# Comprendre el delicte cibernètic i els delictes econòmics

PID_00270000

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

El desenvolupament d'ordinadors i internet els últims trenta anys ha transformat radicalment el món, la qual cosa ha suposat que la comunicació i el comerç siguin inherentment més fàcils i ràpids. Un dels beneficis més immediats dels ordinadors, dels telèfons mòbils i d'internet rau en el fet que ara podem obtenir informació de qualsevol persona o cosa en un instant. El fet de poder adquirir coneixement de persones, llocs i productes des de qualsevol indret del món permet, teòricament, que els éssers humans estiguin més informats en tots els aspectes de la seva vida. Com a conseqüència d'això, la connexió a internet ha augmentat substancialment en les nacions occidentalitzades. Aproximadament el 85% de la població dels països membres de la UE fan servir Internet, amb una proporció d'ús superior a Alemanya i al Regne Unit (Internet World Stats, 2019). Molts usuaris d'internet graviten al voltant de plataformes de xarxes socials, com ara Facebook i Twitter, que permeten que les persones comparteixin punts de vista i opinions sense haver d'interaccionar físicament amb d'altres. De fet, gairebé el 85% de la població dels països europeus fa servir Facebook, en comparació amb una taxa general d'ús del 50% respecte a la resta del món (Internet World Stats, 2019).

De la mateixa manera, l'augment de les compres en línia per mitjà de plataformes de comerç electrònic com Amazon permet que els consumidors obtinguin pràcticament qualsevol article imaginable a tot el món i a bon preu (Wilson, 2011). Les taxes de compres en línia varien segons el lloc, i els països asiàtics tenen un percentatge de compradors en línia més elevat en comparació amb la majoria dels països de la UE (Statista, 2019). L'evidència suggereix que habitualment els consumidors busquen productes des del telèfon mòbil per després comprar mitjançant l'ordinador de taula o el portàtil (Chaffey, 2019). Aquestes transaccions sovint estan habilitades pels processadors de pagaments financers que faciliten les transferències immediates de fons entre comptes mitjançant els sistemes bancaris tradicionals, com també per sistemes de pagaments de tercers, com ara Verse.

Els beneficis inherents a la innovació tecnològica es manifesten en tota la societat, la qual cosa implica canvis en el comportament humà en línia i fora de línia. El creixement de les comunicacions intervingudes per ordinador (*computer-mediated communications*, CMC), com ara el correu electrònic i la missatgeria instantània, ha reestructurat les relacions interpersonals, com també la manera en què interaccionem amb les empreses i les agències governamentals. Com a resultat, els agents infractors i criminals han començat a traslladar-se a espais en línia per delinquir, sigui mitjançant l'ús de CMC o la manipulació directa i la subversió d'ordinadors i internet, amb la finalitat de causar danys.

En aquest material s'analitzaran aquests fenòmens i es destacaran les característiques que distingeixen els delictes facilitats per la tecnologia d'aquells que són considerats delictes tradicionals.

# 1. Definició de l'ús indegut i l'ús maliciós d'ordinadors

El gran potencial d'internet per participar en atacs contra la seva infraestructura, les dades i els usuaris exigeix un conjunt clar de definicions per entendre aquests fenòmens. Amb aquesta finalitat, la majoria dels investigadors han aplicat definicions tradicionals d'irregularitats en entorns virtuals. Per exemple, alguns experts utilitzen l'expressió *infracció cibernètica* per referir-se a l'ús de la tecnologia per participar en comportaments que infringeixen els estàndards o valors locals, encara que no siguin il·legals per llei (Holt, Bossler i May, 2012; Udris, 2016).

**Ciberinfracció no il·legal**

Un exemple de ciberinfracció excel·lent és aquell que afecta persones que consumeixen contingut pornogràfic a través de llocs web i plataformes de xarxes socials (Holt i altres, 2013; Shamsudin, Subramaniam i Alshuaibi, 2012). Aquest comportament pot anar en contra dels estàndards comunitaris de decència o moralitat, encara que no és il·legal en si (Quinn i Forsyth, 2013).

Per contra, els actes delictius són comportaments que infringeixen els estatuts legals codificats i comporten sancions en l'àmbit local, estatal, federal o nacional. Molts països no utilitzen l'expressió *delicte cibernètic* en el Codi penal, sinó que identifiquen les accions que violen la llei per mitjà de diferents tecnologies. Això es deu a la manca de consens pel que fa al significat de *cibercrim*, i al seu ús en la comunitat d'investigadors i professionals.

Per exemple, en la dècada dels noranta i a principis del segle XXI, els termes *cibercrim* i *delicte informàtic* es van emprar per referir-se a activitats delictives relacionades amb la tecnologia (Goodman, 1997; Hollinger i Lanza-Kaduce, 1988). Alguns van fer servir *delicte informàtic* per referir-se a activitats en les quals el delinqüent va aplicar un coneixement especial sobre els ordinadors, mentre que el delicte cibernètic es va emprar per al·ludir a aquells delictes que es van cometre com a resultat d'un ús especialitzat del ciberespai (Furnell, 2002; Wall, 2001).

