Delinqüència associada a l'ús de les TIC

Fernando Miró Llinares

PID_00195938

UOC
Universitat Oberta de Catalunya

Índex

Introducció

La delinqüència en l'àmbit de les tecnologies de la informació i la comunicació (TIC) comprèn tot un seguit de conceptes i conductes que els professionals de la criminologia han de conèixer i saber utilitzar. Amb aquests materials, l'estudiant tindrà la possibilitat de familiaritzar-se amb un altre àmbit de la criminalitat, la cibercriminalitat.

Per començar analitzarem els conceptes que estan relacionats amb el fenomen i després n'estudiarem l'evolució i l'estat actual.

Finalment, farem una anàlisi dels tipus de cibercrims que hi ha i establirem una visió general del problema i de les dimensions que té.

Objectius

En els materials didàctics d'aquesta assignatura, l'estudiant trobarà les eines bàsiques per a aconseguir els objectius següents:

1. Familiaritzar-se amb els conceptes bàsics relacionats amb la delinqüència i les TIC.

2. Conèixer l'origen i l'evolució de la criminalitat en el ciberespai.

3. Adquirir coneixements sobre la realitat de l'amenaça del cibercrim.

4. Conèixer els tipus d'atacs que es produeixen en el ciberespai.

1. Delinqüència i TIC: cibercrim i cibercriminalitat

El fenomen de la criminalitat relacionada amb l'ús de les tecnologies de la informació i la comunicació continua essent totalment nou i, per això, parcialment incomprès per la societat en general i, en concret, per les institucions que han d'afrontar la prevenció d'aquesta amenaça, malgrat que han passat més de tres dècades des que es va començar a parlar de criminalitat informàtica i més de dues des que es va encunyar el terme *cybercrime*.

El cibercrim ja forma part de la realitat criminològica del nostre món; tanmateix, com veurem més endavant, en molts casos s'exagera l'amenaça que representa i en d'altres no es percep el risc real que comporta l'ús de les TIC. La revolució de les TIC –com a concepte ampli, obert i dinàmic que comprèn tots els elements i sistemes utilitzats avui per al tractament de la informació, l'intercanvi i la comunicació d'aquesta en la societat actual, en què s'emmarca el fenomen del cibercrim– encara no s'ha acabat ni ho farà fins d'aquí molt temps, cosa que implica que la cibercriminalitat o delinqüència associada al ciberespai es continuarà expandint i evolucionarà en les properes dècades.

Malgrat que el desenvolupament de les tecnologies informàtiques va començar els anys seixanta i setanta del segle passat, l'embranzida definitiva es va produir amb la creació d'Internet i la universalització posterior d'aquesta xarxa, però els darrers anys la rapidesa amb què apareixen les noves tecnologies ha augmentat exponencialment i tot apunta que ho continuarà fent. També són evidents els efectes socials que ha comportat la revolució de les TIC; així, gràcies a l'aparició d'Internet i a la seva popularització a escala planetària ens hem apropat enormement a la creació del ciberespai virtual tal com el va concebre William Gibson, que és qui va encunyar aquest terme, ja que, de manera paral·lela al món físic, s'ha configurat un espai comunicatiu i interactiu que, sobretot en la primera dècada del segle XXI, ha modificat les relacions econòmiques, polítiques, socials i, molt especialment, les personals. Avui, la utilització dels serveis d'Internet o les xarxes de la telefonia mòbil són la forma més habitual de comunicar-se personalment amb els familiars, els amics o les persones de l'entorn laboral, i no solament per als adults sinó també per als més petits d'una generació que no entendrà la comunicació entre iguals sense la Xarxa; Internet també és el vehicle per on ja flueixen la major part de diners arreu del món: tots els bancs i les entitats financeres actuen per mitjà del ciberespai, i cada vegada hi ha més transaccions econòmiques i negocis a petita, mitjana i gran escala que es duen a terme directament per aquest mitjà de comunicació global.

William Gibson

Novel·lista de ciència-ficció que va crear el terme *cyberspace* en l'obra *Neuromancer* (Nova York, AceBooks, 1984).

A més a més, aparentment tot indica que la incidència del ciberespai en tots els aspectes de la vida social no disminuirà, sinó que continuarà creixent. A mesura que liderin el món els anomenats *nadius digitals* o nascuts en l'era del Web 2.0 popularitzat, amb els sistemes informàtics com a forma de treball i també de diversió, amb les xarxes socials com a forma d'interacció social, amb les tecnologies mòbils totalment connectades i amb tota la informació a l'abast, el ciberespai, com a lloc de trobada per a l'ús de les TIC, s'anirà ampliant i la novetat del cibercrim, com de qualsevol altre element concatenat a aquest espai virtual que per a moltes persones és encara més real que l'altre, anirà desapareixent i l'única cosa que canviarà serà la manifestació concreta d'aquest ciberespai a partir del nou aspecte social que caldrà protegir o la nova tecnologia que facilitarà o modificarà la manera de cometre el delicte.

Nadiu digital

Terme encunyat per Marc Prensky en l'obra "Digital Natives, Digital Immigrants" per a referir-se a la generació nascuda amb la implantació global d'Internet.

