Falsificació i robatori de propietat intel·lectual

PID_00269963

Thomas Holt

Temps mínim de dedicació recomanat: 2 hores

Universitat Oberta de Catalunya

Thomas Holt

L'encàrrec i la creació d'aquest recurs d'aprenentatge UOC han estat coordinats pel professor: Marc Balcells Magrans (2019)

Primera edició: setembre 2019

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

Índex

Introducció

L'aparició dels ordinadors i internet va canviar la manera en què ens comuniquem a tot el món. Al mateix temps, també va influir directament en com adquirim i gaudim de mitjans com la música, la televisió, el cinema i la premsa. El desenvolupament de serveis de transmissió de música, com Pandora, Spotify i Tidal, permet als usuaris compartir llistes de reproducció i gaudir de catàlegs complets d'artistes i estils de música. De la mateixa manera, el desenvolupament de Netflix, YouTube, HBO Go i DisneyNow proporciona eines fàcils que permeten als seus usuaris veure hores de pel·lícules i contingut de televisió en qualsevol moment (Brown i Holt, 2018).

La tecnologia també va afectar directament la nostra capacitat de comprar i consumir mitjans i béns físics tradicionals. Serveis com iTunes permeten comprar pràcticament qualsevol tipus de mitjà i descarregar-lo directament en múltiples dispositius, o transmetre'l des de la seva biblioteca de compres (Brown i Holt, 2018). Amazon i Alibaba també proporcionen accés a productes d'arreu del món, inclosos aliments, roba i béns duradors, com peces d'automòbils i electrodomèstics. De la mateixa manera, llocs com Etsy constitueixen una plataforma perquè els productes artesanals arribin a un mercat global, la qual cosa, en canvi, no seria possible en l'espai físic (Brown i Holt, 2018).

Tots aquests serveis reflecteixen un canvi en la manera en què nosaltres, com a consumidors, podem obtenir accés a béns produïts tant per individus com per corporacions multinacionals. La facilitat d'accés que ofereix la tecnologia també ha creat oportunitats úniques perquè els delinqüents aprofitin aquests recursos i així beneficiar-se dels productes i idees d'uns altres. De fet, la tipologia de Wall (2001) d'engany cibernètic i robatori reconeix actes de frau que suposen l'ús i l'ús indegut de la tecnologia per adquirir béns i serveis gratuïtament, o aprofitar i beneficiar-se de les idees i guanys d'uns altres. Això pot abastar activitats com la pirateria digital o la còpia de mitjans digitals com enregistraments de so o vídeo, programari i altres arxius sense que hi hagi cap autorització o pagament al propietari dels drets d'autor (Gunter, 2009; Higgins i Marcum, 2011; Skinner i Fream, 1997). Així mateix, la gent pot beneficiar-se de la venda de roba, joies i altres productes que semblen de fabricants específics, sobretot marques de luxe, i que en realitat van ser fabricats per altres persones. Aquest capítol permetrà aprofundir en l'ús de la tecnologia per robar idees, béns i serveis, així com comprendre els qui participen en aquestes activitats, sigui com a productors o com a consumidors.

1. Propietat intel·lectual i protecció legal

El disseny i el pas d'una idea a un producte o article físic són una pràctica important, que s'ha convertit en un producte legalment protegit i amb un clar valor econòmic que pot variar segons el lloc. Ja es tracti d'una obra d'art o d'una obra creativa com una peça musical, aquesta idea posseeix un valor en si mateixa que a més pot generar guanys amb el temps. Una vegada la idea es manifesta, ja sigui en escriure-la, en pintar-la o en col·locar-la en qualsevol tipus de mitjà fix, es converteix en propietat intel·lectual, ja que la seva creació es pot associar a una persona o grup específic i unes altres persones poden veure-la (Brown i Holt, 2018; Holt, Bossler i Seigfried-Spellar, 2017).

Si una persona desitja protegir les idees i el material que ha fet i assegurar-se de rebre tots els drets i crèdits de la seva creació, hi ha diferents marcs legals als quals acollir-se. Depenent de la ubicació d'una persona, es poden sol·licitar drets d'autor, marques registrades i patents, que proporcionen diferents proteccions legals de propietat intel·lectual, dissenys i drets de propietat i pagaments per períodes específics de temps. Per exemple, les corporacions i les empreses poden sol·licitar marques registrades que garanteixin que els seus logotips i la seva imatge corporativa estiguin vinculats a productes específics i no puguin ser utilitzats per ningú més.

De la mateixa manera, el dret d'autor és una mesura de protecció legal que vincula una persona o persones amb una obra artística d'algun tipus tan aviat com s'escriu, grava o imprimeix (Yar, 2013). Els drets d'autor són particularment importants, ja que estableixen la propietat i les obligacions financeres envers el propietari i poden aplicar-se a diversos països, especialment en tota la UE. Segons la legislació dels Estats Units, les persones poden rebre drets d'autor des del moment en què es crea l'obra en qüestió. No obstant això, estan obligats a registrar aquests drets d'autor amb el Govern nord-americà per obtenir totes les proteccions legals necessàries. En cas contrari, l'individu no pot emprendre accions civils o penals contra altres persones que utilitzen les seves idees o obres perquè no és un material reconegut sota la protecció legal dels Estats Units (Holt i altres, 2017).

