

Comité Asesor sobre Observancia

Decimoséptima sesión
Ginebra, 4 a 6 de febrero de 2025

DESAFÍOS Y BUENAS PRÁCTICAS EN LA PREVENCIÓN DEL USO DE APLICACIONES Y TIENDAS DE APLICACIONES CON EL FIN DE VULNERAR LA PI

*Contribución preparada por el Sr. Antoine Aubert, especialista en PI en el entorno digital, Observatorio Europeo de las Vulneraciones de los Derechos de Propiedad Intelectual (Observatorio de la EUIPO), Oficina de Propiedad Intelectual de la Unión Europea (EUIPO), Alicante (España)**

RESUMEN

En la actualidad, las aplicaciones son una vía de acceso primordial a contenidos y a una amplia gama de servicios que incluyen desde el comercio electrónico hasta los servicios bancarios. Es más, el uso de aplicaciones ha trascendido de los dispositivos móviles a todos los aparatos conectados, como televisores y relojes inteligentes.

La distribución de las aplicaciones suele efectuarse a través de tiendas especializadas, en particular Google Play y la App Store de Apple. Algunos fabricantes de dispositivos y otras empresas han creado sus propias tiendas de aplicaciones. Por otra parte, también es posible descargar e instalar aplicaciones provenientes de plataformas ajenas a las oficiales.

Si bien el creciente uso de aplicaciones y tiendas de aplicaciones redunda en beneficio de consumidores y empresas, este fenómeno también ha dado lugar a su utilización indebida con fines ilegales y fraudulentos, entre ellos las infracciones de la PI.

La presente contribución se fundamenta en un documento de trabajo del Observatorio de la EUIPO en el que se analiza el uso indebido de aplicaciones y tiendas de aplicaciones con fines de vulneración de la PI, los desafíos derivados de este fenómeno y, lo que es más importante,

* 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.

una serie de buenas prácticas para atajar este tipo de usos.¹ Así, se pretende ayudar a las distintas partes interesadas a entender mejor cómo abordar el problema.

I. EVOLUCIÓN DEL PANORAMA DE LAS APLICACIONES

1. En los últimos 15 años, el número de aplicaciones y su uso han experimentado un aumento considerable. En 2023, el gasto de consumo en tiendas de aplicaciones alcanzó los 171 000 millones de dólares de los EE. UU. y los usuarios pasaron más de cinco horas al día en ellas. Ese mismo año, se descargaron 257 000 millones de nuevas aplicaciones, con una media de 489 000 descargas por minuto.²

2. Si bien las aplicaciones se han convertido en una de las herramientas más utilizadas por los usuarios para acceder a un amplio abanico de contenidos y servicios, como el comercio electrónico y la banca, también constituyen una pieza fundamental de las estrategias de las marcas para acercarse a los consumidores. Las aplicaciones han rebasado el ámbito de los aparatos móviles para abarcar otros dispositivos conectados, como los televisores inteligentes, compatibles con la descarga de aplicaciones tanto de los propios fabricantes como de tiendas de terceros. Los televisores pueden ejecutar aplicaciones a través de videoconsolas, receptores HDMI o dispositivos conectables similares. En los últimos años han surgido las superaplicaciones, plataformas capaces de ofrecer en un solo lugar una amplia gama de prestaciones, desde el comercio electrónico a las transferencias monetarias, pasando por los servicios de mensajería, transporte, comunicación y redes sociales. Aunque Asia es el continente donde más se han popularizado estas superaplicaciones, en Europa ya hay versiones “básicas” en proceso de desarrollo.

3. Por lo general, las aplicaciones vienen preinstaladas en los dispositivos conectados o bien están disponibles para su descarga en una tienda de aplicaciones. Como cualquier otro programa informático, las aplicaciones pueden descargarse e instalarse desde fuentes externas a las tiendas autorizadas (lo que se conoce como carga lateral o *sideloading*). Este tipo de aplicaciones están disponibles en el formato de archivo Android Package Kit (APK) a través de diferentes medios, entre ellos sitios web creados expresamente para este fin en los que se ofrece un catálogo y se explica cómo descargar e instalar las aplicaciones. Los archivos APK también pueden compartirse a través de los medios sociales, grupos de mensajería y URL acortadas.