Innegablement, tots aquests canvis socials que estem vivint arran dels canvis tecnològics que es produeixen, es reflecteixen en la criminalitat com a fenomen social que és. En concret, el tenen en l'aparició d'un nou tipus de delinqüència associat al nou espai de comunicació interpersonal que és Internet. De fet, l'evolució del cibercrim com a fenomen criminològic s'ha esdevingut de manera paral·lela, com veurem posteriorment amb més profunditat, a l'evolució dels interessos socials relacionats amb les TIC. Quan el protagonisme el van tenir els terminals informàtics i la informació personal que podien contenir, van aparèixer noves formes d'afectar la intimitat de les persones; quan aquests terminals i la informació que contenien van començar a tenir valor econòmic i a servir per a la realització de transaccions econòmiques, van sorgir les diverses formes de criminalitat econòmica relacionades amb els ordinadors i, molt especialment, el frau informàtic, que, al seu torn, va evolucionar cap a l'*scam*, el *phishing* i el *pharming* quan va aparèixer Internet. Finalment, amb la universalització de la Xarxa i la constitució del ciberespai van sorgir noves formes de criminalitat que aprofitaven la transnacionalitat d'Internet per a atacar interessos patrimonials i personals d'usuaris concrets, però també per a afectar interessos col·lectius per mitjà del ciberracisme o del ciberterrorisme.

Avui, que comencen a adquirir el protagonisme les xarxes socials i altres formes de comunicació personal en què se cedeixen voluntàriament esferes d'intimitat i en què es creen relacions personals per mitjà del ciberespai, i que, alhora, l'activitat econòmica a Internet no disminueix sinó que augmenta, assistim a un moment àlgid de la criminalitat en el ciberespai, tant en el sentit quantitatiu atès l'ús creixent d'Internet arreu del món com en el sentit qualitatiu pel fet que han aparegut noves formes de delinqüència relacionades amb els nous serveis i usos que han sorgit en l'entorn digital.

L'evolució del cibercrim també comporta una **evolució en els protagonistes essencials**, els **criminals** i les víctimes. Del ja mític ***hacker*** estereotipat en l'**adolescent introvertit** i amb problemes de sociabilitat tancat a casa i convertit en el primer ciberespai en un **geni informàtic** capaç d'aconseguir la guerra entre dues superpotències des de l'ordinador mateix, hem passat a les màfies

organitzades de cibercriminals que aprofiten el nou àmbit per a augmentar les seves activitats il·lícites i els seus recursos. I com que els cibercrims no són únicament els realitzats amb ànim econòmic, també varien els perfils de cibercriminals que cometen delictes, que, de fet, són rèpliques en el ciberespai dels que executarien en l'espai físic.

I succeeix el mateix amb les **víctimes**. Les **empreses** continuen essent objecte de victimització a causa tant de l'ús generalitzat que fan de les TIC com dels recursos econòmics que tenen i que són objecte de desig dels cibercriminals. No obstant això, l'aparició dels cibercrims socials converteix **qualsevol ciutadà que es relacioni a Internet**, que contacti amb altres individus, que enviï missatges, que escrigui en fòrums o que comparteixi les fotografies, en objecte d'un ciberatac personal a l'honor, a la intimitat, a la llibertat sexual o a altres béns jurídics. I succeeix el mateix amb altres **institucions supranacionals** en relació amb els cibercrims polítics o ideològics comesos amb la intenció de desestabilitzar un estat o de difondre un determinat missatge polític aprofitant les possibilitats de comunicació massiva que ofereix el ciberespai; així, la ciberguerra, el hacktivisme o el ciberterrorisme han convertit els estats, i els recursos públics que ofereixen als ciutadans per Internet, en objectiu d'atacs de denegació de serveis, d'infeccions de *malware* o d'altres que poden paralitzar, com ha succeït, l'activitat d'institucions importants d'un país.

Per bé que hi ha moltes definicions del terme *cibercrim*, l'aspecte essencial de totes es redueix a la qüestió de si amb la definició s'adopta una concepció àmplia o restringida de la cibercriminalitat, de manera que en la categoria es dóna cobertura o bé a tots els comportaments criminals realitzats en el ciberespai o bé tan sols a uns quants.

Si utilitzem el terme *cibercrim* en sentit ampli, es tracta de qualsevol comportament delictiu realitzat en el ciberespai, entenent que aquest és el mateix àmbit virtual d'interacció i comunicació personal definit per l'ús de les TIC, de manera que comprèn conductes el contingut il·lícit de les quals és nou i es relaciona directament amb els nous interessos o béns socials que hi ha en el ciberespai, i també comportaments tradicionalment il·lícits en què l'únic que canvia és que ara es duen a terme per mitjà d'Internet.

Si, per contra, utilitzem el terme *cibercrim* de manera restringida, i si bé es poden fer servir diversos criteris per a restringir la categoria, el més habitual és partir de la mateixa idea de la realització del delicte per mitjà de les TIC.

D'acord amb això, només parlarem de *cibercrim* si es tracta d'un comportament delictiu realitzat en el ciberespai l'essència d'injust del qual no es podria haver produït de cap altra manera.

El comportament de qui assetja sexualment un menor per Internet seria un cibercrim des d'una concepció àmplia, atès que s'ha dut a terme en el ciberespai, però es podria haver executat en l'"espai real". Tanmateix, no ho seria si utilitzem un concepte restringit de *cibercrim*, ja que té el referent fora d'ell. Per contra, l'atac anomenat *de denegació de serveis* seria un cibercrim tant en sentit ampli com en sentit restringit, ja que aquesta conducta lesiva dels interessos econòmics de la víctima només es pot realitzar per mitjà d'Internet.

Des d'una concepció àmplia, per *cibercrim* s'entén qualsevol delicte en què les tecnologies de la informació tenen un paper determinant en la comissió concreta; és a dir, qualsevol delicte que s'hagi dut a terme en el ciberespai, amb les particularitats criminològiques, victimològiques i de risc penal que se'n deriven. Per tant, en general aquí utilitzarem el cibercrim en sentit tipològic, o bé com a comportament criminal en el ciberespai o bé com a categoria que els inclou tots o uns quants. Això sí, perquè puguem parlar de *cibercrim* no n'hi haurà prou que s'utilitzin les TIC per a realitzar el comportament criminal, sinó que aquest ús a més ha de tenir a veure amb algun element essencial del delicte.