La capacitat d'accedir i compartir idees a grans distàncies per mitjans tecnològics ha desafiat radicalment els processos establerts de drets de propietat intel·lectual i titularitat arreu del món. La gent pot observar una idea, un disseny o un producte en línia i intentar fer-los per si mateixa o vendre'ls sense contactar amb el creador. També pot trobar un mitjà i després intentar reproduir-lo i possiblement distribuir-lo a altres persones sense el permís del propietari o titular dels drets d'autor.

Per exemple, gravar una peça musical o un clip de televisió al telèfon i després publicar-lo a YouTube és una forma de robatori de propietat intel·lectual, ja que el titular original dels drets d'autor no serà reemborsat per l'ús de la seva creació.

Com a resultat, la tecnologia ha simplificat i globalitzat la nostra capacitat d'infringir els titulars de drets d'autor i creadors de contingut amb un risc mínim de detecció.

2. Pirateria digital i robatori de propietat intel·lectual

Com es va assenyalar anteriorment, la distribució i el robatori de mitjans digitals són un problema en l'era digital. De fet, grups antipirateria com Business Software Alliance (BSA) estimen que el 39% del programari utilitzat arreu del món està piratejat de diferents fonts. El programari piratejat pot trobar-se en governs i sistemes comercials, sobretot en països de baixos ingressos on el cost d'aquests productes pot resultar prohibitiu. Com a resultat, les estimacions suggereixen que molts països d'Àsia, Europa Central i Oriental i Amèrica Llatina tenen taxes de pirateria més altes que altres parts del món (BSA, 2016). Això no significa que els Estats Units i altres països no participin en la pirateria.

> De fet, la Marina dels Estats Units va ser objecte d'una demanda presentada per Bitmanagement Software, que va afirmar que més de 558.000 còpies del seu programari de realitat virtual 3D s'estaven utilitzant sense la llicència correcta (Kravets, 2016). Encara que no està clar com es tancarà el cas, la companyia va afirmar que tenia dret a més de 600 milions de dòlars en honoraris i danys a causa de la pèrdua d'ingressos.

Cal assenyalar que la pirateria existia abans del desenvolupament d'internet, encara que sempre ha tingut una relació simbiòtica amb la tecnologia en qualsevol forma.

> Per exemple, el desenvolupament d'equips d'enregistrament d'àudio i vídeo per a l'usuari domèstic a la dècada de 1960 i el seu cost cada vegada menor van fer possible que les persones gravessin programes de música i televisió mentre es reproduïen. De fet, els anomenats *mixtapes* dels anys vuitanta són el resultat directe del fet que els consumidors poguessin gravar qualsevol enregistrament d'àudio, fins i tot si s'escoltava en directe a la ràdio, afegir diferents peces de música de diferents artistes i gravar etiquetes en un sol casset (Nhan, 2013).

El creixement del mercat de PC a la dècada de 1980 i la popularitat dels videojocs van conduir també a les primeres formes de pirateria de programari. En aquell moment, les proteccions al programari per evitar còpies eren relativament simples.

> Per exemple, l'ús de claus de producte, que consisteix en una cadena de codi alfanumèric, podia enganyar-se amb certa facilitat, la qual cosa permetia copiar una peça de programari. Les tècniques per infringir aquests sistemes de protecció es compartien amb freqüència entre els *hackers* i després en línia per mitjà de *Bulletin Board Systems* (BBS) i fòrums (Meyer, 1989).

En reconeixement de les seves habilitats, als vuitanta alguns van usar el terme *warez doodz* per referir-se a aquells *hackers* que podien traspassar les proteccions de programari (*wares*) (Cooper i Harrison, 2001).

El desenvolupament i la ràpida acceptació de la tecnologia de discos compactes, o CD, als anys noranta també van influir molt en la pirateria de mitjans en general. L'ús de cintes de casset i discos de vinil era atractiu per als consumidors, però suposava un format analògic en el qual les ones de so produïdes pels músics es copiaven i reproduïen d'igual manera en un format

d'emmagatzematge de mitjans extraïble, com la cinta magnètica d'un casset. Un format analògic reprodueix diferents tons i sons que poden resultar agradables a qui els escolta, però no és el mateix que s'escoltaria i gravaria en format digital. Concretament, els CD van permetre a les discogràfiques tractar les ones de so dels músics com a dades binàries emmagatzemables electrònicament en un CD. Aquests mitjans digitals ofereixen a l'oïdor un so més bo i a un preu molt més baix en comparació amb els mitjans tradicionals.

