Falsificación y robo de propiedad intelectual

PID_00270254

Thomas Holt

Tiempo mínimo de dedicación recomendado: 2 horas

Universitat Oberta de Catalunya

Thomas Holt

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por el profesor: Marc Balcells Magrans (2019)

Primera edición: septiembre 2019

Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Índice

Introducción

La aparición de los ordenadores e internet cambió la forma en que nos comunicamos en todo el mundo. Al mismo tiempo, también influyó directamente en cómo adquirimos y disfrutamos medios como la música, la televisión, el cine y la prensa. El desarrollo de servicios de transmisión de música, como Pandora, Spotify y Tidal, permite a los usuarios compartir listas de reproducción y disfrutar de catálogos completos de artistas y estilos de música. Del mismo modo, el desarrollo de Netflix, YouTube, HBO Go y DisneyNow proporciona herramientas fáciles que permiten a sus usuarios ver horas de películas y contenido de televisión en cualquier momento (Brown y Holt, 2018).

La tecnología también afectó directamente a nuestra capacidad de comprar y consumir medios y bienes físicos tradicionales. Servicios como iTunes permiten comprar prácticamente cualquier tipo de medio y descargarlo directamente en múltiples dispositivos, o transmitirlo desde su biblioteca de compras (Brown y Holt, 2018). Amazon y Alibaba también proporcionan acceso a productos de todo el mundo, incluidos alimentos, ropa y bienes duraderos, como piezas de automóviles y electrodomésticos. De la misma manera, sitios como Etsy constituyen una plataforma para que los productos artesanales lleguen a un mercado global, lo que, en cambio, no sería posible en el espacio físico (Brown y Holt, 2018).

Todos estos servicios reflejan un cambio en la manera en que nosotros, como consumidores, podemos obtener acceso a bienes producidos tanto por individuos como por corporaciones multinacionales. La facilidad de acceso que ofrece la tecnología también ha creado oportunidades únicas para que los delincuentes aprovechen estos recursos y así beneficiarse de los productos e ideas de otros. De hecho, la tipología de Wall (2001) de engaño cibernético y robo reconoce actos de fraude que suponen el uso y el uso indebido de la tecnología para adquirir bienes y servicios gratuitamente, o aprovechar y beneficiarse de las ideas y ganancias de otros. Esto puede abarcar actividades como la piratería digital o la copia de medios digitales como grabaciones de sonido o vídeo, software y otros archivos sin que medie la autorización o el pago al propietario de los derechos de autor (Gunter, 2009; Higgins y Marcum, 2011; Skinner y Fream, 1997). Asimismo, la gente puede beneficiarse de la venta de ropa, joyas y otros productos que parecen ser de fabricantes específicos, sobre todo marcas de lujo, y que en realidad fueron fabricados por otros. Este capítulo permitirá profundizar en el uso de la tecnología para robar ideas, bienes y servicios, así como comprender a los que participan en estas actividades, ya sea como productores o como consumidores.

1. Propiedad intelectual y protección legal

El diseño y el paso de una idea a un producto o artículo físico son una práctica importante, que se ha convertido en un producto legalmente protegido y con un claro valor económico que puede variar según el lugar. Ya se trate de una obra de arte o de una obra creativa como una pieza musical, dicha idea posee un valor en sí misma que además puede generar ganancias con el tiempo. Una vez la idea se manifiesta, ya sea al escribirla, al pintarla o al colocarla en cualquier tipo de medio fijo, se convierte en propiedad intelectual, ya que su creación se puede asociar a una persona o grupo específico y otros pueden verla (Brown y Holt, 2018; Holt, Bossler y Seigfried-Spellar, 2017).

Si una persona desea proteger las ideas y el material que ha hecho y asegurarse de recibir todos los derechos y créditos de su creación, existen diferentes marcos legales a los que acogerse. Dependiendo de la ubicación de una persona, se pueden solicitar derechos de autor, marcas registradas y patentes, que proporcionan diferentes protecciones legales de propiedad intelectual, diseños y derechos de propiedad y pagos por períodos específicos de tiempo. Por ejemplo, las corporaciones y las empresas pueden solicitar marcas registradas que garanticen que sus logotipos y su imagen corporativa estén vinculados a productos específicos y no puedan ser utilizados por nadie más.

De la misma manera, el derecho de autor es una medida de protección legal que vincula a una persona o personas con una obra artística de algún tipo tan pronto como se escribe, graba o imprime (Yar, 2013). Los derechos de autor son particularmente importantes, ya que establecen la propiedad y las obligaciones financieras para con el propietario y pueden aplicarse en varios países, especialmente en toda la UE. Según la legislación de Estados Unidos, las personas pueden recibir derechos de autor desde el momento en que se crea la obra en cuestión. Sin embargo, están obligados a registrar estos derechos de autor con el Gobierno estadounidense para obtener todas las protecciones legales necesarias. De lo contrario, el individuo no puede emprender acciones civiles o penales contra otros que usan sus ideas u obras porque no es un material reconocido bajo la protección legal de EE. UU. (Holt y otros, 2017).

La capacidad de acceder y compartir ideas a grandes distancias por medios tecnológicos ha desafiado radicalmente los procesos establecidos de derechos de propiedad intelectual y titularidad en todo el mundo. La gente puede observar una idea, diseño o producto en línea e intentar hacerlo por sí misma o venderlo sin contactar con el creador. También puede encontrar un medio y luego intentar reproducirlo y posiblemente distribuirlo a otros sin el permiso del propietario o titular de los derechos de autor.

Por ejemplo, grabar una pieza musical o un clip de televisión en su teléfono y luego publicarlo en YouTube es una forma de robo de propiedad intelectual, ya que el titular original de los derechos de autor no será reembolsado por el uso de su creación.

Como resultado, la tecnología ha simplificado y globalizado nuestra capacidad de infringir los titulares de derechos de autor y creadores de contenido con un riesgo mínimo de detección.