A mitjans de la primera dècada d'aquest segle, gairebé tots els ordinadors i dispositius mòbils es van habilitar per wifi, la qual cosa va fer que tant els investigadors com els periodistes deixessin d'emprar l'expressió *delicte informàtic* en favor de *delicte cibernètic* o *cibercrim* (Wall, 2007).

Com a resultat, *cibercrim* és el terme preferit per referir-se a l'ús maliciós de la tecnologia.

Una altra preocupació creixent entre els encarregats de formular polítiques rau en la intersecció del mal ús de la tecnologia amb aquella tecnologia que serveix a motivacions ideològiques i polítiques, cosa que a vegades s'anomena *ciberterror* (Foltz, 2004; Holt, 2012). Si bé no hi ha una definició única per a *ciberterrorisme*, alguns acadèmics coincideixen a afirmar que implica l'ús de la tecnologia per apuntar a una plataforma digital, un sistema informàtic o una

xarxa (Britz, 2010; Foltz, 2004; Jarvis i MacDonald, 2015). Alguns autors, com ara Britz (2010), suggereixen que el ciberterror també pot incloure l'ús de plataformes de comunicacions per reclutar i radicalitzar-ne d'altres d'acord amb el sistema de creences (vegeu Britz, 2010). Al mateix temps, aquesta definició pot ser massa genèrica, ja que pràcticament qualsevol ús de tecnologia que facin terroristes i extremistes es podria considerar ciberterror (Jarvis i MacDonald, 2015). Per tant, els investigadors generalment consideren que el ciberterror és l'ús que es fa de la tecnologia per danyar o alterar la tecnologia i els sistemes de comunicació en línia amb una motivació ideològica (Holt, Stonhouse, Freilich i Chermak, 2019; Jarvis i MacDonald, 2015).

## 2. Una tipologia de cibercrim

El concepte *delicte cibernètic* implica un desafiament per al públic en general, com també per als investigadors i encarregats de formular polítiques, ja que es poden produir molts usos indeguts de la tecnologia. Com a resultat, alguns autors han argumentat que cal una tipologia de cibercrim per ajudar a diferenciar les formes de delinqüència que es poden dur a terme (vegeu, per exemple, Holt, 2013; Wall, 2001). David Wall (2001) va crear un dels marcs més àmpliament citats per classificar els delictes cibernètics; va suggerir que hi havia quatre formes de delicte: 1) ciberinvasió, 2) ciberfrau i robatori, 3) ciberpornografia i delictes de pornografia i 4) ciberviolència. Aquestes categories reflecteixen delictes tant instrumentals com expressius, així com la utilització de diferents habilitats i coneixements tecnològics per cometre aquests delictes.

El primer, la **ciberinvasió**, es refereix als intents de creuar els límits invisibles de les propietats en espais virtuals, de manera similar al robatori i a la violació de domicili (Wall, 2001).

> Per exemple, l'ús de contrasenyes per protegir el correu electrònic i els comptes de xarxes socials, així com les xarxes wifi i els sistemes informàtics, són intents d'evitar que un recurs sigui mal emprat per persones que no estan autoritzades a utilitzar aquests serveis. Els usuaris que no hi estan autoritzats i que han d'intentar aconseguir la clau o utilitzar altres mitjans més sofisticats tècnicament traspassen una barrera clara de control en intentar tenir accés sense el permís de l'operador.

La majoria dels actes associats amb la ciberintrusió provenen de *hackers* que utilitzen els coneixements de maquinari i programari per accedir a sistemes informàtics, comptes de correu electrònic i sistemes i serveis protegits que no són propietat seva (Furnell, 2002; Jordan i Taylor, 1998). L'acte de piratejar no és inherentment il·legal, i pot usar-se per protegir els sistemes i posar a prova la seva seguretat. Els membres del públic general no solen comprendre aquesta diferència, de manera que culpen els *hackers* de delictes greus que afecten els sistemes financers i causen danys als ciutadans, la indústria i el govern per igual (vegeu el mòdul 2 per a més detalls).

El segon tipus de ciberdelicte segons Wall (2001) implica actes de **frau cibernètic i robatori**, que poden ser el resultat directe de diverses activitats de ciberintrusió. Aquesta categoria, que és molt àmplia, abasta una sèrie de mètodes que es poden utilitzar per obtenir informació, béns o serveis de persones i xarxes informàtiques. Això pot incloure el robatori d'informació personal provinent de bases de dades mitjançant l'ús de tècniques de pirateria o eines de programari maliciós. A més, els delinqüents poden adquirir de manera fraudulenta informació personal directament de les víctimes mitjançant l'ús de correus electrònics i perfils de xarxes socials falsos (James, 2005; Ponemon Ins-

titute, 2018). Independentment del mètode que empri, el delinqüent pot fer servir aquestes dades per dur a terme transaccions financeres no autoritzades o vendre-les per fer-ne ús (Holt i Lampke, 2010; Yip i altres, 2013).

El robatori cibernètic també inclou diverses formes d'adquirir propietat intel·lectual sense pagar al titular original dels drets d'autor o al creador de contingut, generalment a través de mitjans no autoritzats de còpia de mitjans digitals (Gopal, Saunders, Bhattacharjee, Agrawal i Wagner, 2004).