No es tracta d'un cibercrim si, per exemple, s'envia una carta que ha estat impresa utilitzant el terminal informàtic i que inclou continguts que s'han copiat de recursos d'Internet, però sí quan s'amenaça a una altra persona per mitjà del correu electrònic, o quan l'engany constitutiu de l'estafa es duu a terme usant aquest mitjà.

D'altra banda, és important aclarir que el terme *cibercrim* té una relació directa amb un altre concepte que s'utilitza habitualment en aquest àmbit, la paraula *cibercriminalitat*. Aquest terme no té sentit normatiu, sinó únicament tipològic, com a categoria criminològica que comprèn tots els cibercrims. En general, el terme *cibercriminalitat* s'utilitza per a referir-se al fenomen de la criminalitat en el ciberespai, i, en molts casos, es fa servir el terme *cibercrim* per a situar dins d'aquest fenomen un tipus de comportament concret.

Com acabem de veure, però, en alguns casos el terme *cibercrim* també s'utilitza per a referir-se a tots els comportaments que tenen les característiques tipològiques que constitueixen el fenomen, és a dir, com a sinònim de *cibercriminalitat*. Això és el que succeeix amb l'ús del terme *cybercrime* en anglès, i també en català quan s'afirma, per exemple, que "el cibercrim és una amenaça per a la seguretat dels estats actualment". En tots dos casos, l'ús és correcte i el context permet diferenciar un sentit de l'altre.

2. Passat i present de la criminalitat en el ciberespai

2.1. Evolució de la delinqüència en les TIC

Amb el desenvolupament de les tecnologies informàtiques i l'aparició d'infraccions associades a aquestes tecnologies, els anys setanta va sorgir la creació de la categoria de delictes informàtics que avui dia es continua utilitzant. Formaven part d'aquesta categoria tant els comportaments delictius realitzats per mitjà de processos electrònics com la resta de delictes tradicionals que requeien en béns que tenien una configuració específica en l'activitat informàtica o bé en objectes nous com el *hardware* i el *software*.

En realitat, la delinqüència informàtica definia un àmbit de risc que derivava de l'expansió social de la tecnologia informàtica, comuna a molts béns jurídics la tutela completa dels quals per part del legislador semblava que requeria modificar els tipus penals existents per a adaptar-los a les noves realitats informàtiques o crear-ne de tipus diferents que responguessin a les noves necessitats de protecció. El risc de l'activitat informàtica, diguem-ne, com a àmbit en què apareixien nous interessos, noves formes de comunicació social i, per tot això, nous perills per als béns més importants, era i és, per tant, una cosa comuna a infraccions penals com el frau informàtic, el sabotatge o danys informàtics, el *hacking* o l'accés il·lícit a sistemes informàtics, la sostracció de serveis informàtics, l'espionatge informàtic, o la pirateria informàtica d'obres producte de l'enginy; tipologies de conducta específica que la doctrina penal considera mereixedores de resposta penal i sobre les quals s'analitzava la possible incardinació en els tipus penals tradicionals o la reforma d'aquests, i fins i tot la creació de tipus nous, per a protegir més bé els interessos dignes de tutela. Respecte d'altres categories, doncs, la dels delictes informàtics incloïa tipologies de conductes, i no tipus penals.

En els darrers temps s'ha substituït la denominació de *delicte informàtic* per les de *cibercrim* i *cibercriminalitat* amb referència aquesta vegada al terme anglosaxó *cybercrime* –procedent de la unió entre el prefix *cyber*, derivat del terme *cyberspace*, i el terme *crime*, com a concepte que serveix per a incloure la delinqüència en l'espai de comunicació oberta universal que és el ciberespai. En anglès, sembla que aquest terme s'imposa davant d'altres conceptes com *computer crime*, o encara d'altres en què s'utilitzen prefixos com *virtual*, *online*, *high-tech*, *digital*, *computer-related*, *Internet-related*, *electronic*, i *e-*. En l'arrel d'aquest canvi de denominació hi ha l'evolució, des d'una perspectiva criminològica, dels comportaments il·lícits a la Xarxa i la preocupació legal en relació amb aquests comportaments; en concret, el fet que la informació del sistema infor-

màtic passés de ser el centre del risc a ser-ho les xarxes telemàtiques a les quals es van començar a connectar els sistemes i els interessos personals i socials que s'hi posen en joc.

Així, després d'una primera generació de la cibercriminalitat en què era característic l'ús d'ordinadors per a cometre delictes, va venir una segona època en què la característica central era la comissió del delicte per mitjà d'Internet i encara una tercera en què els delictes estan absolutament determinats per l'ús d'Internet i les TIC. Això ha tingut una correlació en l'àmbit legal; així, a partir del segle actual va començar a preocupar no solament la informació que contenen els sistemes informàtics i l'afectació a la intimitat o el patrimoni que es pugui derivar de l'accés a aquesta informació, sinó també el ciberespai en què interaccionen i els crims que s'hi produeixen i que poden afectar molts altres béns jurídics nous com la indemnitat sexual, la dignitat personal o la mateixa seguretat nacional. I tot això ha portat a l'ús del terme *cibercrim*, que comprèn totes les tipologies de comportaments que hi ha i a més emfatitza el que les uneix; en aquest cas, Internet i les TIC com a mitjà de comissió delictiva.