2. Piratería digital y robo de propiedad intelectual

Como se señaló anteriormente, la distribución y el robo de medios digitales son un problema en la era digital. De hecho, grupos antipiratería como Business Software Alliance (BSA) estiman que el 39 % del software utilizado en todo el mundo está pirateado de diferentes fuentes. El software pirateado puede encontrarse en Gobiernos y sistemas comerciales, sobre todo en países de bajos ingresos donde el coste de estos productos puede resultar prohibitivo. Como resultado, las estimaciones sugieren que muchos países de Asia, Europa Central y Oriental y América Latina tienen tasas de piratería más altas que otras partes del mundo (BSA, 2016). Esto no significa que Estados Unidos y otros países no participen en la piratería.

> De hecho, la Marina de Estados Unidos fue objeto de una demanda presentada por Bitmanagement Software, que afirmó que más de 558.000 copias de su software de realidad virtual 3D se estaban utilizando sin la licencia correcta (Kravets, 2016). Aunque no está claro cómo se cerrará el caso, la compañía afirmó que tenía derecho a más de 600 millones de dólares en honorarios y daños debido a la pérdida de ingresos.

Cabe señalar que la piratería existía antes del desarrollo de internet, aunque siempre ha tenido una relación simbiótica con la tecnología en cualquier forma.

> Por ejemplo, el desarrollo de equipos de grabación de audio y vídeo para el usuario doméstico en la década de 1960 y su coste cada vez menor hicieron posible que las personas grabaran programas de música y televisión mientras se reproducían. De hecho, los llamados *mixtapes* de los años ochenta son el resultado directo de que los consumidores pudieran grabar cualquier grabación de audio, incluso si se escuchaba en directo en la radio, añadir distintas piezas de música de diferentes artistas y grabar etiquetas en un solo casete (Nhan, 2013).

El crecimiento del mercado de PC en la década de 1980 y la popularidad de los videojuegos condujeron también a las primeras formas de piratería de software. En aquel momento, las protecciones en el software para evitar copias eran relativamente simples.

> Por ejemplo, el uso de claves de producto, que consiste en una cadena de código alfanumérico, podía engañarse con cierta facilidad, lo que permitía copiar una pieza de software. Las técnicas para quebrantar estos sistemas de protección se compartían con frecuencia entre los *hackers* y luego en línea a través de *Bulletin Board Systems* (BBS) y foros (Meyer, 1989).

En reconocimiento de sus habilidades, en los ochenta algunos usaron el término *warez doodz* para referirse a aquellos *hackers* que podían traspasar las protecciones de software (*wares*) (Cooper y Harrison, 2001).

El desarrollo y la rápida aceptación de la tecnología de discos compactos, o CD, en los años noventa también influyeron mucho en la piratería de medios en general. El uso de cintas de casete y discos de vinilo era atractivo para los consumidores, pero suponía un formato analógico en el que las ondas de sonido producidas por los músicos se copiaban y reproducían de igual modo en

un formato de almacenamiento de medios extraíble, como la cinta magnética de un casete. Un formato analógico reproduce distintos tonos y sonidos que pueden resultar agradables al oyente, pero no es lo mismo que se escucharía y grabaría en formato digital. Concretamente, los CD permitieron a las discográficas tratar las ondas de sonido de los músicos como datos binarios almacenables electrónicamente en un CD. Estos medios digitales ofrecen al oyente un sonido mejor y a un precio mucho más bajo en comparación con los medios tradicionales.

Conforme el formato de CD iba siendo ampliamente aceptado, otra innovación tecnológica transformó aún más la propiedad intelectual digital. En 1996 se desarrolló un nuevo formato de software para comprimir archivos de audio y multimedia, lo que permite que los archivos grandes sean lo suficientemente pequeños como para compartirlos a través de conexiones a internet (Holt y otros, 2017). Dadas las velocidades de conexión de acceso telefónico a internet relativamente lentas de mediados de los noventa, las organizaciones de medios y las compañías tecnológicas se interesaron en encontrar otra manera de transferir la propiedad intelectual digital de manera rápida y eficiente. El formato de compresión MP3, entonces, se desarrolló con la colaboración entre el Motion Picture Experts Group (MPEG) y la Organización Internacional de Normalización (International Organization for Standardization, o ISO) (Holt y otros, 2017).

El formato MP3 se convirtió rápidamente en el estándar de la industria para el formato de compresión de medios, y todavía se usa y sirve como modelo para la gestión de archivos en la actualidad. De hecho, el lanzamiento del formato MP3 condujo muy pronto a la producción de dispositivos que podrían usarse específicamente con este tipo de medios.

> Por ejemplo, la herramienta de software Winamp para ordenadores de mesa permitió que los usuarios escucharan archivos MP3 en cualquier momento.

Los dispositivos de reproducción portátiles también se desarrollaron y produjeron para la venta al por menor en 1999. Estas tecnologías también posibilitaron copiar música de sus CD a su PC, por lo que el aumento de las unidades de CD que podían leer y escribir en este formato hizo posible crear *mixtapes* en CD.

Como consecuencia, el formato MP3 mejoró la gestión de la propiedad intelectual y simplificó la piratería en todo el mundo.

> Por ejemplo, las redes de piratería pasaron de almacenar grandes cantidades de material en servidores individuales o repositorios de sitios web para su descarga, a métodos de red más distribuidos para minimizar el riesgo de identificación por parte de la policía (Cooper y Harrison, 2001).

Los *hackers* comenzaron a crear protocolos de intercambio de archivos entre pares (P2P) que permitían compartir archivos a través de redes por medio de sistemas individuales. Esto se debe en parte a Internet Relay Chat, o IRC, una forma de mensajería instantánea establecida en 1998 que funcionaba en parte

aislada de internet y que está dividida en salas de chat establecidas y administradas por varias personas. Las comunidades de piratas informáticos adoptaron rápidamente IRC como un cliente de comunicaciones distribuidas y un mecanismo para compartir software, juegos y música (Cooper y Harrison, 2001), así como herramientas y datos de hackeo (Franklin y otros, 2007). En concreto, los individuos podían entrar en un canal, solicitar contenido y negociar intercambios de material (Cooper y Harrison, 2001).

La naturaleza técnica de IRC limitó su popularidad como plataforma de piratería en comparación con servicios P2P más fáciles de usar, como Napster, disponible a partir de 1999 (Nhan, 2013).