**Pirateria digital**

La pirateria digital suposa grans costos per al propietari de la propietat intel·lectual, ja que, segons diversos informes, la indústria discogràfica dels Estats Units perd més de dotze mil milions de dòlars l'any només per descàrregues il·legals de música (Siwek, 2007). La venda de productes falsificats també s'inclou en aquesta tipologia; aquests productes es venen fàcilment a través de minoristes en línia a consumidors que poden no adonar-se de la procedència real (Kennedy, 2016; Wall, 2010).

L'auge de la tecnologia també ha estès un tercer tipus de delicte relacionat amb la **ciberpornografia i el contingut pornogràfic**. Aquesta categoria inclou, específicament, la creació i la difusió de contingut sexualment explícit per mitjà de proveïdors legítims, així com dels creadors de contingut *amateur* que utilitzen eines de captura d'àudio i vídeo d'alta definició (Lane, 2000). A més, hi ha una gran quantitat de serveis sexuals que operen a través de plataformes de comunicació intervingudes per ordinador, com ara les prostitutes que s'anuncien en llocs web com Backpage (Cunningham i Kendall, 2013; Finn i Stalans, 2016). Finalment, la tecnologia ha estat utilitzada per pedòfils per adquirir imatges i vídeos de joves que participen en actes sexuals (Jenkins, 2001; Quayle i Taylor 2002). Una petita proporció de delinqüents també empra la tecnologia per enganyar menors d'edat i aconseguir el contacte i abús sexual fora de línia (Wolak, Finkelhor i Mitchell, 2004; Wolak, Mitchell i Finkelhor, 2003).

L'última categoria assenyalada per Wall inclou actes de **violència cibernètica** per mitjà dels quals un delinqüent utilitza la tecnologia per enviar, rebre o accedir en línia a materials nocius, punyents o perillosos. Aquests delictes afecten tant joves com adults, ja que les xarxes socials permeten que la informació sobre els altres s'observi en temps gairebé real i sempre romangui en línia (Finkelhor, Mitchell i Wolak, 2000; Finn, 2004; Hinduja i Patchin, 2009; Holt i Bossler, 2009). La naturalesa del delicte varia des de l'assetjament, l'amenaça o els missatges sexuals enviats per correu electrònic, text o alguna altra forma de CMC (Bocij, 2004; Finn, 2004). El contingut d'un missatge també pot adreçar-se a un sol individu o a grups socials més amplis que poden associar-se més comunament amb grups d'odi i violència política en el món real (Hegghammer, 2013; Holt, 2012; Weimann, 2011). A més, aquells *hackers* i agents motivats ideològicament poden atacar els espais virtuals per participar en actes de terrorisme o extremisme en plataformes en línia (vegeu Holt i altres, 2019).

# 3. Reconèixer les motivacions després dels delictes cibernètics

La diversitat de delictes que es classifiquen com a ciberdelictes posa en qüestió per què els actors s'han adaptat als espais virtuals. La primera raó, i la més directa, seria la facilitat amb la qual es pot utilitzar la tecnologia per infringir la llei. Els ordinadors, els telèfons mòbils i la connexió a internet són relativament econòmics i fàcils d'adquirir en gairebé qualsevol país del món. De fet, no cal tenir un ordinador; només cal disposar d'accés a internet en un cibercafè o en una biblioteca pública. Molts ciberdelictes també requereixen una competència tècnica mínima per part de l'infractor. Si bé se suposa que tots els *hackers* tenen habilitats tecnològiques, molts dels seus atacs s'aprofiten de simples errors de seguretat o de descuits comesos pels usuaris (Holt i Bossler, 2016; Ponemon Institute, 2018). A més, ara hi ha una sèrie de proveïdors de serveis que ofereixen eines i serveis de pirateria a canvi d'una tarifa (Holt, 2013; Hutchings i Clayton, 2016; Leukfeld i altres, 2017). Per tant, ja no cal tenir una gran experiència informàtica per cometre un delicte cibernètic si es pot pagar a una altra persona per fer atacs cibernètics en nom seu (Holt, Smirnova, Chua i Copes, 2015).

La connexió a internet i la tecnologia informàtica també permeten que els delinqüents ataquin amb èxit un gran nombre de persones, corporacions i entitats simultàniament i des de qualsevol part del món. En la realitat, la tria de les víctimes està influenciada per les capacitats del delinqüent, com ara les dimensions, la rapidesa o l'ús d'una arma per intimidar aquestes víctimes (Miller, 1998; Wright i Decker, 1997). Fins i tot en el millor dels casos, sovint un delinqüent no pot participar físicament en un atac a un grup per la possibilitat de ser aplacat per les seves víctimes. Aquestes característiques físiques són absents en els entorns virtuals, en què els delinqüents tenen temps per adquirir quantitats massives d'informació sobre individus i empreses. Després poden adreçar-se a possibles víctimes per diferents punts de contacte, com ara el correu electrònic i les xarxes socials o bé diferents formes de programari maliciós en el context de la pirateria (Cross, 2015; Holt i Kilger, 2012; Whitty, 2013).