Al cap i a la fi, si bé Internet, la xarxa més popular i per mitjà de la qual es realitzen pràcticament totes aquestes infraccions, és en si mateixa un mitjà informàtic i, per tant, tots els ciberdelictes es podrien incloure en la categoria dels delictes informàtics, amb l'ús del terme *cibercriminalitat* es posa de manifest que les implicacions de risc van més enllà de la utilització de tecnologies informàtiques i es relacionen molt més amb el fet que avui aquestes estiguin unides a xarxes telemàtiques, amb els problemes politicocriminals concrets que això planteja actualment. A més a més, com que es té en compte no solament l'aspecte "informacional" de les TIC sinó també el comunicatiu, es fa referència a un catàleg més ampli d'infraccions que inclou les que es relacionen amb el (mal) ús de les comunicacions personals entre particulars per mitjà de xarxes telemàtiques o amb la introducció i mala utilització de continguts que s'han introduït en aquestes xarxes.

2.2. El cibercrim avui és realitat o ficció?

És important determinar les dimensions actuals de la cibercriminalitat i alhora conèixer l'amenaça real del cibercrim, ja que els discursos en relació amb aquests fenòmens solen ser contradictoris.

Exemple

En són un exemple els informes de la Fiscalia General de l'Estat que amb prou feines fan esment de la cibercriminalitat i, no obstant això, paral·lelament es continua afirmant, des de molts àmbits, que es tracta d'una amenaça creixent.

Certament, el fet que des del punt de vista comunicatiu sigui molt poderosa la suma de la imatge d'un ciberespai universal i transnacional que comprèn milions de conductes en un únic punt amb la del crim en les diverses manifestacions, i tot això des del prisma d'una societat del risc insegura com la societat en què vivim, ha fet que hi hagi un temor a la cibercriminalitat que, en molts aspectes, es podria titllar d'exagerat.

Són molts els que assenyalen que l'amenaça d'una ciberguerra és totalment remota, malgrat que hi ha una por social en relació amb això. En el cas del ciberterrorisme, entès en el sentit més estricte de la utilització del ciberespai per a la realització d'atacs terroristes, també hi ha hagut una exageració significativa de l'abast del fenomen que comporta un temor social més enllà de la realitat de l'amenaça. I aquest mateix temor s'estén al cibercrim, que se sobredimensiona no tant des del punt de vista quantitatiu com del qualitatiu, com una amenaça desconeguda i més enllà de la realitat. Així, pot sorprendre que en algunes enquestes poblacionals hi hagi un 13% de persones que estan més preocupades per si són víctima d'un cibercrim que per si ho són d'un delicte en l'espai físic, especialment si el que es mesura és el temor més que la probabilitat atesa la gravetat general més gran que comporta la victimització en l'espai físic.

En realitat, el discurs sobre les amenaces cibernètiques sol estar dominat per l'excés de publicitat donada a algunes amenaces en perjudici dels altres, i per les afirmacions exagerades sobre la freqüència i la magnitud dels atacs.

En alguns casos, l'exageració prové de les mateixes empreses de *software* que col·laboren amb els organismes públics per avaluar l'amenaça del cibercrim i que, com a interessades en el finançament de sistemes de protecció, poden exagerar les xifres del crim. És especialment significativa, però, la cobertura que duen a terme els mitjans de comunicació, que se centra, per exemple, en la presentació d'informes sobre atacs a gran escala, com si, com més gran sigui l'atac, més gran és l'amenaça. No obstant això, els ciberincidents poden ser menys dramàtics des del punt de vista comunicatiu, però molt més problemàtics.

Per posar-ne un exemple, la realització d'atacs de denegació de serveis contra les pàgines web de la SGAE i els principals partits polítics espanyols rep una cobertura informativa impressionant, i fins i tot arriba a ser portada dels diaris nacionals més destacats, malgrat que la conseqüència dels atacs sigui simplement que unes pàgines web amb poca afluència d'usuaris no s'han pogut visitar durant unes quantes hores. Molt més greu és, però, la pèrdua d'informació per a les empreses o els usuaris a causa de les infeccions de *malware* o l'augment de les conductes de ciberassetjament escolar a menors tal com certifica l'anàlisi jurisprudencial, si bé aquest tipus de comportament mai no rebrà la cobertura informativa que hem esmentat.

De fet, aquesta forma de relat distorsiona la percepció pública de les amenaces i, per tant, emmascara la realitat i pot produir l'efecte contrari. Efectivament, l'exageració, juntament amb la desinformació, pot portar-nos a menysprear l'amenaça del cibercrim a partir de la creença que se sobrevalora tenint en compte l'aparent constatació vàlida que aquest tipus de criminalitat no ha arribat als tribunals de manera massiva els darrers anys.

En altres paraules, si fa més d'una dècada que avisem del risc que representarà la cibercriminalitat, parlant de ciberguerra i d'altres aspectes, i, no obstant això, els tribunals es continuen ocupant de delictes contra la seguretat viària, de violència de gènere i de tràfic de drogues essencialment, potser cal convenir

que aquesta amenaça no ho era tant. Aquesta argumentació resumiria l'efecte contraposat, la "banalització" del cibercrim, que també és manifestament perillós i a més erroni.

És perillós perquè es menysvaloren els riscos existents i, amb això, es deixen d'adoptar mesures de protecció i d'obtenció d'informació per a conèixer les dimensions reals de l'amenaça del cibercrim. Certament, malgrat la implantació completa de les TIC en els àmbits empresarial i comercial, i malgrat l'expansió d'aquests àmbits a altres contextos socials en què els béns jurídics en joc poden ser fins i tot més importants, com ara tot el que està relacionat amb la intercomunicació personal, encara hi ha molts sistemes informàtics que no tenen sistemes de protecció bàsics i, cosa encara més important, continua sense haver-hi una educació en les TIC que, a banda dels aspectes tècnics, centri l'atenció en els riscos reals que hi ha i en les possibilitats per a detectar-los i evitar-los. **El mercat de les TIC tampoc no té com a prioritat la seguretat** i es continuen venent sistemes informàtics que accedeixen immediatament a xarxes telemàtiques sense antivirus o amb *software* que l'usuari ha d'actualitzar i pagar si vol seguretat, mentre que la velocitat o la memòria d'alta capacitat vénen incorporades de sèrie.