Napster

Napster era un programa de software gratuito que conectaba sistemas de usuarios a través de los servidores corporativos de Napster e indexaba archivos específicos designados para compartir archivos codificados en MP3. A su vez, los usuarios podían buscar medios por nombre y descargar los archivos de otros ordenadores rápidamente. Si bien las velocidades de descarga variaron según el tipo de conexión disponible para el usuario, esto permitió optimizar el proceso de identificación de archivos y materiales piratas de manera más eficiente (Nhan, 2013).

La cantidad de archivos compartidos a través del software de Napster hizo que varios artistas y compañías discográficas se dieran cuenta. Después de solo dos años en funcionamiento, Napster fue demandado por la banda Metallica y A&M Records en 2001, quienes afirmaron que el sitio les causó graves daños económicos al posibilitar que se compartiera su propiedad intelectual gratis (McCourt y Burkart, 2003). Napster fue objeto de duras críticas en los medios tras estas demandas, y finalmente puso fin a su servicio gratuito de intercambio de archivos P2P a favor de un modelo de pago que garantizaría una retribución justa a los artistas de grabación. La popularidad de Napster disminuyó rápidamente conforme los usuarios se trasladaron a otros servicios P2P gratuitos, como LimeWire y Kazaa, con una infraestructura similar para facilitar la piratería.

El desarrollo de discos de vídeo digital o DVD en 1996 supuso una transformación similar en la piratería de cine y televisión. La producción de DVD y la posterior tecnología Blu-ray se volvió más fácil con la creación del formato MPEG, que combinaba digitalización y compresión de vídeo y audio en un solo paquete. La primera copia de formato MPEG se hizo pública en 1993, aunque con el tiempo ha sufrido numerosos cambios que mejoraron la calidad de los archivos de sonido y audio. Además, el formato MPEG permitió que los titulares de propiedad intelectual implementaran la protección de gestión de derechos digitales (*Digital Rights Management*, o DRM) para reducir la probabilidad de que los consumidores copiaran el contenido en discos duros y otros dispositivos. Los *hackers* hallaron muchas soluciones para traspasar las protecciones DRM, incluidos los programas de software simples que permitirían a los usuarios copiar directamente el contenido de DVD a un DVD en blanco (Karagiannis y otros, 2004).

Conforme la tecnología de discos y reproductores de DVD comenzó a expandirse en todo el mundo a finales de los años noventa y principios del siglo XXI, el formato digital permitió a los piratas encontrar nuevas formas de compartir

audio y vídeo de alta calidad a través de internet. Además, comenzaron a surgir nuevas plataformas para la piratería, en particular el *torrenting*, estrechamente relacionada con BitTorrent.

BitTorrent

El uso de *torrents* implica un programa de software especial que permite a los usuarios rastrear y administrar la carga y descarga de archivos desde una enorme red distribuida de otros usuarios de *torrents*. El software indexa los archivos disponibles en los sistemas de usuario, de manera similar a Napster y otros programas P2P, pero luego descarga simultáneamente el archivo de otros usuarios en pequeños fragmentos. El programa *torrent* vuelve a unir los componentes en un único archivo utilizable que puede reproducirse. Este software garantiza descargas rápidas y distribuidas, lo que hace más difícil detener las redes de piratería, ya que ahora existen múltiples maneras de descargar archivos. El software de *torrent* se convirtió en un método extremadamente popular para la piratería, por lo que algunos sugirieron que fue la fuente de más de la mitad de todos los materiales pirateados en línea en 2004 (Pouwelse, Garbacki, Epema y Sips, 2005).

A medida que los servicios de transmisión de medios ganaron mayor popularidad a mediados y finales de la década de 2000, existen algunas pruebas de que los *hackers* han ido cambiando de nuevo sus métodos para obtener contenido de manera ilegal (MUSO, 2016). La proliferación de servicios que van desde YouTube hasta Spotify y Netflix permite a los usuarios el acceso directo a toda una gama de propiedad intelectual con costes variables dependiendo de la suscripción seleccionada. La accesibilidad de estos servicios ha llevado a algunos piratas a comenzar a «extraer» o copiar contenido conforme se reproduce en la plataforma del proveedor de servicios. A su vez, estos *hackers* usan dicho contenido o lo comparten con la comunidad en general mediante servicios de *streaming* de contenido pirateado (MUSO, 2016). De hecho, hubo más de 190.000 millones de visitas a sitios web de piratería en 2018, el 60 % de las cuales fueron a plataformas de *streaming* (Stokel-Walker, 2019). Estas estadísticas llevaron a algunos a sugerir que a medida que los servicios de *streaming* aumentan en número y cambian sus modelos de precios, es más probable que sufran pérdidas económicas por el aumento de piratas que ofrecen acceso a su contenido (Stokel-Walker, 2019). Por lo tanto, la piratería y la tecnología tienen una relación simbiótica que continuará evolucionando en el futuro.

3. Comprender quiénes piratean los medios y la propiedad intelectual

La naturaleza cambiante de las prácticas de piratería digital y la probabilidad de que alguien pueda descargar o compartir contenido pirateado invita a cuestionar quién es proclive a piratear contenido.

Las estadísticas sugieren que la mayoría de las personas en todo el mundo han participado en la piratería en algún momento, aunque está menos claro si existen diferencias en los factores de comportamiento o actitud que influyan en el uso constante de contenido pirateado.

Los resultados de la investigación criminológica sugieren que los primeros actos de piratería forman parte en gran medida de un proceso de aprendizaje social, ya que se aprende a piratear materiales de otros (Higgins y Marcum, 2011; Holt y Copes, 2010). Las relaciones con otros *hackers* pueden provenir de interacciones en el mundo real (Higgins y Marcum, 2011; Hinduja e Ingram, 2008, Holt, Bossler y May, 2012), así como en espacios virtuales como foros y redes sociales (Miller y Morris, 2014). Estas relaciones las pueden constituir amigos, padres o incluso tutoriales publicados en línea con los que el usuario interactúa para obtener información sobre el proceso de piratería (Burruss, Holt y Bossler, 2013; Miller y Morris, 2014). Asimismo, dichas relaciones ofrecen información sobre los mejores lugares para piratear contenido y cómo se puede justificar este comportamiento delictivo ante otros.