> Internet, sense fronteres i sota demanda, també torna absurdes les relacions físiques i espacials tradicionals, cosa que fa que les víctimes quedin potencialment vulnerables davant els delinqüents en tot moment (Yar, 2005).

Un altre avantatge del ciberdelicte des de la perspectiva del delinqüent és que el risc de detecció i arrest per part dels agents policials és més petit que en els espais físics. Els delinqüents que participen en delictes personals i de propietat

en el món real han de prendre mesures per ocultar la identitat: utilitzar roba ampla o fer canvis d'aspecte (Miller, 1998; Wright i Decker, 1997). En espais virtuals, en canvi, hi ha pocs factors relacionats amb l'aparença física que es poden identificar en un delinqüent, com ara l'alçada, el pes i la raça (Wall, 2001). Les persones poden crear identitats falses a través del correu electrònic i les xarxes socials per ajudar a ocultar la seva identitat real envers les víctimes (Bocij, 2004). Des d'un punt de vista tècnic, els delinqüents poden amagar-se fàcilment mitjançant l'ús de servidors intermediaris que ocultaran informació sobre la seva ubicació física. Alguns fins i tot utilitzen ordinadors aliens per encobrir més fàcilment les seves accions i entorpir el procés d'investigació (Holt, 2013).

No només és difícil conèixer la veritable identitat de l'usuari en el ciberespai, sinó que també pot ser extremament complicat arrestar-lo i processar-lo en cas que participi en certes formes de delicte cibernètic. Si bé la majoria de les nacions industrialitzades tenen lleis relacionades amb el cibercrim i l'ús indegut de la tecnologia, no han establert relacions consistents que permetin investigacions transnacionals de delictes (Brenner, 2008; Wall, 2007).

**Exemple**

Les persones que viuen a Rússia i que ataquen sistemes informàtics als Estats Units poden estar violant les lleis de tots dos països. No obstant això, no hi ha una relació d'extradició entre aquestes dues nacions, la qual cosa fa difícil portar aquest individu als Estats Units per ser jutjat pels seus delictes. Aquests factors poden provocar que els delinqüents ataquin selectivament determinats països, atès el petit risc de detecció percebut (Brenner, 2008).

Els desafiaments que hi ha en la detecció i la investigació del delicte cibernètic també afecten la probabilitat que les víctimes denunciïn les seves experiències a la policia. Algunes formes de delicte cibernètic, com ara la pirateria informàtica, poden passar desapercebudes per la víctima fins que es produeix efectivament el delicte. Amb la pirateria, les víctimes poden pensar que la lentitud del seu sistema informàtic o el mal funcionament es deu, simplement, a un problema tècnic (Holt i Bossler, 2013; Ngo i Paternoster, 2011). Els errors i els desperfectes poden ser un símptoma d'infeccions de programari maliciós o algun altre risc informàtic, de manera que la víctima ja pot haver perdut arxius clau o informació confidencial. El programari de protecció, com ara les eines antivirus, pot disminuir la probabilitat que un atac es produeixi amb èxit, encara que només sigui efectiu si l'usuari sap com utilitzar correctament aquesta eina en el seu sistema informàtic (vegeu Holt i Bossler, 2016). Si una persona no actualitza sovint el programari o fa que escanegi activament els arxius que intenta descarregar, és possible que no sigui tan útil per protegir el sistema.

En alguns casos, les víctimes també poden sentir-se massa avergonyides per denunciar el delicte a la policia, la qual cosa redueix la probabilitat d'investigarlo. Algunes formes de frau en línia requereixen que la víctima i el delinqüent interaccionin directament, de manera que la primera se sent còmplice del delicte. Com a resultat, poden arribar a pensar que la seva experiència serà ignorada per la policia, o que fins i tot poden haver comès algun delicte, cosa

que incrementaria la seva por d'informar (Button, 2012; Button, Nicholls, Kerr i Owen, 2014; Cross, 2015). Moltes empreses i grans organitzacions tampoc estan disposades a informar que han estat blanc de ciberdelinqüents per la preocupació que els seus clients puguin perdre la fe en ells i recórrer als serveis d'altres proveïdors (Brenner, 2008; Holt, 2003). De la mateixa manera, poden pensar que un atac reduirà els preus de les accions i tindrà un impacte negatiu en el valor de l'empresa (Holt i Bossler, 2016). Per això, molts defensen que els ciberdelictes són un problema molt poc reportat en els països occidentals.

# 4. Identificació d'un ciberdelicte econòmic

Tot i que la tecnologia ha influït en quasi tots els tipus de delinqüència, probablement aquest impacte és més gran en els delictes econòmics. Els actes de robatori cibernètic, incloent-hi diverses formes de frau, són efectuats molt més fàcilment i poden afectar una població de víctimes més gran a causa de l'ús d'internet i dels ordinadors (Baker i Faulkner, 2003; Grabosky, 2007). Així doncs, alguns defineixen aquests delictes com a *delictes cibernètics*, ja que els delictes tradicionals se simplifiquen amb l'ús de la tecnologia (Holt, 2015; Wall, 2007). Al mateix temps, els actes de ciberintrusió que s'adrecen directament a sistemes informàtics i repositoris de dades són únics i donen noves oportunitats als delinqüents per accedir a informació confidencial a tot el món. Aquests crims poden produir un dany econòmic important, i es consideren delictes ciberdependents, ja que no poden existir sense ordinadors i connexió a internet.