Riscos molt llunyans

La ciberguerra i altres ciberatacs que afectin la població són riscos molt llunyans i que només es podran produir quan hi hagi una dependència més gran de la tecnologia que també estigui relacionada amb els serveis i les atencions bàsiques.

És sorprenent que nosaltres, ciutadans privats, però també institucions privades i públiques, tolerem un gran nombre de vulnerabilitats tècniques i les conseqüències d'aquestes, com el preu que cal pagar per la innovació i la competència en un mercat lliure, quan ningú no toleraria un cotxe que té un sistema de frenada que el mateix usuari ha d'activar i actualitzar. El cas és que es perceben com a riscos aspectes que encara són molt llunyans i no es perceben com a riscos altres aspectes que són reals, però que, d'alguna manera, es mantenen ocults, essencialment, a causa del desconeixement de les mateixes TIC i, en alguns casos, de la **voluntat d'amagar** aquestes **amenaces per a l'èxit de la implantació social** corresponent.

Ara bé, només hi ha **banalització de la cibercriminalitat si aquesta forma de delinqüència existeix** o, més aviat, si representa una problemàtica creixent i digna d'estudi. Al capdavall, totes les expectatives de creixement de la cibercriminalitat i totes les previsions sobre el cibercrim sembla que xoquen violentament amb l'efecte escàs del ciberdelicte en els tribunals de justícia. A l'**Estat espanyol**, les estadístiques oficials també constaten un **augment del cibercrim**; certament, encara és tènue, però sens dubte la tipificació de noves figures delictives i, especialment, la popularització del Web 2.0 comporta la realització de conductes delictives en el ciberespai que es comencen a denunciar, si bé encara no tenen gaire reflex en els processos judicials.

En aquest punt cal preguntar-se si **aquesta escassetat de processos judicials per cibercrims es deu a l'absència de proves per a la imputació o més aviat a la mateixa absència de cibercrims**; és a dir, si en realitat hi ha una sobredimensió de l'amenaça del cibercrim o una resposta judicial pobra a aquest tipus de delicte a causa de factors diversos, relacionats de manera més o menys

directa amb la novetat del fenomen i l'anquilosament espacioterritorial del sistema d'administració de justícia. En el primer cas no hi hauria banalització sinó valoració del cibercrim en la mesura justa, com una simple anècdota en l'oceà de la delinqüència tradicional; en el segon cas sí que hi hauria banalització, i caldria tant una millora de l'observació criminològica d'aquest fenomen per a mesurar-lo correctament com una intervenció decidida amb vista a prevenir-lo.

Doncs bé, segons la major part dels que han tractat el tema de la cibercriminalitat amb profunditat hi ha una **xifra negra** important en matèria de cibercriminalitat; és a dir, els delictes que es cometen són molts més que els que apareixen en les estadístiques oficials i que són jutjats i condemnats com a tals, fins al punt que alguns han assenyalat que la cibercriminalitat és la forma de delinqüència més infradenunciada de totes.

Ho entén així la doctrina, segons la qual, si en tots els tipus de delinqüència hi ha una xifra negra, aquesta deu ser més gran en el cas de la cibercriminalitat. Però, a més a més, hi ha dades, i no simples hipòtesis, que certifiquen que amb la cibercriminalitat succeeix una cosa semblant al que passa amb els icebergs: el que es percep o visualitza és tan sols un percentatge ínfim en comparació del que realment existeix.

Estudis sobre cibercrim

Diversos estudis insisteixen que el cibercrim creix des de fa més de deu anys, i que els atacs que es reben diàriament al nostre país són molts; alguns no són pròpiament delictius (el cas de l'enviament de *spam*), però d'altres sí (com els danys, l'accés informàtic il·lícit, les injúries i les calúmnies, o els atacs de DoS). Així ho posen de manifest nombrosos informes independents d'algunes empreses de seguretat importants, com Javelin, que en l'estudi sobre frau d'identitat que va dur a terme va detectar un increment d'un 12% de víctimes d'aquesta modalitat de ciberdelicte, o l'informe encarregat a PricewaterhouseCoopers, en què es posa de manifest que, mentre que en un estudi del 2008 sobre forats de seguretat en les empreses el 21% dels enquestats van declarar que havien estat infectats per virus o un altre *software* maliciós, el 2010 aquesta xifra va pujar al 61%.

Aquest mateix informe destaca una altra dada que crida l'atenció: únicament el 16% de les empreses enquestades esperen un nombre inferior d'atacs l'any vinent. Altres informes publicats per institucions governamentals o afavorides pels governs, com l'Internet CrimeComplaintCenter (IC3), constaten que les denúncies per cibercrims van passar de 16.838 el 2000 a 303.809 el 2010. També sembla que certifiquen aquesta tendència d'increment del cibercrim un altre tipus d'estudis contra els quals no es podrà argumentar, com es fa amb els realitzats per empreses de *software*, la falta d'imparcialitat. Ens referim a les investigacions sobre victimització en el ciberespai que inclouen molts tipus de ciberdelictes, si bé s'ocupen més especialment de les infeccions de *malware*, el *phishing*, el *cyberbullying*, el *online grooming* o el *cyberstalking*. Totes les investigacions reflecteixen un augment de la criminalitat, si bé se'ls pot retreure que cap d'aquestes investigacions no qüestiona les raons per la falta de denúncia d'aquests delictes.