El conocimiento técnico requerido para participar en algunas formas de piratería supone una barrera inicial que requiere cierto grado de intercambio de información con sus compañeros o lazos sociales para poder superarla (Hinduja, 2003; Holt y Copes, 2010; Holt, Burruss y Bossler, 2010; Ingram e Hinduja, 2008; Skinner y Fream, 1997). Una vez que un individuo se ha iniciado en la piratería, la importancia de los lazos sociales puede disminuir a la hora de identificar diferentes estrategias para descargar materiales de otros sitios (Holt y Copes, 2010).

La investigación también demuestra que las personas que piratean tienden a mantener creencias y actitudes que respaldan su violación de los derechos y las leyes de propiedad intelectual, lo que les permite continuar participando en comportamientos ilegales (Brown, 2016; Higgins y Marcum, 2011; Ingram e Hinduja, 2008; Skinner y Fream, 1997).

Por ejemplo, aquellos que descargan música suelen pensar que sus acciones tienen un escaso daño económico para los titulares y creadores de derechos de autor (Brown, 2016; Higgins y Marcum, 2011; Ingram e Hinduja, 2008; Ulsperger, Hodges y Paul, 2010). Aquellos que piratean videojuegos suelen argumentar que sus acciones ayudan a mantener

el interés del público en las consolas de juegos retro o de la «vieja escuela», que de otro modo quedarían obsoletas (Downing, 2011). Otros sugieren que piratean solo para identificar nuevos artistas o creadores de medios y determinar si les gustan sus ideas antes de invertir dinero en su música o sus películas (véase, por ejemplo, Holt y Copes, 2010). A este respecto, la piratería puede ser una forma de probar contenido antes de pagar álbumes o temporadas de programas de televisión. Otros también culpan a los productores de medios por cobrar demasiado por sus productos, por lo que adquirir legalmente todos los medios que se querrían consumir resultaría demasiado caro (Higgins y Marcum, 2011; Holt y Copes, 2010; Ulsperger y otros, 2010). Parte de los *hackers* también sugiere que descargan contenido porque no existe un conjunto inherente de conductas éticas que puedan orientar las actividades en línea, por lo que es posible hacer lo que uno quiere independientemente de la ley (Higgins y Marcum, 2011; Ulsperger y otros, 2010).

Otro factor claramente asociado con la piratería digital es el nivel de autocontrol de un individuo, o la capacidad de regular su propio comportamiento ante la oportunidad de infringir la ley (Gottfredson y Hirschi, 1990). Las personas con poco autocontrol son cortas de miras, impulsivas, asumen riesgos y tienen menos probabilidades de sentir empatía hacia sus víctimas. Esto se alinea bastante bien con la piratería digital, ya que los materiales pirateados se encuentran en un enorme suministro relativamente fácil de adquirir y requiere poca habilidad técnica en general, al mismo tiempo que proporciona una satisfacción inmediata para los descargadores, que pueden compartir su sentido de la responsabilidad en sus acciones ilegales. Esto está respaldado por la literatura existente sobre el tema, pues los estudios reflejan que las personas con bajo autocontrol son consistentemente más propensas a participar en la piratería, ya sea en muestras juveniles o adultas (Higgins y Marcum, 2011; Holt y otros, 2013).

Estos factores pueden explicar las dificultades inherentes a detener la piratería a nivel mundial. Si bien existen sanciones civiles y penales por piratería, a muchas personas que descargan propiedad intelectual no les preocupan, por lo general, las sanciones formales de la policía (Al-Rafee y Cronan, 2006; Holt y Copes, 2010). Esto puede deberse a que las personas consideran que la piratería digital es diferente al robo físico en tiendas y supermercados (Downing, 2011; Holt y Copes, 2010). De hecho, una de las únicas formas de disuadir potencialmente la piratería es destacar el hecho de que los archivos descargados puedan contener software malicioso (Wolf, Higgins y Marcum, 2008). De lo contrario, las intervenciones formales para minimizar la piratería son generalmente ineficaces (Nhan, 2013). Por lo tanto, es probable que la piratería digital persista mientras exista internet.

4. La falsificación e internet

Otra forma de robo de propiedad intelectual implica aquella producción y venta de bienes que utilizan fraudulentamente diseños con derechos de autor o logotipos y envases de marcas registradas sin devolver las ganancias al propietario original, lo que generalmente se conoce como falsificación (Wall y Large, 2010).

Prácticamente cualquier producto puede ser falsificado, ya sea alimentario, farmacéutico o de ropa, aunque en general están hechos de materiales de menor calidad (Wall y Large, 2010). Al igual que la piratería, los productos falsificados se pueden distribuir y vender sin internet, y así ha sido a lo largo de la historia (Chaudry y Zimmerman, 2009). De hecho, los productos falsificados quedan a menudo ocultos en la cadena superior de distribución de productos legítimos y puede ser difícil distinguirlos de los artículos originales (Kennedy, 2016). Estimaciones recientes sugieren que los falsificadores pueden haber ganado 200.000 millones de dólares a nivel mundial por la venta de productos farmacéuticos ilícitos (Sophic Capital, 2015).

Algunas entidades están directamente perjudicadas por la creación y venta de productos falsificados. En primer lugar, aquel que compra productos falsificados puede perder dinero si el producto no funciona o no es efectivo para tratar enfermedades específicas en el caso de productos farmacéuticos y sanitarios. Además, algunos consumidores han sufrido lesiones físicas tras utilizar productos hechos con materiales de peor calidad, como se observó cuando las baterías falsificadas (Fagioli, 2017) y los cigarrillos electrónicos (Saxena y otros, 2018) prendieron fuego y explotaron. Del mismo modo, medicamentos falsificados han causado lesiones graves e incluso la muerte a algunos de quienes los han ingerido (Kennedy y otros, 2018).

Los propietarios de marcas encargados de producir productos originales también pierden dinero y participación en el mercado a medida que las compras son absorbidas por falsificadores (Commuri, 2009). En algunos casos, los reclamos de falsificación también pueden llevar a que los fabricantes legítimos reemplacen los productos afectados y minimicen la atención negativa de la prensa. Más allá de estas pérdidas directas, la falsificación supone para los fabricantes legítimos gastos de millones de dólares y mano de obra para identificar productos falsificados en la cadena de suministro y evitar así que lleguen a los consumidores (Commuri, 2009). Además, se ven obligados a gastar dinero en abogados y honorarios legales para hacer cumplir las patentes y los reclamos de marcas comerciales que puedan tener en varios países y poder reducir la producción de falsificaciones (US Government Accountability Office,

2010). De hecho, algunos estiman que los gastos asociados a la falsificación para la comunidad empresarial alcanzan los cientos de miles de millones cada año (BASCAP, 2011; US Government Accountability Office, 2010).