A mesura que el format de CD anava sent àmpliament acceptat, una altra innovació tecnològica va transformar encara més la propietat intel·lectual digital. El 1996 es va desenvolupar un nou format de programari per comprimir arxius d'àudio i multimèdia, la qual cosa permet que els arxius grans siguin prou petits com per compartir-los per mitjà de connexions a internet (Holt i altres, 2017). Donades les velocitats de connexió d'accés telefònic a internet relativament lentes de mitjan anys noranta, les organitzacions de mitjans i les companyies tecnològiques es van interessar per trobar una altra forma de transferir la propietat intel·lectual digital de manera ràpida i eficient. El format de compressió MP3, llavors, es va desenvolupar amb la col·laboració entre el Motion Picture Experts Group (MPEG) i l'Organització Internacional de Normalització (International Organization for Standardization, o ISO) (Holt i altres, 2017).

El format MP3 es va convertir ràpidament en l'estàndard de la indústria per al format de compressió de mitjans, i encara s'utilitza i serveix com a model per a la gestió d'arxius en l'actualitat. De fet, el llançament del format MP3 va conduir molt ràpid a la producció de dispositius que podrien usar-se específicament amb aquest tipus de mitjans.

> Per exemple, l'eina de programari Winamp per a ordinadors de taula va permetre que els usuaris escoltessin arxius MP3 en qualsevol moment.

Els dispositius de reproducció portàtils també es van desenvolupar i es van produir per a la venda al detall l'any 1999. Aquestes tecnologies també van possibilitar copiar música dels seus CD al seu PC, per la qual cosa l'augment de les unitats de CD que podien llegir i escriure en aquest format va fer possible crear *mixtapes* en CD.

Com a conseqüència, el format MP3 va millorar la gestió de la propietat intel·lectual i va simplificar la pirateria arreu del món.

> Per exemple, les xarxes de pirateria van passar d'emmagatzemar grans quantitats de material en servidors individuals o repositoris de llocs web per a la seva descàrrega, a mètodes de xarxa més distribuïts per minimitzar el risc d'identificació per part de la policia (Cooper i Harrison, 2001).

Els *hackers* van començar a crear protocols d'intercanvi d'arxius entre parells (P2P) que permetien compartir arxius en xarxes per mitjà de sistemes individuals. Això es deu en part a Internet Relay Chat, o IRC, una forma de missatgeria instantània establerta el 1998 que funcionava en part aïllada d'internet i que està dividida en sales de xat establertes i administrades per diverses perso-

nes. Les comunitats de pirates informàtics van adoptar ràpidament IRC com un client de comunicacions distribuïdes i un mecanisme per compartir programari, jocs i música (Cooper i Harrison, 2001), així com eines i dades de *hacking* (Franklin i altres, 2007). En concret, els individus podien entrar en un canal, sol·licitar contingut i negociar intercanvis de material (Cooper i Harrison, 2001).

La naturalesa tècnica d'IRC va limitar la seva popularitat com a plataforma de pirateria en comparació amb serveis P2P més fàcils d'usar, com Napster, disponible a partir de 1999 (Nhan, 2013).

Napster

Napster era un programa gratuït que connectava sistemes d'usuaris per mitjà dels servidors corporatius de Napster i indexava arxius específics designats per compartir arxius codificats en MP3. Al seu torn, els usuaris podien buscar mitjans per nom i descarregar els arxius d'altres ordinadors ràpidament. Si bé les velocitats de descàrrega van variar segons el tipus de connexió disponible per a l'usuari, això va permetre optimitzar el procés d'identificació d'arxius i materials pirates de manera més eficient (Nhan, 2013).

La quantitat d'arxius compartits amb el programari de Napster va fer que diversos artistes i companyies discogràfiques se n'adonessin. Després de només dos anys en funcionament, Napster va ser demandat per la banda Metallica i A&M Records el 2001, que van afirmar que el lloc els va causar greus danys econòmics en possibilitar que es compartís la seva propietat intel·lectual gratis (McCourt i Burkart, 2003). Napster va ser objecte de dures crítiques en els mitjans després d'aquestes demandes, i finalment va posar fi al seu servei gratuït d'intercanvi d'arxius P2P a favor d'un model de pagament que garantiria una retribució justa als artistes d'enregistrament. La popularitat de Napster va disminuir ràpidament a mesura que els usuaris es van traslladar a altres serveis P2P gratuïts, com LimeWire i Kazaa, amb una infraestructura similar per facilitar la pirateria.

El desenvolupament de discos de vídeo digital o DVD el 1996 va suposar una transformació similar en la pirateria de cinema i televisió. La producció de DVD i la posterior tecnologia Blu-ray es va tornar més fàcil amb la creació del format MPEG, que combinava digitalització i compressió de vídeo i àudio en un sol paquet. La primera còpia de format MPEG es va fer pública el 1993, encara que amb el temps ha sofert nombrosos canvis que van millorar la qualitat dels arxius de so i àudio. A més, el format MPEG va permetre que els titulars de propietat intel·lectual implementessin la protecció de gestió de drets digitals (*Digital Rights Management*, o DRM) per reduir la probabilitat que els consumidors copiessin el contingut en discos durs i altres dispositius. Els *hackers* van trobar moltes solucions per traspassar les proteccions DRM, inclosos els programes de programari simples que permetrien als usuaris copiar directament el contingut del DVD a un DVD en blanc (Karagiannis i altres, 2004).