Per tant, la criminalitat en el ciberespai augmenta i ho continuarà fent mentre s'ampliïn els àmbits de comunicació entre les persones a Internet. No s'ha d'exagerar l'amenaça, ja que, si bé és cert que els atacs s'han incrementat al llarg dels anys, també ho és que els procediments en seguretat han millorat, i a mesura que sorgeixin àmbits de criminalitat s'aniran desenvolupant estratè-

gies preventives que en limitaran els efectes. Tampoc no estem en condicions de quantificar la xifra negra sense cap classe de suport empíric. Per contra, seria recomanable la realització d'investigacions criminològiques empíriques profundes que servissin per a reflectir les dimensions reals del fenomen o bé per mitjà de l'estudi de les denúncies arxivades o bé a partir d'estudis de victimització entra la població. Seria una manera de solucionar els problemes que comporta l'anàlisi, únicament, de les dades oficials i la impossibilitat que implica de quantificar l'abast real del fenomen.

Quantificar qualsevol tipus de delicte és una tasca difícil i complicada, però ho és especialment en l'àmbit de la cibercriminalitat per dos motius principals: d'una banda, per la falta de denúncies d'aquest tipus de delicte i, de l'altra, per les característiques que presenta que dificulten els processos judicials tot i que hi hagi denúncia.

Començant per aquests darrers, no és cap descoberta l'afirmació que els processos judicials contra una gran part dels cibercrims poden tenir moltes més complicacions generals que els que s'inicien contra crims en l'espai físic. La raó principal és que quan hi ha una denúncia, generalment en aquests casos no adreçada contra ningú en concret sinó com a reflex d'una victimització específica, els primers passos de la investigació policial s'orienten a determinar-ne els autors i hi ha diversos motius pels quals aquesta tasca pot ser especialment complicada en aquests delictes:

Exemples

Exemples de denuncies sense determinació d'autor són uns diners defraudats per un usuari indeterminat, un dany en el sistema per un virus, una calúmnia en una pàgina web, etc.

- **Anonimat a la Xarxa**. En primer lloc, per les mateixes característiques, que afavoreixen l'anonimat, del ciberespai. Encara que el ciberdelicte sigui comès per algú en concret, a Internet només es mostra una representació virtual de l'autor (l'adreça IP) que pot ser concretada, però a la qual després cal atribuir la persona física concreta que hi ha darrere l'acció, i això ja és més complicat, ja que exigeix, primer, la col·laboració de les empreses proveïdores de serveis i, després, la investigació del titular del sistema informàtic des del qual s'ha realitzat l'atac i la concreció, entre tots els usuaris del sistema, del que l'ha executat en concret.

Col·laboració dels estats contra el cibercrim

No és el mateix sol·licitar l'extradició d'una persona concreta per la comissió d'un delicte determinat que sol·licitar a un estat estranger que investigui qui pot ser el subjecte que hi ha darrere d'una IP concreta que presumptivament ha perpetrat una infracció penal. La pràctica judicial demostra que la fiscalia sol claudicar en l'intent d'identificació quan la IP és a Rússia o en països similars que estan relacionats amb màfies de cibercriminals.

- **Transnacionalitat del delicte**. En segon lloc, i en relació amb el primer aspecte, la determinació judicial de les persones autores del cibercrim se sol complicar a causa de la transnacionalitat del delicte. Ja no es tracta, com en la criminalitat física, que el delinqüent s'hagi pogut traslladar a un altre país després de cometre el delicte i calgui sol·licitar el lliurament del delinqüent a les autoritats judicials espanyoles, sinó que el delicte hagi estat directament comès des de l'estranger, amb la qual cosa els processos per a identificar el cibercriminal requereixen la col·laboració d'altres estats, que no sempre és fàcil d'aconseguir.

El segon grup de motius té a veure amb la falta de denúncia de la víctima del cibercrim. Les raons són diverses i, probablement, s'han de valorar de diversa manera segons el delicte. Al cap i a la fi, la cibercriminalitat és tota la criminalitat en el ciberespai i la xifra negra no serà idèntica en totes i cadascuna de les tipologies de delictes. Vegem aquestes raons.

1) Conducta criminal inadvertida. D'entrada, en molts casos la conducta criminal passa directament inadvertida, de manera que no és denunciada encara que hagi estat consumada i fins i tot s'hagin aconseguit els efectes criminals volguts. Això pot succeir amb altres delictes comesos a l'espai físic, però d'una manera molt excepcional, ja que en aquest espai la visualitat dels efectes i les conseqüències de les accions és més gran.

Això és el que pot passar, per exemple, amb les infeccions de virus maliciosos que produeixin danys en els sistemes informàtics, també amb injúries i calúmnies penjades en llocs web i que siguin percebudes per altres subjectes però no per la víctima mateixa, però succeirà especialment en el cas del *hacking* o accés informàtic il·lícit, conducta consistent en la simple intromissió en el sistema informàtic aliè, delicte reconegut a partir de la reforma del Codi penal del 2010, i que en molts casos, pràcticament en tots, no serà percebuda pel titular del sistema. Fins i tot pot succeir que la víctima no percebi l'atac en el cas de les defraudacions en el ciberespai. Així, l'intent de descobrir la comissió de fraus informàtics pot implicar uns costos enormes a causa de les comprovacions minucioses i altres aspectes que poden comportar unes pèrdues més grans que el mateix perjudici causat.

2) Percepció tardana de l'atac. En altres casos, la víctima s'adona de l'atac però ho fa tard, quan aquest ha prescrit o quan ja valora que és absurd presentar una demanda judicial ateses les poques possibilitats que la policia identifiqui, detingui i processi els delinqüents. Això és habitual en els ciberfraus, especialment en relació amb els bancs, ja que pot succeir que la víctima s'adoni que li falten diners en el compte o que li han imputat una despesa que no pertoca després que s'esdevingui. Això és el que passarà amb el *hacking* en els casos en què la víctima ho percebi, ja que és pràcticament impossible que la víctima visualitzi aquesta conducta delictiva en el mateix moment en què es produeix. També succeirà en les infeccions de virus amb resultat de danys, que en alguns casos el subjecte les percep però en d'altres no, a banda que l'efecte del virus es pot desencadenar en un moment determinat, però la infecció es pot haver produït en un altre moment molt anterior.