El auge de los sitios web de comercio electrónico, correo electrónico y redes sociales simplificó el proceso de publicidad y venta de productos directamente a los consumidores con menor riesgo de detección por parte de las fuerzas del orden o del titular de la propiedad intelectual (Kennedy y otros, 2018; Wall y Large, 2010). Además, internet permite obtener acceso al mercado global de productos independientemente de la ubicación del comprador en el espacio físico. Las diferencias geográficas en las leyes relacionadas con las protecciones de propiedad intelectual hacen posible que los productos falsificados se adquieran de manera más inmediata a través de sitios web de comercio electrónico.

> Por ejemplo, Estados Unidos ofrece protección legal a la primera empresa que demuestra haber utilizado una marca comercial en la práctica, mientras que naciones como China protegen a la primera empresa que presente una marca comercial u otros documentos legales ante agencias gubernamentales (Kennedy y otros, 2018). Como consecuencia, un producto puede ser falsificado en un país y estar protegido legalmente en otro, aunque en ambos casos pueden adquirirse a través de minoristas en línea.

Estas dinámicas explicarían la gran cantidad de productos falsificados que la policía confisca cada año (US Government Accounting Office, 2018). El Departamento de Seguridad Nacional de los Estados Unidos (Department of Homeland Security, o DHS) aseguró haber confiscado más de 34.000 envíos de productos falsificados que llegaron a Estados Unidos desde puertos extranjeros (US Department of Homeland Security, 2018). Del mismo modo, la Organización para la Cooperación y el Desarrollo Económico (OCDE) informó de que más de 461.000 millones de dólares en bienes importados a Estados Unidos eran falsos, incluidos los productos falsificados que infringían directamente las marcas registradas, las patentes y los derechos de propiedad intelectual (OCDE, 2016). Más del 84 % de estos productos se originaron en China y Hong Kong, lo que sugiere que estas naciones son los principales impulsores de la producción de productos falsificados. Esto es particularmente cierto para los productos farmacéuticos falsificados, que se envían desde países asiáticos con destino a distintos puertos de América del Norte (PSI, 2017a).

Pese a los intentos de incautar bienes a medida que circulan en el espacio físico, uno de los mayores desafíos radica en interrumpir la venta en línea de productos falsificados de cualquier tipo. La infraestructura que soporta sitios web y plataformas de comercio electrónico permite a los proveedores crear rápidamente perfiles y anunciar bienes y servicios con cierto grado de anonimato. Si se cierra un sitio web, los operadores pueden crear y registrar nuevos sitios fácilmente y continuar vendiendo con una dificultad mínima (Newman y Clarke, 2003). Como resultado, la circulación de productos falsificados es difícil de detener, independientemente de en qué parte del mundo puedan operar los proveedores.

Es importante tener en cuenta que existen diferencias fundamentales en el proceso de venta de productos falsificados. En concreto, algunos pueden anunciar sus productos de manera engañosa e intencionalmente al comprador al sugerir que el producto es legítimo o «el original». Este tipo de anuncios se consideran una falsificación engañosa, ya que el cliente tendría poca capacidad para determinar la legitimidad del artículo.

Por ejemplo, los componentes automotrices, los productos farmacéuticos y los alimentos están disponibles en espacios virtuales y reales, pero hay pocas razones para pensar que la gente buscaría versiones falsificadas de estos productos. Al contrario, aquellos que necesitan estos artículos asumen que están adquiriendo la versión real del producto.

Los espacios en línea crean una oportunidad especialmente única tanto para los falsificadores como para sus clientes, pues los consumidores pueden buscar lo que consideran medicamentos recetados legítimamente sin obtener una receta médica real. Estudios anteriores de la Junta Internacional de Fiscalización de Estupefacientes (JIFE) de las Naciones Unidas sugieren que aproximadamente el 90 % de todas las ventas farmacéuticas realizadas en línea se llevan a cabo sin receta (Finley, 2009). Estudios similares han encontrado que las farmacias en línea solicitan de manera inconsistente recetas médicas o incluso cuestionarios médicos completos para validar los síntomas y la información de salud antes de entregar medicamentos a posibles clientes (Finley, 2009; Kennedy, 2016; Sullivan, 2004).

Estos problemas limitan la capacidad de los consumidores para determinar si una farmacia en línea ofrece productos legítimos o falsificados. En el caso de que el cliente reciba los medicamentos que solicitó, existen riesgos importantes para la salud dependiendo de la calidad del proveedor y sus productos (Grow y otros, 2006; Herper, 2005; Phillips, 2005; Stoppler, 2005; Tinnin, 2005). Los datos sugieren que los productos farmacéuticos en línea pueden estar adulterados o no incluir todos los ingredientes activos necesarios según el fabricante.

Por ejemplo, un estudio realizado por Stoppler (2005) encontró que los medicamentos comprados en farmacias en línea pueden haber quedado obsoletos o caducados, fabricados en instalaciones inseguras, tener formulaciones inconsistentes del estándar del fabricante que podrían tratar una afección de manera incorrecta o simplemente no contener ingredientes activos. La Asociación de Alimentos y Medicamentos de los Estados Unidos (Tinnin, 2005) llegó a una conclusión similar, y descubrió que aproximadamente el 90 % de todos los medicamentos recetados que entran en Estados Unidos a través de vendedores en línea o por correo incluían ingredientes activos mínimos y composiciones químicas incorrectas (Tinnin, 2005).