A mesura que la tecnologia de discos i reproductors de DVD va començar a expandir-se arreu del món a la fi dels anys noranta i principis del segle XXI, el format digital va permetre als pirates trobar noves formes de compartir àudio i vídeo d'alta qualitat a internet. A més, van començar a sorgir noves plataformes per a la pirateria, en particular el *torrenting*, estretament relacionada amb BitTorrent.

BitTorrent

L'ús de *torrents* implica un programa especial que permet als usuaris rastrejar i administrar la càrrega i descàrrega d'arxius des d'una enorme xarxa distribuïda d'altres usuaris de *torrents*. El programari indexa els arxius disponibles en els sistemes d'usuari, de manera similar a Napster i altres programes P2P, però després descarrega simultàniament l'arxiu d'altres usuaris en petits fragments. El programa *torrent* torna a unir els components en un únic arxiu utilitzable que pot reproduir-se. Aquest programari garanteix descàrregues ràpides i distribuïdes, la qual cosa fa més difícil aturar les xarxes de pirateria, ja que ara hi ha múltiples maneres de descarregar arxius. El programari de *torrent* es va convertir en un mètode extremament popular per a la pirateria, per la qual cosa alguns van suggerir que va ser la font de més de la meitat de tots els materials piratejats en línia el 2004 (Pouwelse, Garbacki, Epema i Sips, 2005).

A mesura que els serveis de transmissió de mitjans van guanyar més popularitat a mitjans i finals de la dècada de l'any 2000, hi ha algunes proves que els *hackers* han anat canviant de nou els seus mètodes per obtenir contingut de manera il·legal (MUSO, 2016). La proliferació de serveis que van des de YouTube fins a Spotify i Netflix permet als usuaris l'accés directe a tota una gamma de propietat intel·lectual amb costos variables depenent de la subscripció seleccionada. L'accessibilitat d'aquests serveis ha portat alguns pirates a començar a «extreure» o copiar contingut a mesura que es reprodueix en la plataforma del proveïdor de serveis. Al seu torn, aquests *hackers* usen aquest contingut o el comparteixen amb la comunitat en general mitjançant serveis d'*streaming* de contingut piratejat (MUSO, 2016). De fet, va haver-hi més de 190.000 milions de visites a llocs web de pirateria el 2018, el 60% de les quals van ser a plataformes d'*streaming* (Stokel-Walker, 2019). Aquestes estadístiques van fer que alguns suggerissin que a mesura que els serveis d'*streaming* augmenten en nombre i canvien els seus models de preus, és més probable que pateixin pèrdues econòmiques per l'augment de pirates que ofereixen accés al seu contingut (Stokel-Walker, 2019). Per tant, la pirateria i la tecnologia tenen una relació simbiòtica que continuarà evolucionant en el futur.

3. Comprendre qui pirateja els mitjans i la propietat intel·lectual

La naturalesa canviant de les pràctiques de pirateria digital i la probabilitat que algú pugui descarregar o compartir contingut piratejat convida a qüestionar qui és procliu a piratejar contingut.

Les estadístiques suggereixen que la majoria de les persones arreu del món han participat en la pirateria en algun moment, encara que està menys clar si hi ha diferències en els factors de comportament o actitud que influeixin en l'ús constant de contingut piratejat.

Els resultats de la recerca criminològica suggereixen que els primers actes de pirateria formen part en gran manera d'un procés d'aprenentatge social, ja que s'aprèn a piratejar materials d'altres (Higgins i Marcum, 2011; Holt i Copes, 2010). Les relacions amb altres *hackers* poden provenir d'interaccions en el món real (Higgins i Marcum, 2011; Hinduja i Ingram, 2008, Holt, Bossler i May, 2012), així com en espais virtuals com fòrums i xarxes socials (Miller i Morris, 2014). Aquestes relacions les poden constituir amics, pares o fins i tot tutorials publicats en línia amb els quals l'usuari interactua per obtenir informació sobre el procés de pirateria (Burruss, Holt i Bossler, 2013; Miller i Morris, 2014). Així mateix, aquestes relacions ofereixen informació sobre els millors llocs per piratejar contingut i com es pot justificar aquest comportament delictiu davant dels altres.

El coneixement tècnic requerit per participar en algunes formes de pirateria suposa una barrera inicial que requereix cert grau d'intercanvi d'informació amb els seus companys o llaços socials per poder superar-la (Hinduja, 2003; Holt i Copes, 2010; Holt, Burruss i Bossler, 2010; Ingram i Hinduja, 2008; Skinner i Fream, 1997). Una vegada que un individu s'ha iniciat en la pirateria, la importància dels llaços socials pot disminuir a l'hora d'identificar diferents estratègies per descarregar materials d'altres llocs (Holt i Copes, 2010).

La recerca també demostra que les persones que pirategen tendeixen a mantenir creences i actituds que donen suport a la seva violació dels drets i les lleis de propietat intel·lectual, la qual cosa els permet continuar participant en comportaments il·legals (Brown, 2016; Higgins i Marcum, 2011; Ingram i Hinduja, 2008; Skinner i Fream, 1997).