3) Falta de percepció com a conducta delictiva. Un altre factor que cal tenir en compte com a motiu de la xifra negra de la cibercriminalitat és que la mateixa víctima, que sí que percep el ciberatac, no el valora com una conducta delictiva, per la qual cosa no el denuncia. Això succeix sobretot en el cas de les infeccions de virus, de les quals molts desconeixen que generalment pot ser un delicte d'acord amb el que estableix el Codi penal; però també passa amb una gran part de l'enviament de *spam* que conté missatges de *scam* o *phishing* que es pot reconèixer com a temptativa d'estafa en alguns casos si no és utilització il·lícita fraudulenta de la imatge d'una empresa o estafa punible en el cas que es creï un web per al *pharming* i malgrat que no hi hagi pèrdua patrimonial; per descomptat, succeeix amb el *hacking* o accés informàtic il·lícit que encara no té la valoració social de comportament delictiu; i fins i tot pot passar amb els

petits fraus, amb els que produeixen una pèrdua patrimonial tan ínfima per a la víctima que pot pensar que ni tan sols resulten delictius. No obstant això, els criminals cibernètics aprofiten aquesta subestimació crònica dels delictes cibernètics, ja que una pèrdua de trenta lliures o euros per a una persona pot significar un guany mínim de tres mil lliures o euros per a l'infractor, tenint en compte que les estafes s'adrecen a centenars de milers de persones en línia.

4) Falta de confiança en la justícia. En altres casos, la raó de la denúncia és precisament la falta de confiança en les autoritats judicials per a esbrinar els fets, generalment per la convicció de la dificultat que comportarà identificar els responsables. Això succeirà especialment en els cibercrims econòmics, especialment en els casos en què les pèrdues no siguin dràstiques, i en què la víctima preferirà la pèrdua a la despesa judicial pròpia a causa dels dubtes que li planteja l'èxit del cas. Al capdavall, els problemes d'identificació i la qüestió de la transnacionalitat de l'atac no són aliens a la víctima, i els tindrà en compte a l'hora d'iniciar un procés judicial incert. Per contra, quan la víctima constati que el ciberatac ha estat efectuat per algú conegut (encara que no estigui identificat) o de nacionalitat pròpia hi ha més possibilitats que es denunciï amb l'esperança que es pugui identificar l'agressor. I el mateix succeirà quan la denúncia tracti d'esborrar els efectes visibles del delicte (en el cas de les injúries, les calúmnies o els atemptats a la dignitat d'una persona per mitjà d'una publicació en una pàgina web o similar).

Xifra negra d'algunes empreses

Convé fer esment de la xifra negra que generen algunes empreses, especialment en el cas dels bancs, que prefereixen assumir les pèrdues provocades per ciberatacs i indemnitzar els clients en comptes de fer pública la vulnerabilitat dels seus sistemes mitjançant la denúncia, ja que el cost que provocaria la pèrdua de clients per un motiu de desconfiança podria superar el cost generat per la conducta criminal.

3. Fenomenologia dels atacs en el ciberespai

La realitat criminològica ens ensenya, de primer, que el ciberespai s'ha convertit en alguns casos en un àmbit autènticament generador de noves conductes delictives quan les TIC són l'única forma de realització de la infracció; en d'altres, en canvi, el que ha comportat la irrupció del "nou espai" ha estat l'aparició no de noves formes pures de delinqüència sinó de rèpliques d'unes altres formes ja existents que canvien els trets bàsics pel fet que es duen a terme en el nou àmbit virtual; i, finalment, el ciberespai de sistemes connectats en xarxes també ha potenciat la importància dels continguts, ja que n'ha facilitat enormement la difusió global i ha generat, amb això, tot un conjunt de conductes en què la il·licitud només es troba en la difusió o l'accés a unes formes determinades d'informació il·lícita o socialment considerada perillosa.

Així, podem distingir tres blocs de conductes delictives en el ciberespai tenint en compte el paper que exerceixen les TIC en el seu desenvolupament anomenats:

- *ciberatacs purs*,
- *ciberatacs rèplica* i
- *ciberatacs de contingut*.

3.1. Ciberatacs purs

Són categoritzats com a **ciberatacs purs** els que únicament poden succeir en el ciberespai.

Es tracta d'un nou conjunt d'infraccions completament noves que sorgeixen del desenvolupament de les TIC.

3.1.1. El *hacking*

Es pot definir ***hacking*** com qualsevol conducta per la qual un subjecte accedeix a un sistema o equip informàtic sense l'autorització del titular d'aquest, de manera que té capacitat potencial d'utilitzar-lo o d'accedir a qualsevol tipus d'informació que hi hagi en el sistema.

El *hacking*, en aquest sentit ampli, és l'activitat dels *hackers* que consisteix a superar qualsevol barrera informàtica, tant per a accedir a un sistema com per a configurar una programació funcional determinada, per exemple. En sentit estricte, en canvi, és equivalent a un altre terme utilitzat de manera general, l'intrusisme informàtic, que posa l'accent en el fet que una conducta comporta la violació d'una esfera d'exclusivitat reservada al titular del sistema, tant si conté informació privada com confidencial.

Hacking i cracking

Cal distingir entre el *hacking* blanc, en què l'objectiu del *hacker* és simplement l'accés al sistema o a les dades i la informació que conté, sense cap propòsit de sabotatge o utilització posterior de la informació, i el *cracking*, en què el *cracker* accedeix al sistema per realitzar qualsevol tipus de dany al sistema, als elements que conté o al titular corresponent per mitjà de l'adquisició, l'eliminació o la modificació de la informació que comprèn.