De fet, l'auge d'internet i dels ordinadors va produir dos canvis socials clau que afecten directament el risc de dany econòmic que pot haver-hi. En primer lloc, els ciutadans han perdut el control de la seva informació d'identificació personal (*personally identifiable information*, PII), que comprèn des de detalls simples com el nom, l'adreça i la data de naixement fins a la informació molt més sensible, com ara hàbits de compra i preferències polítiques (Byer, 2018; Federal Trade Commission, 2016). La gran quantitat de dades que ara estan disponibles en tots els serveis en línia sobre un individu també suposa una amenaça per a la seguretat pública. Els webs de comerç electrònic retenen informació financera del client per permetre compres immediates i el lliurament ràpid de productes. La seguretat d'aquesta informació no està garantida i depèn completament dels protocols de seguretat que les companyies estableixin per assegurar la confidencialitat i privacitat de les dades (Brown, 2019).

> Aquesta informació té un valor substancial, ja que es pot utilitzar per obtenir targetes de crèdit, préstecs i diversos serveis d'agències governamentals (Federal Trade Commission, 2016).

En segon lloc, les companyies i les xarxes socials han monetitzat la informació sobre els interessos, els comportaments i la identitat individuals dels consumidors. Això es deu, sobretot, a l'ús voluntari de xarxes socials per part de la població i a la seva predisposició per compartir la informació en la comunitat mundial (Byer, 2018). Les plataformes com Facebook i Twitter guanyen diners en oferir serveis de publicitat a empreses i organitzacions que poden adaptar els missatges a un públic molt reduït, basat en coneixements demogràfics i de comportament obtinguts de les seves publicacions (Byer, 2018; Zunger, 2018).

A més, els llocs web de comerç electrònic i els minoristes físics registren el comportament dels clients i ofereixen accés a la seva informació a canvi d'una tarifa de serveis. Com a conseqüència, la majoria de la informació sobre les vides dels usuaris en línia i fora de línia s'està fusionant per esdevenir fonts de dades que les corporacions poden estudiar i utilitzar per a una millor captació de minoristes i clients (Zunger, 2018).

Com a resultat, la tecnologia ha permès una varietat de possibles delictes comunament coneguts com a *frau*. Els actes de frau es poden definir generalment com l'adquisició delictiva de diners o propietats de les víctimes mitjançant l'ús d'enganys o trampes (vegeu, per exemple, Baker i Faulkner, 2003). Això últim pot suposar una organització complexa, amb múltiples delinqüents que coordinen les seves forces, o delictes comesos per un únic agent (Button i altres, 2012; Graobsky, 2007). Molts d'aquests plans d'actuació delictiva impliquen l'ús indegut dels CMC, especialment el correu electrònic i les pàgines web, per presentar una imatge suggerent que pugui atraure possibles víctimes. Al seu torn, la víctima pot proporcionar voluntàriament informació personal i detalls financers als delinqüents (Button, 2012; Whitty, 2013). Altres formes de frau no requereixen la interacció amb les víctimes, ja que el delinqüent simplement ataca les bases de dades financeres corporatives i els sistemes de pagament per aconseguir informació confidencial (James, 2005; Holt i Lampke, 2010).

Aquestes condicions han creat un entorn en què els delinqüents poden adquirir informació confidencial de diverses maneres per defraudar tant bancs com proveïdors de serveis financers, sol·licitar serveis il·legalment o crear documents d'identitat falsos, com ara passaports i carnets de conduir, per ocultar la seva veritable identitat davant les forces policials.

El públic en general, els legisladors i els investigadors sovint es refereixen a aquestes activitats com a *frau* o *robatori d'identitat*.

El significat i l'ús de cada terme varia segons el lloc, encara que sovint es fan servir indistintament (Copes i Vieraitis, 2009; Koops, Leenes, Meints, Van der Meulen i Jaquet-Chiffelle, 2009). Per exemple, els investigadors nord-americans han definit el robatori d'identitat com l'ús o la possessió il·legal dels documents d'identitat d'una altra persona per cometre, donar suport o participar en activitats il·legals (Allison, Schuck i Learsch, 2005; Copes i Vieraitis, 2009). L'Oficina d'Estadístiques Judicials dels Estats Units va definir el robatori d'identitat de manera una mica diferent, ja que se centrava en els seus aspectes econòmics, incloent-hi «l'ús indegut amb èxit d'un compte existent, com un compte de targeta de dèbit o crèdit, l'ús indegut d'informació personal per obrir un compte nou o l'ús indegut d'informació personal per a altres finalitats fraudulentes, com ara obtenir préstecs públics o proporcionar informació falsa a la policia en un delicte o en un control de trànsit» (Harrell, 2014).

El concepte *robatori d'identitat* s'empra en altres països occidentals per reflectir l'ús indegut de la informació d'identificació personal d'una altra persona per tal d'obtenir diners, crèdit, béns o serveis en nom seu, com també per habilitar altres formes de frau financer (National Fraud Authority, 2013).