Per exemple, aquells que descarreguen música solen pensar que les seves accions tenen un escàs dany econòmic per als titulars i creadors de drets d'autor (Brown, 2016; Higgins i Marcum, 2011; Ingram i Hinduja, 2008; Ulsperger, Hodges i Paul, 2010). Aquells que pirategen videojocs solen argumentar que les seves accions ajuden a mantenir l'interès del públic en les consoles de jocs retro o de la «vella escola», que d'una altra manera quedarien obsoletes (Downing, 2011). Uns altres suggereixen que pirategen solament per

identificar nous artistes o creadors de mitjans i determinar si els agraden les seves idees abans d'invertir diners en la seva música o les seves pel·lícules (vegeu, per exemple, Holt i Copes, 2010). Referent a això, la pirateria pot ser una forma de provar contingut abans de pagar àlbums o temporades de programes de televisió. Uns altres també culpen els productors de mitjans per cobrar massa pels seus productes, per la qual cosa adquirir legalment tots els mitjans que es voldrien consumir resultaria massa car (Higgins i Marcum, 2011; Holt i Copes, 2010; Ulsperger i altres, 2010). Part dels *hackers* també suggereix que descarreguen contingut perquè no hi ha un conjunt inherent de conductes ètiques que puguin orientar les activitats en línia, per la qual cosa és possible fer el que es vulgui independentment de la llei (Higgins i Marcum, 2011; Ulsperger i altres, 2010).

Un altre factor clarament associat amb la pirateria digital és el nivell d'autocontrol d'un individu, o la capacitat de regular el seu comportament davant l'oportunitat d'infringir la llei (Gottfredson i Hirschi, 1990). Les persones amb poc autocontrol són curtes de mires, impulsives, assumeixen riscos i tenen menys probabilitats de sentir empatia cap a les seves víctimes. Això s'alinea bastant bé amb la pirateria digital, ja que els materials piratejats es troben en un enorme subministrament relativament fàcil d'adquirir i requereix poca habilitat tècnica en general, al mateix temps que proporciona una satisfacció immediata als descarregadors, que poden compartir el seu sentit de la responsabilitat en les seves accions il·legals. Això té el suport de la literatura existent sobre el tema, ja que els estudis reflecteixen que les persones amb baix autocontrol són consistentment més propenses a participar en la pirateria, sigui en mostres juvenils o adultes (Higgins i Marcum, 2011; Holt i altres, 2013).

Aquests factors poden explicar les dificultats inherents a detenir la pirateria a escala mundial. Si bé hi ha sancions civils i penals per pirateria, a moltes persones que descarreguen propietat intel·lectual no els preocupen, en general, les sancions formals de la policia (Al-Rafee i Cronan, 2006; Holt i Copes, 2010). Això es pot deure al fet que les persones consideren que la pirateria digital és diferent del robatori físic en botigues i supermercats (Downing, 2011; Holt i Copes, 2010). De fet, una de les úniques formes de dissuadir potencialment la pirateria és destacar el fet que els arxius descarregats puguin contenir programari maliciós (Wolf, Higgins i Marcum, 2008). En cas contrari, les intervencions formals per minimitzar la pirateria són generalment ineficaces (Nhan, 2013). Per tant, és probable que la pirateria digital persisteixi mentre existeixi internet.

4. La falsificació i internet

Una altra forma de robatori de propietat intel·lectual implica aquella producció i venda de béns que utilitzen fraudulentament dissenys amb drets d'autor o logotips i envasos de marques registrades sense retornar els guanys al propietari original, la qual cosa generalment es coneix com a falsificació (Wall i Large, 2010).

Pràcticament qualsevol producte pot ser falsificat, ja sigui alimentari, farmacèutic o de roba, encara que en general estan fets de materials de menor qualitat (Wall i Large, 2010). Igual que la pirateria, els productes falsificats es poden distribuir i vendre sense internet, i així ha estat al llarg de la història (Chaudry i Zimmerman, 2009). De fet, els productes falsificats queden sovint ocults en la cadena superior de distribució de productes legítims i pot ser difícil distingir-los dels articles originals (Kennedy, 2016). Estimacions recents suggereixen que els falsificadors poden haver guanyat 200.000 milions de dòlars a escala mundial per la venda de productes farmacèutics il·lícits (Sophic Capital, 2015).

Algunes entitats estan directament perjudicades per la creació i venda de productes falsificats. En primer lloc, aquell que compra productes falsificats pot perdre diners si el producte no funciona o no és efectiu per tractar malalties específiques en el cas de productes farmacèutics i sanitaris. A més, alguns consumidors han sofert lesions físiques després d'utilitzar productes fets amb materials de pitjor qualitat, com es va observar quan les bateries falsificades (Fagioli, 2017) i els cigarrets electrònics (Saxena i altres, 2018) van calar foc i van explotar. De la mateixa manera, medicaments falsificats han causat lesions greus i fins i tot la mort a algunes persones que els han ingerit (Kennedy i altres, 2018).