Si alguien anuncia un producto cercano al original que sin embargo no es el artículo real, se consideraría un producto falsificado «no engañoso». La diferencia respecto a la falsificación engañosa es complicada, ya que depende del consumidor discernir que el producto sea o no legítimo y que, por lo tanto, se den cuenta con anterioridad de lo que están comprando. En algunos casos, las señales de que un producto es falso pueden ser obvias para el posible cliente. Que el vendedor anuncie los productos a un precio muy reducido puede ser una herramienta útil para evaluar la autenticidad del producto. Otros pueden usar el término *réplica* como una forma de identificar productos que parecen

reales, pero que son reproducciones. El uso de tales frases ayuda al consumidor a justificar potencialmente su compra, ya que se da cuenta de que no es el artículo original. Como resultado, sentiría que sus acciones fueron moralmente aceptables, aunque potencialmente supongan pérdidas para el proveedor legítimo.

5. Métodos de publicidad de productos falsificados en línea

Existen diversos lugares en los que anunciar productos falsificados en espacios virtuales, de la misma manera que los hay fuera de línea. En primer lugar, muchos vendedores ofrecen productos ilegítimos a través de plataformas primarias de comercio electrónico occidentales y orientales, como Amazon y AliBaba (Wall y Large, 2010). Estas plataformas permiten a los fabricantes de productos falsificados ofrecer directamente sus productos a los consumidores, en algunos casos enviados desde las propias plantas de producción. La gran cantidad de consumidores que utilizan estos servicios los convierten en una plataforma ideal para las ventas, aunque los proveedores corren el riesgo de que se eliminen sus anuncios en el caso de que se identifique la naturaleza falsificada de sus productos.

Algunos también utilizan Google y otros motores de búsqueda para garantizar que la mayor cantidad posible de clientes vean sus productos. Un estudio reciente, que examinó los productos de Nike anunciados en Google, observó que el 20 % de los resultados de búsqueda dirigían a los consumidores a sitios web de productos falsificados (Wadleigh, Drew y Moore, 2015). Además, la publicidad de Instagram y Facebook proporciona a los falsificadores una vía directa de contacto con los consumidores que dependen de lo visual y de la naturaleza social de la publicación para alentar posibles compras (Jamieson, 2018; Little, 2018; Wolfram, 2017).

Por ejemplo, un estudio de Parsons (2018) demostró que el 50 % de las ventas de cosméticos falsificados se realizan a través de redes sociales.

Algunos falsificadores también utilizarían webs secundarias de minoristas como eBay, así como plataformas de ventas de consumidor a consumidor, como Craigslist, Facebook Marketplace y otras que permiten ventas directas entre individuos (Wall y Large, 2010). Estas plataformas suelen estar muy poco reguladas por parte de los operadores del mercado, por lo que a menudo se permite la publicación de anuncios con una inspección o supervisión mínimas, que podrían restringir la venta de artículos de contrabando. Como resultado, algunos fabricantes de productos falsificados pueden vender productos a través de estos sitios web, aunque también pueden encontrarse intermediarios que simplemente venden productos falsificados a precios bajos para tratar de obtener ganancias (Wall y Large, 2010). En algunos casos, los proveedores pueden crear múltiples perfiles individuales en caso de que sus anuncios sean detectados y eliminados. Esto asegura que puedan operar por largos períodos de tiempo. También existen pruebas de que los falsificadores pueden atacar los perfiles de vendedores en sitios como eBay y hacerse pasar fraudulentamente

por otro usuario con altas clasificaciones de ventas, y operar, así, desde una ubicación específica que puede no estar asociada con la falsificación (Chua, Wareham y Robey, 2007; Gregg y Scott, 2006).

Otro método de venta de productos falsificados implica el uso de *spam* para anunciar sitios web y mercados minoristas en los que el falsificador opera de manera independiente de las principales plataformas minoristas. En algunos casos, estas tiendas pueden vender productos físicos que son falsificaciones engañosas o no, incluidas aquellas «réplicas» que parecen originales (Kennedy, 2016). Una pequeña parte de estos sitios también puede funcionar completamente como una herramienta para el fraude al cliente y el robo de identidad. Pueden anunciar productos, y en realidad no entregar ningún producto al cliente después de que se haya efectuado el pago. Los datos provenientes de los estudios del servicio de protección minorista sugieren que uno de cada seis consumidores en busca de productos originales fueron redirigidos a sitios web ilegítimos de un solo operador para realizar su compra (Smith, 2014).

El correo electrónico no deseado o *spam* es una herramienta particularmente útil para que los falsificadores vendan medicamentos recetados y suplementos falsificados de manera directa a los consumidores. Los estudios existentes sugieren que casi una cuarta parte de todos los correos *spam* publicitan productos farmacéuticos directamente a los consumidores, con independencia de si en realidad necesitan el producto por razones médicas (Grow, Elgin y Weintraub, 2006; Kerner, 2018). De hecho, los falsificadores se centran frecuentemente en medicamentos para la salud sexual, como Viagra, Cialis y otros relacionados con la disfunción eréctil (Fox, 2004). Esto se debe en parte al cada vez mayor uso de medicamentos con receta en todo el mundo, ya sea para afecciones crónicas o para el consumo adictivo asociado con opioides (Cicero y Ellis, 2012; Finely, 2009). Además, algunos consideran que el precio de los medicamentos recetados es demasiado alto para pagarlo a través de canales legítimos (Cicero y Ellis, 2012). Por último, algunos consumidores informan de que están demasiado avergonzados para pedir medicamentos con receta que sirven de tratamiento a necesidades de salud sexual y mental (Finley, 2009).

Resumen

Por lo general, el robo de propiedad intelectual se ha vuelto mucho más fácil a raíz del surgimiento de internet y la tecnología informática. La gente tiene innumerables oportunidades de adquirir propiedad intelectual, ya sea pirateando música, películas o comprando productos falsificados. Conforme la tecnología se vuelva más fácil de usar y permita el acceso a todas las formas de contenido a nivel mundial, es probable que estos delitos económicos continúen evolucionando. Como consecuencia, el sistema de justicia penal se verá obligado a cambiar sus estrategias para repercutir directamente sobre estos delitos en el contexto de un mercado global.

Bibliografía

Al-Rafee, S.; Cronan, T. P. (2006). «Digital piracy: Factors that influence attitude toward behavior». *Journal of Business Ethics* (núm. 63, págs. 237-259).