Independentment del llenguatge utilitzat, els delictes d'identitat són un problema greu a tot el món (Button, 2012; Harrell, 2019). De fet, l'amenaça potencial de diverses formes de frau i robatori d'identitat és alta en tota la Unió Europea, a causa de la facilitat de l'encreuament de fronteres i les comunicacions per internet en general (Button, 2012). És difícil avaluar l'impacte econòmic d'aquests delictes atesa la manca de denúncies i les dificultats per determinar el nombre de víctimes, sobretot quan es tenen en compte els casos de victimització transnacionals (Anderson i altres, 2013; Button, 2012; Internet Crime Complaint Center, 2018).

Un exemple en són les dades recopilades als Estats Units que demostraven que hi va haver més de catorze milions de víctimes de robatori d'identitat el 2012, amb pèrdues variables en funció de l'ús de la informació. Aquestes víctimes van perdre una mitjana de 552 $ quan el delinqüent havia utilitzat la seva targeta de dèbit, mentre que si aquest havia fet ús de la targeta de crèdit de les víctimes, les pèrdues eren de 1.448 $ (Harrell, 2019).

Per tant, no podem ignorar l'abast del dany causat pel delicte d'identitat i la seva relació amb el frau i el delicte cibernètic en general.

# Resum

Mentre els avenços tecnològics continuïn transformant la societat, aquests canvis també influiran sobre els delictes financers i la criminalitat. En aquest material es dona una visió general de les formes més comunes de frau i robatori emprades pels delinqüents en els mitjans tecnològics i, a més, s'exploraran els factors associats amb la victimització per avaluar l'abast del dany que es produeix amb aquests delictes. Cada mòdul se centra en diferents delictes i formes de cibercrim econòmic. Aquest primer mòdul ens introdueix el delicte cibernètic i els delictes econòmics que hi estan relacionats. El mòdul 2 examina els actes de ciberintrusió, concretament la pirateria informàtica i les infeccions de programari maliciós. El mòdul 3 analitza el problema de les targetes o el robatori i la venda d'informació financera adquirida per mitjà de diferents formes de ciberintrusió. El mòdul 4 considera els diversos fraus que pot haver-hi a través del correu electrònic, incloent-hi correus nigerians i estafes romàntiques. El mòdul 5 detalla les amenaces plantejades pel robatori de propietat intel·lectual, incloent-hi la falsificació de productes i la pirateria digital. El mòdul 6 aborda els nous ciberdelictes econòmics que es poden produir en funció del canvi tecnològic.

# Bibliografia

**Allison, S. F. H.; Schuck, A. M.; Learsch, K. M.** (2005). «Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics». *Journal of Criminal Justice* (núm. 33, pàg. 19-29).

**Anderson, R.; Barton, C.; Böhme, R.; Clayton, R.; Van Eeten, M. J.; Levi, Moore, T.; Savage, S.** (2013). «Measuring the cost of cybercrime». A: *The economics of information security and privacy* (pàg. 265-300). Berlín/Heidelberg: Springer.

**Baker, W. E.; Faulkner, R. R.** (2003). «Diffusion of fraud: Intermediate economic crime and investor dynamics». *Criminology* (vol. 41, núm. 4, pàg. 1173-1206).

**Bocij, P.** (2004). *Cyberstalking: Harassment in the Internet Age and How to Protect your Family*. Westport, CT: Praeger.

**Brenner, S. W.** (2008). *Cyberthreats: The Emerging Fault Lines of the Nation State*. Nova York: Oxford University Press.

**Britz, M. T.** (2010). «Terrorism and Technology: Operationalizing Cyberterrorism and Identifying Concepts». A: T. J. Holt (ed.). *Crime On-Line: Correlates, Causes, and Context* (pàg. 193-220). Raleigh, NC: Carolina Academic Press.

**Brown, E.** (2019). «Two thirds of US consumers say government should do more to protect data privacy» [en línia]. *ZDNet* (22 de gener). <https://www.zdnet.com/article/two-thirds-of-us-consumers-say-government-should-do-more-to-protect-data-privacy/>

**Button, M.** (2012). *Private policing*. Nova York: Willan.

**Button, M.; Nicholls, C. M.; Kerr, J.; Owen, R.** (2014). «Online frauds: Learning from victims why they fall for these scams». *Australian & New Zealand Journal of Criminology* (vol. 47, núm. 3, pàg. 391-408).

**Byer, B.** (2018). «Internet users worry about online privacy but feel powerless to do much about it» [en línia]. *Entrepreneur* (20 de juny). <https://www.entrepreneur.com/article/314524>

**Chaffey, D.** (2019). «E-commerce conversion rates- how do yours compare?» [en línia]. *Smart Insights*. <https://www.smartinsights.com/ecommerce/ecommerce-analytics/ecommerce-conversion-rates/>

**Copes, H.; Vieraitis, L. M.** (2009). «Bounded rationality of identity thieves: Using offender-based research to inform policy». *Criminology & Public Policy* (vol. 8, núm. 2, pàg. 237-262).

**Cross, C.** (2015). «No laughing matter: Blaming the victim of online fraud». *International Review of Victimology* (núm. 21, pàg. 187-204).

