓN

14. Mastercard mantiene un firme compromiso con la lucha contra las infracciones de la PI y con el establecimiento de una red mundial de pagos segura, inteligente y fiable. Mastercard considera que, en esta lucha contra las infracciones de los derechos de PI, es fundamental forjar alianzas de intercambio de información con colectivos de titulares de derechos, redes de pago, entidades encargadas de aplicar la ley y organismos gubernamentales que colaboran en la identificación de infracciones y en la suspensión de la aceptación de tarjetas Mastercard y otros métodos de pago. La clave para poner fin a esta actividad ilegal es la interrupción del flujo de fondos hacia los agentes infractores. Mastercard aguarda con entusiasmo la continuación del debate en torno a la prevención, la detección y la mitigación de las infracciones de la PI y confía en descubrir más formas de entablar nuevas alianzas en este ámbito.

[Fin de la contribución y del documento]