II. USO INDEBIDO DE APLICACIONES Y TIENDAS DE APLICACIONES CON EL FIN DE VULNERAR LA PI

4. Si bien el creciente uso de aplicaciones y tiendas de aplicaciones redundará en beneficio de consumidores y empresas, este fenómeno también ha dado lugar a su utilización indebida con fines ilegales y fraudulentos, entre ellos distintos tipos de infracciones de la PI. A continuación, figuran algunos de estos usos indebidos.

a) Vulneración de los derechos de PI con aplicaciones legítimas. Como ocurre con otros programas informáticos, las aplicaciones pueden ser objeto de copia ilegal, ya sea total o parcial. A menudo, al margen de las tiendas de aplicaciones oficiales, se distribuyen copias

¹ Oficina de Propiedad Intelectual de la Unión Europea, *APPS & APP STORES - Challenges and good practices to prevent the use of apps and app stores for IP infringement activities*, (“APLICACIONES Y TIENDAS DE APLICACIONES - Desafíos y buenas prácticas en la prevención del uso de aplicaciones y tiendas de aplicaciones con fines de vulneración de la PI”). Disponible en: <https://www.euipo.europa.eu/es/publications/apps-app-stores-challenges-and-good-practices>.

² data.ai, *State of Mobile 2024 – The Industry’s Leading Report* (informe de la empresa data.ai sobre las tendencias del mercado de la telefonía móvil). Disponible en: <https://sensortower.com/state-of-mobile-2024>.

pirata de aplicaciones legítimas que suelen utilizarse para la difusión de programas malignos o *adware* (programas que muestran publicidad de forma automática). Por otra parte, también se dan casos de copias o réplicas ilegales de partes protegidas por derechos de PI de aplicaciones conocidas (como el código, la interfaz de usuario y las funcionalidades). En ocasiones, las entidades infractoras de derechos de PI utilizan algunos componentes de aplicaciones que han dado buenos resultados para diseñar otras destinadas a la propagación de programas malignos o *adware*.

- b) Infracción de los derechos de PI de terceros mediante la usurpación de aplicaciones, que consiste en la utilización del nombre protegido o los elementos visuales de una empresa con el fin de inducir a error a los usuarios al hacerles creer que la aplicación pertenece a esa empresa. Como sucede con la ciberocupación, estas prácticas pueden dar una impresión equivocada a los usuarios y dirigir el tráfico hacia aplicaciones fraudulentas, que difunden programas malignos, infringen los derechos de PI, proporcionan acceso a contenidos pirateados o venden productos falsificados, o bien hacia aplicaciones con un doble propósito, es decir, que tienen un uso plenamente legítimo, pero se utilizan de forma principal o exclusiva con el fin de vulnerar la PI.
- c) Uso indebido de aplicaciones legítimas por parte de entidades infractoras de derechos de PI en el contexto de sus actividades ilegales con aplicaciones que permiten la comercialización y el pago de productos y servicios que vulneran la PI, por ejemplo, aplicaciones de medios sociales o de pago y aplicaciones de comunicación y mensajería privadas cuyo uso indebido con el fin de vulnerar la PI tiene por objeto proporcionar información, prestar asistencia o cerrar transacciones.

5. Algunas de estas vulneraciones de la PI no solo perjudican a los titulares de los derechos, sino que, en algunos casos, también se emplean para estafar a los usuarios a través de programas espía propagados mediante aplicaciones de piratería o aplicaciones que suplantan la identidad de una marca legítima para transferir los datos personales del dispositivo y de los usuarios sin su conocimiento ni consentimiento. Asimismo, pueden causar perjuicios a los anunciantes, susceptibles de ser víctimas de fraude en la inserción de sus anuncios al creer que los publican en aplicaciones legítimas cuando, en realidad, son falsas o han sido clonadas.

III. TÉCNICAS UTILIZADAS POR LOS INFRACTORES DE DERECHOS DE PI Y DESAFÍOS EN MATERIA DE OBSERVANCIA

6. Los infractores de derechos de PI recurren a diferentes técnicas al objeto de eludir la detección por parte de las tiendas de aplicaciones, los titulares de derechos y los subsiguientes mecanismos de observancia. Entre ellas se encuentran las aplicaciones encubiertas como juegos y otras que, tras su apariencia legítima, ocultan sus fines ilegales. Las aplicaciones maliciosas también pueden camuflar su código dañino para esquivar los controles de detección de la tienda de aplicaciones mediante el cifrado o la demora de la activación. Asimismo, algunas aplicaciones de piratería han integrado redes privadas virtuales (VPN) con ánimo de ocultar las direcciones IP de los usuarios y burlar los bloqueos o las restricciones por geolocalización.