Els propietaris de marques encarregats de produir productes originals també perden diners i participació en el mercat a mesura que les compres són absorbides per falsificadors (Commuri, 2009). En alguns casos, els reclams de falsificació també poden portar al fet que els fabricants legítims reemplacin els productes afectats i minimitzin l'atenció negativa de la premsa. Més enllà d'aquestes pèrdues directes, la falsificació suposa per als fabricants legítims despeses de milions de dòlars i mà d'obra per identificar productes falsificats en la cadena de subministrament i evitar així que arribin als consumidors (Commuri, 2009). A més, es veuen obligats a gastar diners en advocats i honoraris legals per fer complir les patents i els reclams de marques comercials que puguin tenir en diversos països i poder reduir la producció de falsificacions (US Government Accountability Office, 2010). De fet, alguns estimen que les

despeses associades a la falsificació per a la comunitat empresarial assoleixen centenars de milers de milions cada any (BASCAP, 2011; US Government Accountability Office, 2010).

L'auge dels llocs web de comerç electrònic, correu electrònic i xarxes socials va simplificar el procés de publicitat i venda de productes directament als consumidors amb menor risc de detecció per part de les forces de l'ordre o del titular de la propietat intel·lectual (Kennedy i altres, 2018; Wall i Large, 2010). A més, internet permet obtenir accés al mercat global de productes independentment de la ubicació del comprador a l'espai físic. Les diferències geogràfiques en les lleis relacionades amb les proteccions de propietat intel·lectual fan possible que els productes falsificats s'adquireixin de manera més immediata en llocs web de comerç electrònic.

> Per exemple, els Estats Units ofereixen protecció legal a la primera empresa que demostra haver utilitzat una marca comercial en la pràctica, mentre que nacions com la Xina protegeixen la primera empresa que presenti una marca comercial o altres documents legals davant agències governamentals (Kennedy i altres, 2018). Com a conseqüència, un producte pot ser falsificat en un país i estar protegit legalment en un altre, encara que en tots dos casos poden adquirir-se mitjançant detallistes en línia.

Aquestes dinàmiques explicarien la gran quantitat de productes falsificats que la policia confisca cada any (US Government Accounting Office, 2018). El Departament de Seguretat Nacional dels Estats Units (Department of Homeland Security, o DHS) va assegurar haver confiscat més de 34.000 enviaments de productes falsificats que van arribar als Estats Units des de ports estrangers (US Department of Homeland Security, 2018). De la mateixa manera, l'Organització per a la Cooperació i el Desenvolupament Econòmic (OCDE) va informar que més de 461.000 milions de dòlars en béns importats als Estats Units eren falsos, inclosos els productes falsificats que infringien directament les marques registrades, les patents i els drets de propietat intel·lectual (OCDE, 2016). Més del 84% d'aquests productes es van originar a la Xina i Hong Kong, la qual cosa suggereix que aquestes nacions són els principals impulsors de la producció de productes falsificats. Això és particularment cert per als productes farmacèutics falsificats, que s'envien des de països asiàtics amb destinació a diferents ports d'Amèrica del Nord (PSI, 2017a).

Malgrat els intents de confiscar béns a mesura que circulen a l'espai físic, un dels majors desafiaments radica a interrompre la venda en línia de productes falsificats de qualsevol tipus. La infraestructura que suporta llocs web i plataformes de comerç electrònic permet als proveïdors crear ràpidament perfils i anunciar béns i serveis amb cert grau d'anonimat. Si es tanca un lloc web, els operadors poden crear i registrar nous llocs fàcilment i continuar venent amb una dificultat mínima (Newman i Clarke, 2003). Com a resultat, la circulació de productes falsificats és difícil d'aturar, independentment de la part del món on puguin operar els proveïdors.

És important tenir en compte que hi ha diferències fonamentals en el procés de venda de productes falsificats. En concret, alguns poden anunciar els seus productes de manera enganyosa i intencionalment al comprador en suggerir que el producte és legítim o «l'original». Aquest tipus d'anuncis es consideren una falsificació enganyosa, ja que el client tindria poca capacitat per determinar la legitimitat de l'article.

Per exemple, els components automotrius, els productes farmacèutics i els aliments estan disponibles en espais virtuals i reals, però hi ha poques raons per pensar que la gent buscaria versions falsificades d'aquests productes. Al contrari, aquells que necessiten aquests articles assumeixen que estan adquirint la versió real del producte.

Els espais en línia creen una oportunitat especialment única tant per als falsificadors com per als seus clients, ja que els consumidors poden buscar el que consideren medicaments receptats legítimament sense obtenir una recepta mèdica real. Estudis anteriors de la Junta Internacional de Fiscalització d'Estupefaents (JIFE) de les Nacions Unides suggereixen que aproximadament el 90% de totes les vendes farmacèutiques realitzades en línia es duen a terme sense recepta (Finley, 2009). Estudis similars han trobat que les farmàcies en línia sol·liciten de manera inconsistent receptes mèdiques o fins i tot qüestionaris mèdics complets per validar els símptomes i la informació de salut abans de lliurar medicaments a possibles clients (Finley, 2009; Kennedy, 2016; Sullivan, 2004).