**Cunningham, S.; Kendall, T.** (2013). «Sex for Sale: Online Commerce in the World's Oldest Profession». A: T. J. Holt (ed.). *Crime On-Line: Correlates, Causes, and Context* (2a. ed., pàg. 40-75). Raleigh, NC: Carolina Academic Press.

**Federal Trade Commission** (2016). *Consumer Sentinel Network Data Book for January - December 2016* [en línia]. <https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf>

**Finkelhor, D.; Mitchell, K. J.; Wolak, J.** (2000). *Online Victimization: A Report on the Nation's Youth*. Washington DC: National Center for Missing and Exploited Children.

**Finn, J.** (2004). «A survey of online harassment at a university campus». *Journal of Interpersonal Violence* (núm. 19, pàg. 468-483).

**Finn, M. A.; Stalans, L. J.** (2016). «Understanding how the internet facilitates crime and deviance. *Victims and Offenders* (núm. 11, pàg. 501-508).

**Foltz, B. C.** (2004). «Cyberterrorism, computer crime, and reality». *Information Management & Computer Security* (vol. 12, núm. 2, pàg. 154-166).

**Furnell, S.** (2002). *Cybercrime: Vandalizing the Information Society*. Boston: Addison-Wesley.

**Goodman, M. D.** (1997). «Why the police don't care about computer crime». *Harvard Journal of Law and Technology* (núm. 10, pàg. 465-494).

**Gopal, R.; Sanders, G. L.; Bhattacharjee, S.; Agrawal, M. K.; Wagner, S. C.** (2004). «A behavioral model of digital music piracy». *Journal of Organizational Computing & Electronic Commerce* (núm. 14, pàg. 89-105).

**Grabosky, P. N.** (2007). *Electronic crime*. Upper Saddle River, NJ: Pearson Prentice Hall.

**Harrell, E.** (2019). *Victims of Identity Theft, 2016 (NCJ 248991)* [en línia]. <www.bjs.gov/index.cfm?ty=pbdetail&iid=5408>

**Hegghammer, T.** (2013). «Should I Stay or Should I Go? Explaining Variation in Western Jihadists' Choice Between Domestic and Foreign Fighting». *American Political Science Review* (núm. 107, pàg. 1-15).

**Hinduja, S.; Patchin, J. W.** (2009). *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying*. Nova York: Corwin Press.

**Hollinger, R. C.; Lanza-Kaduce, L. O. N. N.** (1988). «The process of criminalization: The case of computer crime laws». *Criminology* (vol. 26, núm. 1, pàg. 101-126).

**Holt, T. J.** (2012). «Exploring the Intersections of Technology, Crime and Terror». *Terrorism and Political Violence* (vol. 24, núm. 2, pàg. 337-354).

**Holt, T. J.** (2013). «Exploring the social organisation and structure of stolen data markets». *Global Crime* (vol. 14, núm. 2-3, pàg. 155-174).

**Holt, T. J.; Bossler, A. M.** (2009). «Examining the applicability of lifestyle-routine activities theory for cybercrime victimization». *Deviant Behavior* (núm. 30, pàg. 1-25).

**Holt, T. J.; Bossler, A. M.** (2013). «Examining the relationship between routine activities and malware infection indicators». *Journal of Contemporary Criminal Justice* (vol. 29, núm. 4, pàg. 420-436).

**Holt, T. J.; Bossler, A. M.** (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Londres: Routledge.

**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.; Kilger, M.** (2012). «Know your enemy: The social dynamics of hacking» [en línia]. *The Honeynet Project*. <https://honeynet.org/files/Holt%20and%20Kilger%20-%20KYE%20-%20The%20Social%20Dynamics%20of%20Hacking.pdf>

**Holt, T. J.; Lampke, E.** (2010). «Exploring stolen data markets on-line: Productes and market forces». *Criminal Justice Studies* (núm. 23, pàg. 33-50).

**Holt, T. J.; Smirnova, O.; Chua, Y. T.; Copes, H.** (2015). «Examining the risk reduction strategies of actors in online criminal markets». *Global Crime* (vol. 16, núm. 2, pàg. 81-103).

**Holt, T. J.; Stonhouse, M.; Freilich, J.; Chermak, S. M.** (2019). «Examining Ideologically Motivated Cyberattacks Performed by Far-Left Groups». *Terrorism and Political Violence* (pàg. 1-22).

**Hutchings, A.; Clayton, R.** (2016). «Exploring the provision of online booter services». *Deviant Behavior* (vol. 37, núm. 10, pàg. 1163-1178).

**Internet Crime Complaint Center** (2018). *Federal Bureau of Investigation Internet Crime Complaint Center (IC3)* [en línia]. <https://www.ic3.gov/about/default.aspx>

**Internet World Stats** (2019). «Internet Users by Country, 2019» [en línia]. <http://www.internetlivestats.com/>

**James, L.** (2005). *Phishing Exposed*. Rockland: Syngress.

**Jarvis, L.; MacDonald, S.** (2015). «What is cyberterrorism? Findings from a survey of researchers». *Terrorism and Political Violence* (vol. 27, núm. 4, pàg. 657-678).