7. La lucha contra el uso indebido de aplicaciones y tiendas de aplicaciones con el fin de vulnerar la PI plantea una serie de desafíos particulares en materia de control, detección y observancia. Si bien es cierto que algunas tiendas de aplicaciones cuentan con procesos de control para impedir la presencia de aplicaciones fraudulentas e infractoras de derechos de PI, la proliferación de tiendas de aplicaciones de terceros exige una vigilancia más estricta de aquellas cuyos sistemas de supervisión son limitados o inexistentes. Además de las tiendas de aplicaciones, la multiplicación de métodos de descarga e instalación de aplicaciones desde fuentes externas no oficiales expande aún más el espectro de posibilidades de vulneración de

la PI y, por ende, es preciso llevar un seguimiento exhaustivo. En este sentido, conviene vigilar los medios sociales y los foros, ya que son los espacios en los que se comparten los enlaces a los archivos APK.

8. En cuanto a la detección de aplicaciones que infringen los derechos de PI, existen distintos métodos según la funcionalidad de la aplicación y su procedencia. Para determinar si una aplicación vulnera la PI, puede ser necesario que los titulares de los derechos dispongan de los equipos y los programas específicos pertinentes para su instalación e inspección.

9. Con respecto a la observancia de los derechos de PI de las aplicaciones disponibles en las tiendas, aunque se retiren aquellas que infringen los derechos, estas permanecen en los dispositivos de los usuarios y pueden seguir en uso. Como ocurre con otras modalidades de piratería, las aplicaciones infractoras de la PI que se han descargado de fuentes no autorizadas conllevan ciertos desafíos, como la notificación a los proveedores de alojamiento de los archivos APK. Por otra parte, hay proveedores que no acostumbran a responder a las solicitudes de retirada y, en algunos casos, los servicios de alojamiento advierten de que no atienden ese tipo de peticiones bajo ninguna circunstancia.

IV. BUENAS PRÁCTICAS CONTRA EL USO INDEBIDO DE APLICACIONES CON EL FIN DE VULNERAR LA PI

10. Algunas tiendas de aplicaciones, titulares de derechos y autoridades encargadas de velar por la observancia de la ley han puesto en marcha una serie de prácticas orientadas a la prevención del uso indebido de aplicaciones con el fin de vulnerar la PI. La presente contribución tiene su fundamento en un documento de trabajo elaborado antes de febrero de 2024 y de la entrada en vigor plena del Reglamento de Servicios Digitales, habida cuenta de que, en la Unión Europea, parte de las buenas prácticas señaladas pasarían a ser obligaciones reglamentarias o podrían requerir ajustes de conformidad con este nuevo instrumento.

11. El Reglamento establece una serie de directrices relativas a las responsabilidades de intermediarios y plataformas en línea como mercados virtuales, redes sociales, plataformas de intercambio de contenidos y tiendas de aplicaciones. Entre las nuevas reglas figuran la obligación de fijar condiciones claras y de fácil acceso, presentar informes de transparencia, introducir mecanismos de notificación y acción y poner en marcha un sistema de alertadores fiables. Todos los intermediarios en línea que ofrezcan sus servicios en la Unión Europea, tanto si están radicados dentro como fuera de sus fronteras, deben atenerse a lo dispuesto en el Reglamento. La Comisión Europea velará por su observancia en colaboración con las autoridades nacionales, que deberán supervisar su cumplimiento por parte de las plataformas establecidas en su territorio.

Medidas preventivas

12. Numerosas aplicaciones y tiendas de aplicaciones han adoptado medidas contra el uso indebido de sus servicios con fines ilegales o perjudiciales. En las tiendas de aplicaciones, los contratos celebrados con los desarrolladores y las políticas que rigen su actividad contienen disposiciones generales sobre las condiciones que han de reunir las aplicaciones, entre ellas las relativas a la PI.