BASCAP (2016). «The economic impacts of counterfeiting and piracy» [en línea]. <https://cdn.iccwbo.org/content/uploads/sites/3/2017/02/ICC-BASCAP-Frontier-report-2016.pdf>

Brown, S. C. (2016). «Where do beliefs about music piracy come from and how are they shared? An ethnographic study». *International Journal of Cyber Criminology* (vol. 10, núm. 1, págs. 21-39.

Brown, S. C.; Holt, T. J. (eds.) (2018). *Digital Piracy: A Global, Multidisciplinary Account*. Londres: Routledge.

Burruss, G. W.; Bossler, A. M.; Holt, T. J. (2013). «Assessing the mediation of a fuller social learning model on low self-control's influence on software piracy». *Crime & Delinquency* (vol. 59, núm. 8, págs. 1157-1184).

Business Software Alliance (2016). *Seizing opportunity through license compliance* [en línea]. <http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf>

Chaudry, P. E.; Zimmerman, A. (2009). *The Economics of Counterfeit Trade: Governments, Pirates and Intellectual Property*. Nueva York: Springer.

Chua, C. E. H.; Wareham, J.; Robey, D. (2007). «The role of online trading communities in managing Internet auction fraud». *MIS Quarterly* (núm. 31, págs. 750-781).

Cicero, T. J.; Ellis, M. S. (2012). «Health outcomes in patients using no-prescription online pharmacies to purchase prescription drugs». *Journal of medical Internet research* (vol. 14, núm. 6, pág. e174).

Commuri, S. (2009). «The Impact of Counterfeiting on Genuine-Item Consumers' Brand Relationships». *Journal of Marketing* (núm. 73, págs. 6-98).

Cooper, J.; Harrison, D. M. (2001). «The social organization of audio piracy on the Internet». *Media, Culture, and Society* (núm. 23, págs. 71-89).

Downing, S. (2011). «Retro gaming subculture and the social construction of a piracy ethic». *International Journal of Cyber Criminology* (vol. 5, núm. 1, págs. 749-771).

Fagioli, B. (agosto de 2017). «Samsung Galaxy batteries discovered to be counterfeit- recalled due to fire hazard» [en línea]. *Betanews*. <https://betanews.com/2017/08/16/samsung-galaxy-battery-recall/>

Finley, L. L. (2009). «Online Pharmaceutical Sales and the Challenge for Law Enforcement». En: F. Schmalleger y M. Pittaro (eds.). *Crime of the Internet* (págs. 101-128). Saddle River, NJ: Prentice Hall.

Fox, S. (2004). *Prescription drugs online* [en línea]. PewInternet/American Life Project. <www.pewinternet.org/2004/10/10/prescription-drugs-online/>

Franklin, J.; Paxson, V.; Perrig, A.; Savage, S. (2007). «An inquiry into the nature and cause of the wealth of internet miscreants». En: *CCS07* (20 de octubre - 2 de noviembre, Alexandria).

Gottfredson, M. R.; Hirschi, T. (1990). *A General Theory of Crime*. Stanford, CA: Stanford University Press.

Gregg, D. G.; Scott, J. E. (2006). «The role of reputation systems in reducing on-line auction fraud». *International Journal of Electronic Commerce* (núm. 10, págs. 95-120).

Grow, B.; Elgin, B.; Weintraub, A. (2006). «Bitter pills: More and more people are buying prescription drugs from shady online marketers. That could be hazardous to their health» [en línea]. *BusinessWeek*. <www.businessweek.com/stories/2006-12-17/bitter-pills>

Gunter, W. D. (2009). «Internet scallywags: A comparative analysis of multiple forms and measurements of digital piracy». *Western Criminology Review* (vol. 10, núm. 1, págs. 15-28).

Herper, M. (2005). «Bad medicine» [en línea]. *Forbes*. <www.forbes.com/forbes/2005/0523/202.html>

Higgins, G. E.; Marcum, C. D. (2011). *Digital piracy: An integrated theoretical approach*.

Durham, NC: Carolina Academic Press.

Hinduja, S. (2003). «Trends and patterns among online software pirates». *Ethics and Information Technology* (núm. 5, págs. 49-61).

Hinduja, S.; Ingram, J. R. (2008). «Self-control and ethical beliefs on the social learning of intellectual property theft». *Western Criminology Review* (núm. 9, págs. 52-72).

Holt, T. J.; Bossler, A. M.; May, D. C. (2012). «Low self-control, deviant peer associations, and juvenile cyberdeviance». *American Journal of Criminal Justice* (vol. 37, núm. 3, págs. 378-395).

Holt, T. J.; Bossler, A.; Seigfried-Spellar, K. C. (2017). Cybercrime and Digital Forensics: An

Introduction (2.ª ed.). Londres: Routledge.

Holt, T. J.; Burruss, G. W.; Bossler, A. M. (2010). «Social learning and cyber deviance: Examining the importance of a full social learning model in the virtual world». *Journal of Crime and Justice* (núm. 33, págs. 15-30).

Holt, T. J.; Copes, H. (2010). «Transferring subcultural knowledge online: Practices and beliefs of persistent digital pirates». *Deviant Behavior* (núm. 31, págs. 625-654). Ingram & Hinduja.

Jamieson, C. (2 de enero de 2018). «Fakes get sneakier on social media» [en línea]. *MarkMonitor Blog*. <https://www.markmonitor.com/mmblog/fakes-get-sneakier-on-social-media>

Karagiannis, T.; Briodo, A.; Brownlee, N.; Broido, A.; Claffy, K. C.; Faloutsos, M. (2004). «Is P2P dying or just hiding?» [en línea]. *IEEE Globecom Global Internet and Next Generation Networks*. <http://alumni.cs.ucr.edu/~tkarag/papers/gi04.pdf>

Kennedy, J. (2016). «Proposed Solutions to the Brand Protection Challenges and Counterfeiting Risks Faced by Small and Medium Enterprises (SMEs)». *Journal of Applied Security Research* (vol. 11, núm. 4, págs. 450-468).

Kennedy, J. P.; Haberman, C. P.; Wilson, J. M. (2018). «Occupational pharmaceutical counterfeiting schemes: A crime scripts analysis». *Victims and Offenders* (vol. 13, núm. 2, págs. 196-214).