Aquests problemes limiten la capacitat dels consumidors per determinar si una farmàcia en línia ofereix productes legítims o falsificats. En el cas que el client rebi els medicaments que va sol·licitar, hi ha riscos importants per a la salut depenent de la qualitat del proveïdor i els seus productes (Grow i altres, 2006; Herper, 2005; Phillips, 2005; Stoppler, 2005; Tinnin, 2005). Les dades suggereixen que els productes farmacèutics en línia poden estar adulterats o no incloure tots els ingredients actius necessaris segons el fabricant.

Per exemple, un estudi realitzat per Stoppler (2005) va trobar que els medicaments comprats en farmàcies en línia poden haver quedat obsolets o caducats, fabricats en instal·lacions insegures, tenir formulacions inconsistents de l'estàndard del fabricant que podrien tractar una afecció de manera incorrecta o simplement no contenir ingredients actius. L'Associació d'Aliments i Medicaments dels Estats Units (Tinnin, 2005) va arribar a una conclusió similar, i va descobrir que aproximadament el 90% de tots els medicaments receptats que entren als Estats Units per mitjà de venedors en línia o per correu incloïen ingredients actius mínims i composicions químiques incorrectes (Tinnin, 2005).

Si algú anuncia un producte proper a l'original que, no obstant això, no és l'article real, es consideraria un producte falsificat «no enganyós». La diferència respecte a la falsificació enganyosa és complicada, ja que depèn del consumidor destriar que el producte sigui o no legítim i que, per tant, s'adonin amb anterioritat del que estan comprant. En alguns casos, els senyals que un producte és fals poden ser obvis per al possible client. Que el venedor anunciï els productes a un preu molt reduït pot ser una eina útil per avaluar l'autenticitat del producte. Uns altres poden usar el terme *rèplica* com una forma d'identificar productes que semblen reals, però que són reproduccions. L'ús d'aquestes frases ajuda el consumidor a justificar potencialment la seva compra, ja que s'adona

que no és l'article original. Com a resultat, sentiria que les seves accions van ser moralment acceptables, encara que potencialment suposin pèrdues per al proveïdor legítim.

5. Mètodes de publicitat de productes falsificats en línia

Hi ha diversos llocs en els quals es poden anunciar productes falsificats en espais virtuals, de la mateixa manera que n'hi ha fora de línia. En primer lloc, molts venedors ofereixen productes il·legítims per mitjà de plataformes primàries de comerç electrònic occidentals i orientals, com Amazon i AliBaba (Wall i Large, 2010). Aquestes plataformes permeten als fabricants de productes falsificats oferir directament els seus productes als consumidors, en alguns casos enviats des de les mateixes plantes de producció. La gran quantitat de consumidors que utilitzen aquests serveis els converteixen en una plataforma ideal per a les vendes, encara que els proveïdors corren el risc que s'eliminin els seus anuncis en el cas que s'identifiqui la naturalesa falsificada dels seus productes.

Alguns també utilitzen Google i altres motors de cerca per garantir que la major quantitat possible de clients vegin els seus productes. Un estudi recent, que va examinar els productes de Nike anunciats a Google, va observar que el 20% dels resultats de cerca dirigien els consumidors a llocs web de productes falsificats (Wadleigh, Drew i Moore, 2015). A més, la publicitat d'Instagram i Facebook proporciona als falsificadors una via directa de contacte amb els consumidors que depenen del visual i de la naturalesa social de la publicació per encoratjar possibles compres (Jamieson, 2018; Little, 2018; Wolfram, 2017).

> Per exemple, un estudi de Parsons (2018) va demostrar que el 50% de les vendes de cosmètics falsificats es realitzen per mitjà de xarxes socials.

Alguns falsificadors també utilitzarien webs secundàries de detallistes com eBay, així com plataformes de vendes de consumidor a consumidor, com Craigslist, Facebook Marketplace i altres que permeten vendes directes entre individus (Wall i Large, 2010). Aquestes plataformes solen estar molt poc regulades per part dels operadors del mercat, per la qual cosa sovint es permet la publicació d'anuncis amb una inspecció o supervisió mínimes, que podrien restringir la venda d'articles de contraban. Com a resultat, alguns fabricants de productes falsificats poden vendre productes per mitjà d'aquests llocs web, encara que també poden trobar-se intermediaris que simplement venen productes falsificats a preus baixos per tractar d'obtenir guanys (Wall i Large, 2010). En alguns casos, els proveïdors poden crear múltiples perfils individuals en cas que els seus anuncis siguin detectats i eliminats. Això assegura que puguin operar per llargs períodes de temps. També hi ha proves que els falsificadors poden atacar els perfils de venedors en llocs com eBay i fer-se passar fraudulentament per un altre usuari amb altes classificacions de vendes, i operar, així, des d'una ubicació específica que pot no estar associada amb la falsificació (Chua, Wareham i Robey, 2007; Gregg i Scott, 2006).