**Jenkins, P.** (2001). *Beyond Tolerance: Child Pornography on the Internet*. Nova York: New York University Press.

**Jordan, T.; Taylor, P.** (1998). «A sociology of hackers». *The Sociological Review* (núm. 46, pàg. 757-780).

**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).

**Koops, B. J.; Leenes, R.; Meints, M.; van der Meulen, N.; Jaquet-Chiffelle, D. O.** (2009). «A typology of identity-related crime: Conceptual, technical, and legal issues». *Information, Communication & Society* (vol. 12, núm. 1, pàg. 1-24).

**Lane, F. S.** (2000). *Obscene Profits: The Entrepreneurs of Pornography in the Cyber Age*. Nova York: Routledge.

**Leukfeldt, E. R.; Kleemans, E. R.; Stol, W. P.** (2017). «Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks». *The British Journal of Criminology* (vol. 57, núm. 3, pàg. 704-722).

**Miller, J.** (1998). «Up it up: Gender and the accomplishment of street robbery». *Criminology* (núm. 36, pàg. 37-66).

**National Fraud Authority** (2013). *Annual Fraud Indicator June 2013* [en línia]. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf>

**Ngo, F. T.; Paternoster, R.** (2011). «Cybercrime Victimization: An examination of Individual and Situational level factors». *International Journal of Cyber Criminology* (vol. 5, núm. 1).

**Ponemon Institute** (2018). *2018 Cost of Data Breach Study: Impact of Business Continuity Management* [en línia]. <https://www.ibm.com/account/reg/us-en/signup?formid=urx-33253&cm_mmc=Search_Google-_-Global+Technology+Services_GTS+Resiliency+Services-_-WW_NA-_-%2Bponemon_b_OV65329&cm_mmca1=000000XA&cm_mmca2=10000924&cm_mmca7=1025197&cm_mmca8=kwd-377907906217&cm_mmca9=_k_EAIaIQobChMIuNrj2bSb4gIViJOzCh2GWgtvEAAYASAAEgK37_D_BwE_k_&cm_mmca10=341628554353&cm_mmca11=b&gclid=EAIaIQobChMIuNrj2bSb4gIViJOzCh2GWgtvEAAYASAAEgK37_D_BwE>

**Quayle, E.; Taylor, M.** (2002). «Child pornography and the Internet: Perpetuating a cycle of abuse». *Deviant Behavior* (núm. 23, pàg. 331-361).

**Quinn, J. F.; Forsyth, C. J.** (2013). «Xarxa Light districts on blue screens: A typology for understanding the evolution of deviant communities on the internet». *Deviant Behavior* (vol. 34, núm. 7, pàg. 579-585).

**Shamsudin, F. M.; Subramaniam, C.; Alshuaibi, A. S.** (2012). «The Effect of HR Practices, Leadership Style on Cyberdeviance: The Mediating Role of Organizational Commitment». *Journal of Marketing & Management* (vol. 3, núm. 1).

**Siwek, S. E.** (2007). *The true cost of sound recording piracy to the U.S. economy* [en línia]. <https://www.ipi.org/ipi_issues/detail/the-true-cost-of-sound-recording-piracy-to-the-us-economy>

**Statista** (2019). «Global markets with the highest online shopping penetration, 2017» [en línia]. <https://www.statista.com/statistics/274251/retail-site-penetration-across-markets/>

**Udris, R.** (2016). «Cyber Deviance among Adolescents and the Role of Family, School, and Neighborhood: A Cross-National Study». *International Journal of Cyber Criminology* (vol. 10, núm. 2).

**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.** (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press.

**Weimann, G.** (2011). «Cyber-Fatwas and terrorism». *Studies in Conflict & Terrorism* (vol. 34, núm. 10, pàg. 765-781).

**Whitty, M. T.** (2013). «The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam». *British Journal of Criminology* (vol. 53, núm. 4, pàg. 665-684).

**Wilson, M.** (2011). «Accenture survey: Discounters continue to dominate back-to-school shopping» [en línia]. *Chain Store Age* <www.chainstoreage.com/article/accenture-survey-discounters-continue-dominate-back-school-shopping>

**Wolak, J.; Finkelhor, D.; Mitchell, K.** (2004). «Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study». *Journal of Adolescent Health* (núm. 35, pàg. 424).

**Wolak, J.; Mitchell, K.; Finkelhor, D.** (2003). *Internet Sex Crimes Against Minors: The Response of Law Enforcement*. Washington, DC: Office of Juvenile Justice and Delinquency Prevention.

**Wright, R. T.; Decker, S. H.** (1997). *Armed Robbers In Action: Stickups and Street Culture*. Boston, MA: Northeastern University Press.

**Yar, M.** (2005). «The Novelty of "Cybercrime". An Assessment in Light of Routine Activity Theory». *European Journal of Criminology* (vol. 2, núm. 4, pàg. 407-427).

**Yip, M.; Shadbolt, N.; Webber, C.** (maig de 2013). «Why forums?: an empirical analysis into the facilitating factors of carding forums». A: *Proceedings of the 5th Annual ACM Web Science Conference* (pàg. 453-462). ACM.

**Zunger, Y.** (2018). «Computer science faces an ethics crisis. The Cambridge Analytica scandal proves it». *New York Times* (22 de març).