Kerneer, S. M. (16 de febrero de 2018). «Spam volume down, phishing attacks up in 2017 Kaspersky Lab finds» [en línea]. *eWeek*. <https://www.eweek.com/security/spam-volume-down-phishing-attacks-up-in-2017-kaspersky-lab-finds>

Kravets, D. (14 de noviembre de 2016). «Navy denies it pirated 558k copies of software, says contractor consented» [en línea]. <http://arstechnica.com/tech-policy/2016/11/navy-denies-it-pirated-558k-copies-of-software-says-contractor-consented/>

Little, T. (31 de mayo de 2018). «As cosmetic counterfeiters turn to social media, consumers expect brands to protect them» [en línea]. *World Trademark Review*. <https://www.lexology.com /library/detail.aspx?g=892e5074-cec7-4fb5-9830-04cae53708ed>

McCourt, T.; Burkart, P. (2003). «When creators, corporations and consumers collide: Napster and the development of on-line music distribution». *Media, Culture & Society* (núm. 25, págs. 333-350).

Meyer, G. R. (1989). *The Social Organization of the Computer Underground* (tesis de máster). Northern Illinois University.

Miller, B. M.; Morris, R. G. (2016). «Virtual peer effects in social learning theory». *Crime & Delinquency* (vol. 62, núm. 12, págs. 1543-1569).

MUSO (2016). *MUSO Global Film & TV Piracy Insights Report 2016* <https://www.muso.com/market-analytics-insights-reports/>

Newman, G.; Clarke, R. (2003). *Superhighway Robbery: Preventing E-commerce Crime*. Cullompton: Willan Press.

Nhan, J. (2013). «The Evolution of Online Piracy: Challenge and Response». En T. J. Holt (ed.). *Crime On-line: Causes, Correlates, and Context* (págs. 61-80). Raleigh, NC: Carolina Academic Press.

Organization for Economic Co-Operation and Development (OECD) (2016). *Trade in counterfeit and pirated goods* [en línea]. <http://www.oecd.org/governance/trade-in-counterfeit-and-pirated-goods-9789264252653-en.htm>

Parsons, S. (4 de junio 2018). «Social media now contributes to 50 % of counterfeit cosmetics sales» [en línea]. *Cosmetics Business*. <https://www.cosmeticsbusiness.com/news/article_page/Social_media_now_contributes_to_50_of_counterfeit_cosmetics_sales/143579>

Phillips, T. (2005). *Knockoff: The Deadly Trade in Counterfeit Goods*. Sterling, VA: Kogan Page Ltd.

Pouwelse, J.; Garbacki, P.; Epema, D.; Sips, H. (febrero de 2005). «The bit torrent P2P file-sharing system: Measurements and analysis». En: 4th International Workshop on Peer-to-Peer Systems (IPTPS'05). <http://iptps05.cs.cornell.edu/PDFs/CameraReady_202.pdf>

Saxena, S.; Kong, L.; Pecht, M. G. (2018). «Exploding e-cigarettes: A battery safety issue». *IEEE Access*. doi:10.1109/ACCESS.2018.2821142.

Skinner, W. F.; Fream, A. M. (1997). «A social learning theory analysis of computer crime among college students». *Journal of Research in Crime and Delinquency* (núm. 34, págs. 495-518).

Smith, T. (2014). «New Shopping Report reveals one in six bargain-hunters duped by rogue sites» [en línea]. <https://www.markmonitor.com/mmblog/new-shopping-report-reveals-one-in-six-bargain-hunters-duped-by-rogue-sites/>

Sophic Capital (2015). *Counterfeit Pharmaceuticals* [en línea]. <http://sophiccapital.com/wp-content/uploads/2015/04/DOWNLOAD-SOPHIC-CAPITALS-COUNTERFEIT-PHARMACEUTICAL-REPORT.pdf>

Stokel-Walker, C. (23 de marzo de 2019). «To compete with Netflix, online piracy is upping its game» [en línea]. *Wired*. <https://www.wired.co.uk/article/online-video-piracy-is-on-the-rise>

Stoppler, M. (2005). *Buying prescription drugs online – are the risks worth it?* [en línea]. <www.medicinenet.com/>

Sullivan, M. (2004). «Online drug sales targeted». PC World.

Tinnin, A. (2005). «Online pharmacies are new vehicle for raising some old legal issues». *Kansas City Missouri Daily Record*.

Ulsperger, J. S.; Hodges, S. H.; Paul, J. (2010). «Pirates on the plank: Neutralization theory and the criminal downloading of music among Generation Y in the era of late modernity». *Journal of Criminal Justice and Popular Culture* (vol. 17, núm. 1, págs. 124-151).

U. S. Department of Homeland Security (2018). *Intellectual Property Rights Seizure Statistics: Fiscal Year 2017* [en línea]. <https://www.cbp.gov/document/stats/fy-2017-ipr-seizure-statistics>.

U. S. Government Accounting Officer (2018). *Agencies Can Improve Efforts to Address Risks Posed by Changing Counterfeits Markets* [en línea]. <https://www.gao.gov/products/GAO-18-216/>

Wadleigh, J.; Drew, J.; Moore, T. (2015). «The E-Commerce Market for Lemons: Identification and Analysis of Websites Selling Counterfeit Goods». En: *Proceedings of the 24th International Conference on World Wide Web* (págs. 1188-1197). International World Wide Web Conferences Steering Committee.

Wall, D. S. (2001). «Cybercrimes and the Internet». En: D. S. Wall (ed.). *Crime and the Internet* (págs. 1-17). Nueva York: Routledge.

Wall, D. S.; Large, J. (2010). «Locating the public interest in policing counterfeit luxury fashion goods». *British Journal of Criminology* (núm. 50, págs. 1094-1116).

Wolfram, J. (22 de octubre de 2017). «Why kicking out counterfeit crooks on Instagram is so important» [en línea]. *Entrepreneur.com*. <https://www.entrepreneur.com/article/296783>

Wolfe, S. E.; Higgins, G. E.; Marcum, C. D. (2008). «Deterrence and digital piracy: A preliminary examination of the role of viruses». *Social Science Computer Review* (vol. 26, núm. 3, págs. 317-333).

Yar, M. (2013). *Cybercrime and Society* (2.ª ed.). Londres: Sage Publications.