Un altre mètode de venda de productes falsificats implica l'ús d'*spam* per anunciar llocs web i mercats minoristes en els quals el falsificador opera de manera independent de les principals plataformes minoristes. En alguns casos, aquestes botigues poden vendre productes físics que són falsificacions enganyoses o no, incloses aquelles «rèpliques» que semblen originals (Kennedy, 2016). Una petita part d'aquests llocs també pot funcionar completament com una eina per al frau al client i el robatori d'identitat. Poden anunciar productes, i en realitat no lliurar cap producte al client després que s'hagi efectuat el pagament. Les dades provinents dels estudis del servei de protecció minorista suggereixen que un de cada sis consumidors a la recerca de productes originals van ser redirigits a llocs web il·legítims d'un sol operador per realitzar la seva compra (Smith, 2014).

El correu electrònic no desitjat o *spam* és una eina particularment útil perquè els falsificadors venguin medicaments receptats i suplements falsificats de manera directa als consumidors. Els estudis existents suggereixen que gairebé una quarta part de tots els correus *spam* publiciten productes farmacèutics directament als consumidors, amb independència de si en realitat necessiten el producte per raons mèdiques (Grow, Elgin i Weintraub, 2006; Kerner, 2018). De fet, els falsificadors se centren freqüentment en medicaments per a la salut sexual, com Viagra, Cialis i altres relacionats amb la disfunció erèctil (Fox, 2004). Això es deu en part al cada vegada major ús de medicaments amb recepta arreu del món, ja sigui per a afeccions cròniques o per al consum addictiu associat amb opioides (Cicero i Ellis, 2012; Finely, 2009). A més, alguns consideren que el preu dels medicaments receptats és massa alt per pagar-lo mitjançant canals legítims (Cicero i Ellis, 2012). Finalment, alguns consumidors informen que estan massa avergonyits per demanar medicaments amb recepta que serveixen de tractament a necessitats de salut sexual i mental (Finley, 2009).

Resum

En general, el robatori de propietat intel·lectual s'ha tornat molt més fàcil arran del sorgiment d'internet i la tecnologia informàtica. La gent té innombrables oportunitats d'adquirir propietat intel·lectual, ja sigui piratejant música, pel·lícules o comprant productes falsificats. A mesura que la tecnologia es torni més fàcil d'utilitzar i permeti l'accés a totes les formes de contingut a escala mundial, és probable que aquests delictes econòmics continuïn evolucionant. Com a conseqüència, el sistema de justícia penal es veurà obligat a canviar les seves estratègies per repercutir directament sobre aquests delictes en el context d'un mercat global.

Bibliografia

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

BASCAP (2016). «The economic impacts of counterfeiting and piracy» [en línia]. <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, pàg. 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, pàg. 1157-1184).

Business Software Alliance (2016). *Seizing opportunity through license compliance* [en línia]. <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*. Nova 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, pàg. 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, pàg. e174).

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

Cooper, J.; Harrison, D. M. (2001). «The social organization of audio piracy on the Internet». *Media, Culture, and Society* (núm. 23, pàg. 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, pàg. 749-771).

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

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

Fox, S. (2004). *Prescription drugs online* [en línia]. 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». A: *CCS07* (20 d'octubre - 2 de novembre, 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, pàg. 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 línia]. *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, pàg. 15-28).

Herper, M. (2005). «Bad medicine» [en línia]. *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, pàg. 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, pàg. 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, pàg. 378-395).

Holt, T. J.; Bossler, A.; Seigfried-Spellar, K. C. (2017). Cybercrime and Digital Forensics: An IntroductionLondres: 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, pàg. 15-30).

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

Jamieson, C. (2 de gener de 2018). «Fakes get sneakier on social media» [en línia]. *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 línia]. *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, pàg. 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, pàg. 196-214).

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

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

Little, T. (31 de maig de 2018). «As cosmetic counterfeiters turn to social media, consumers expect brands to protect them» [en línia]. *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, pàg. 333-350).

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

Miller, B. M.; Morris, R. G. (2016). «Virtual peer effects in social learning theory». *Crime & Delinquency* (vol. 62, núm. 12, pàg. 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». A: T. J. Holt (ed.). *Crime On-line: Causes, Correlates, and Context* (pàg. 61-80). Raleigh, NC: Carolina Academic Press.

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

Parsons, S. (4 de juny 2018). «Social media now contributes to 50 % of counterfeit cosmetics sales» [en línia]. *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. (febrer de 2005). «The bit torrent P2P file-sharing system: Measurements and analysis». A: 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, pàg. 495-518).

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

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

Stokel-Walker, C. (23 de març de 2019). «To compete with Netflix, online piracy is upping its game» [en línia]. *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 línia]. <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, pàg. 124-151).

U. S. Department of Homeland Security (2018). *Intellectual Property Rights Seizure Statistics: Fiscal Year 2017* [en línia]. <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 línia]. <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». A: *Proceedings of the 24th International Conference on World Wide Web* (pàg. 1188-1197). International World Wide Web Conferences Steering Committee.

Wall, D. S. (2001). «Cybercrimes and the Internet». A: D. S. Wall (ed.). *Crime and the Internet* (pàg. 1-17). Nova York: Routledge.

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

Wolfram, J. (22 d'octubre de 2017). «Why kicking out counterfeit crooks on Instagram is so important» [en línia]. *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, pàg. 317-333).

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