13. En lo atinente a la infracción de derechos de PI por parte de la propia aplicación, los contratos suscritos con los desarrolladores suelen exigirles garantías de la titularidad de todos los derechos de PI necesarios y la ausencia de vulneración de derechos de PI de terceros. Las políticas de algunas tiendas de aplicaciones van un paso más allá al precisar que no solo se trata de la aplicación en sí, sino también de los metadatos utilizados para describirla (por ejemplo, el uso de una marca protegida en los metadatos de la aplicación), o que quedan

prohibidas las aplicaciones que induzcan a error a los usuarios mediante el uso de iconos, descripciones o títulos que suplanten la identidad de otra empresa o entidad o que tergiversen sin autorización su relación con el titular de una marca.

14. Con respecto a las infracciones de los derechos de PI que puedan derivarse del uso de las aplicaciones, algunas tiendas prohíben las que inducen o alientan la vulneración del derecho de autor o exigen que aquellas que contengan contenidos generados por los usuarios adopten medidas de filtrado, notificación y bloqueo de contenidos y usuarios objetables. En lo referente a las aplicaciones de inteligencia artificial (IA) generativa, algunas tiendas de aplicaciones establecen que deben incluir funciones que permitan a los usuarios denunciar contenidos que puedan ser ofensivos o ilegales, entre ellos los que vulneren los derechos de PI, así como utilizar esas denuncias para “mejorar el filtrado y la moderación de los contenidos” de sus aplicaciones.

15. Las políticas de algunas tiendas de aplicaciones también especifican las sanciones a las que pueden enfrentarse los desarrolladores en caso de incumplimiento, como la retirada o la suspensión de la aplicación y, en algunos casos, la rescisión de su cuenta de desarrollador.

16. Como parte del proceso de creación de una cuenta de desarrollador de aplicaciones, las tiendas suelen pedir distintos datos identificativos y de verificación de la legitimidad de las empresas y particulares que publican aplicaciones en sus plataformas. Aunque algunas tiendas de aplicaciones ya habían impuesto este tipo de requisitos por iniciativa propia, el Reglamento ha pasado a hacerlos obligatorios en la Unión Europea, con criterios pormenorizados que han de cumplirse al objeto de garantizar la trazabilidad de los comerciantes.³

17. Una vez creada una cuenta de desarrollador, las tiendas de aplicaciones examinan las aplicaciones propuestas antes de ponerlas a disposición de los usuarios. Este proceso consiste en revisar el modelo de negocio de la aplicación, sus prestaciones técnicas (incluidas las autorizaciones necesarias), su diseño, su contenido y sus aspectos relativos a la privacidad. Además, algunas tiendas de aplicaciones efectúan comprobaciones específicas de las aplicaciones instaladas desde otras tiendas o directamente desde Internet. Estos controles tienen por objeto detectar aplicaciones maliciosas e ilegales, entre ellas las que vulneran la PI, y pueden llevarse a cabo tantas veces como cambios o actualizaciones efectúe el desarrollador antes, durante y después de la publicación de la aplicación.

MEDIDAS DE RESPUESTA

18. Algunas tiendas de aplicaciones han puesto en marcha medidas para tramitar y dar curso a las reclamaciones de usuarios y titulares de derechos en materia de PI. Entre otras, cabe destacar los mecanismos de notificación y acción, mediante los que los usuarios y las partes interesadas, como los titulares de derechos de PI, pueden avisar sobre la existencia de aplicaciones o contenidos que contravengan la legislación correspondiente o las políticas de las tiendas de aplicaciones para que estas emprendan las acciones oportunas. Algunas tiendas de aplicaciones han habilitado procesos guiados de notificación a través de formularios web en aras de la simplificación y la agilización de los trámites. Los formularios de relleno automático y las instrucciones facilitan el envío de notificaciones sobre distintos tipos de vulneraciones de los derechos de PI.

19. Asimismo, hay tiendas de aplicaciones que emiten mensajes de advertencia sobre aplicaciones potencialmente maliciosas que están a punto de instalarse o que se han descargado en el mismo dispositivo desde otras fuentes (por ejemplo, las que proceden de medios no autorizados ajenos a las tiendas de aplicaciones autorizadas). Estos avisos se

³ Véase el artículo 30 del Reglamento de Servicios Digitales. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022R2065>.

generan de forma automática para informar al usuario del motivo de la alerta a partir de una lista predeterminada en la que se recogen distintos tipos de fraude, programas malignos, correo basura y actividades de suplantación de identidad que puedan perjudicar a los usuarios o a sus dispositivos. El funcionamiento de estos sistemas es similar al de los programas antivirus. Si bien su objetivo no está vinculado de forma estricta con las infracciones de los derechos de PI, sí impiden la instalación y el uso de aplicaciones que los vulneran y que participan en prácticas fraudulentas en detrimento de los usuarios y los anunciantes.

20. Ante el auge de la publicidad dentro de las aplicaciones (en 2024, el gasto previsto en este tipo de anuncios a escala mundial rondaba los 322 000 millones de euros),⁴ algunas entidades que cometen vulneraciones de los derechos de PI monetizan sus actividades ilegales mediante el fraude a los anunciantes con aplicaciones falsas o pirateadas creadas con el único propósito de insertar anuncios, mostrarlos o cometer fraude de clics. También hay quienes sacan rédito económico de su audiencia con aplicaciones de piratería en las que se muestran anuncios. Además de suponer una fuente de ingresos para los infractores de derechos de PI, la presencia de publicidad de marcas legítimas en aplicaciones que los vulneran puede llevar a los consumidores a la creencia errónea de que esas aplicaciones proporcionan acceso a contenidos, productos o servicios legales.⁵

21. En este sentido, hay una serie de buenas prácticas orientadas a atajar la monetización de las aplicaciones de piratería a través de la publicidad de marca. Es el caso del Memorando de Entendimiento de la Comisión Europea sobre publicidad en línea y derechos de PI,⁶ suscrito en 2018 por las partes interesadas en la inserción, compra, venta y facilitación de publicidad. En virtud de este acuerdo, las partes se comprometen a reducir al mínimo la inserción de publicidad en sitios web y aplicaciones móviles que vulneren los derechos de PI, con miras a privarlos de los flujos de ingresos necesarios para que sus actividades sean rentables. Del mismo modo, el Trustworthy Accountability Group (TAG) puso en marcha la herramienta TAG Pirate Mobile App Tool para ayudar a sus miembros a evitar que su publicidad figure en aplicaciones conocidas por la distribución de contenidos pirateados.⁷

V. CONCLUSIÓN

22. El creciente uso de aplicaciones y tiendas de aplicaciones entraña multitud de ventajas para consumidores y empresas y, al igual que sucedió en su día con los sitios web, estas se han convertido en un instrumento esencial de interacción entre las marcas y los usuarios. No obstante, al igual que la mayoría de los nuevos avances digitales, las aplicaciones y sus tiendas también son objeto de uso indebido con fines ilegales y fraudulentos, entre ellos las infracciones de la PI. En este abanico de usos indebidos figuran varias tendencias que no solo perjudican a los titulares de derechos, sino también a los usuarios, que quedan expuestos a amenazas a la ciberseguridad, así como a los anunciantes, que son víctimas de nuevas técnicas de fraude publicitario.

⁴ Statista, "In-App Advertising – Worldwide" ("La publicidad dentro de las aplicaciones – Perspectiva mundial"). Disponible en: <https://www.statista.com/outlook/amo/advertising/in-app-advertising/worldwide>.

⁵ Véase: Oficina de Propiedad Intelectual de la Unión Europea, *Online advertising on IPR-Infringing Websites and Apps* ("Publicidad en línea en sitios web y aplicaciones que vulneran los derechos de PI"), pág. 7. Disponible en: <https://www.euipo.europa.eu/es/publications/online-advertising-on-ipr-infringing-websites-and-apps>.

⁶ Véase: https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/enforcement-intellectual-property-rights/memorandum-understanding-online-advertising-and-ipr_en.

⁷ El Grupo de Trabajo Antipiratería del TAG ha recopilado una serie de recomendaciones de buenas prácticas al objeto de ayudar a los anunciantes, las agencias y los intermediarios del ámbito de la tecnología publicitaria en dispositivos móviles a detectar y retirar de sus inventarios publicitarios las aplicaciones móviles que infrinjan los derechos de PI.

23. Las buenas prácticas descritas en la presente contribución tienen por objeto contribuir a su aplicación general y ofrecer una visión más clara de las medidas susceptibles de impedir el uso indebido de las aplicaciones y las tiendas de aplicaciones con el fin de vulnerar los derechos de PI, más allá de los nuevos requisitos reglamentarios establecidos a escala comunitaria.

[Fin del documento]