El *hacking* es pot dur a terme de moltes maneres diferents, si bé, en general, la manera de procedir consisteix a cercar vulnerabilitats en els sistemes informàtics derivades d'una programació deficient, d'un canvi tecnològic que fa obsoleta la formulació binària existent o, fins i tot, aprofitant les portes que involuntàriament pot haver deixat obertes el mateix titular del sistema informàtic o qualsevol dels nombrosos subjectes que hi interaccionen. En tot cas, el *hacking* és sempre, per naturalesa, un accés remot; és a dir, realitzat a distància pel subjecte que per mitjà d'Internet, normalment, s'entremet en un sistema sense tenir-hi contacte físic.

No és *hacking* pròpiament dit l'accés directe en el mateix terminal i no autoritzat a un sistema informàtic. Aquest comportament, usual en l'àmbit familiar o laboral i generalment realitzat per a obtenir informació sensible que pot estar continguda en el sistema, no es pot considerar *hacking* a efectes criminològics, atès que modifica l'àmbit de risc que caracteritza el més usual que és el que s'executa en el ciberespai; tanmateix, és evident que aquesta forma de *hacking*, que aquí no ens interessa, sí que constitueix un accés il·lícit a un sistema informàtic, tal com descriuen la major part dels codis penals en relació amb aquesta conducta.

Tampoc no es pot considerar *hacking* la situació en què el subjecte utilitza uns programes informàtics determinats per a extreure informació del sistema, però sense que es pugui dir que el *hacker* ha tingut cap tipus d'accés real al sistema.

És a dir, independentment que s'hagi accedit a les dades o no, el fet rellevant perquè puguem dir que el tipus de ciberatac que s'ha comès és *hacking* és que s'hagi produït una entrada no autoritzada en el sistema aliè, i no n'hi ha prou que a causa de la introducció d'algun *malware* o un altre tipus de rutina el mateix sistema enviï informació al *hacker*.

3.1.2. Infeccions de *malware* i altres formes de sabotatge cibernètic

Un dels principals riscos, molts dels quals assumits, a què s'enfronten tant les empreses com els particulars a l'hora d'endinsar-se en el ciberespai és patir l'anomenat *sabotatge informàtic*, que inclou tant l'enviament de virus informàtics que aprofiten la immensitat del ciberespai per a multiplicar-se i accedir

a milers de terminals, com qualsevol altra forma de destrucció d'arxius o dades de terminals concrets i determinats, amb finalitats industrials o de dany individual.

En relació amb el sabotatge informàtic tenim el sabotatge cibernètic, que altres autors anomenen *cibervandalisme*, com ara atacs als sistemes informàtics, a la informació que contenen, a les xarxes de comunicació o als serveis d'Internet. El sabotatge cibernètic pot afectar els mateixos sistemes informàtics i altres elements de *hardware* que els constitueixen i que són avaluables econòmicament; també pot afectar la informació continguda en aquests sistemes i que pot tenir un valor econòmic o personal, en el sentit sentimental i relacionat amb la pròpia dignitat, per al subjecte passiu, i també pot afectar la funcionalitat del sistema informàtic en el marc de l'activitat econòmica de què es tracti.

La forma més popular de sabotatge és l'enviament de virus destructius, que s'ha de considerar una forma de distribució de *malware* o *software* maliciós destinat a danyar, controlar o modificar un sistema informàtic.

Des que van aparèixer als anys setanta, els virus han esdevingut un fenomen gairebé natural en el ciberespai, si bé en els darrers anys, a mesura que la interconnexió de sistemes en xarxa s'ha anat popularitzant, hi ha hagut un creixement exponencial i s'ha passat dels més de dos mil virus que es calculaven l'any 2000 fins als 137.000 virus del 2003; actualment es calcula que hi ha milions d'ordinadors infectats per tot tipus de *malware*.

Tipus de *malware*

Dins del *malware* hi ha diverses modalitats de *software* amb objectius molt diferents, des dels que tracten de destruir el sistema o la informació que contenen, com els virus i alguns tipus de cucs (*worms*) o troians (*trojans*), fins als *keystrokeloggers* o *spyware*, que capturen informació dels sistemes informàtics, passant pels que permeten l'accés remot del sistema informàtic per mitjà de la Xarxa, com els *botnets* o els *rootkits*, que amaguen el *software* maliciós o permeten el control del sistema.

Avui, l'enviament de *malware* per a infectar un sistema sol ser un pas rutinari més dins d'una dinàmica complexa definida amb la finalitat d'aconseguir objectius generalment consistents en la defraudació econòmica. En altres paraules, l'enviament de *malware* actualment és un comportament inicial necessari per a la realització de l'atac final consistent en un atac al patrimoni o a la intimitat dels usuaris.

De fet, els darrers estudis demostren que el *malware* ja és el principal tipus de virus existent: troians, cucs, *backdoors* i d'altres. Tots tracten de permetre l'entrada posterior a l'ordinador o tenir-ne el control futur, creant vulnerabilitats que posteriorment aprofitaran els *hackers*. Els usos que després es donen al sistema infectat poden ser diversos: des de constituir l'objecte mateix de l'atac en obrir el *malware* una porta per al *hacking*, fins a l'ús com a terminal des del qual s'efectuaran enviaments futurs de *malware* per a infectar altres terminals, passant per la seva utilització perquè el sistema enviï informació per a una pròpia victimització.

Atacs de *botnet*

Això succeeix sobretot en el cas dels atacs de *botnet*, en què s'infecta amb *backdoors* un conjunt de sistemes (*bots*) que passen a ser controlats per un únic usuari (*botmaster*). Un *botnet* pot ser instruït pel seu controlador per a realitzar funcions de tipus molt divers, entre les quals destaquen els atacs de denegació de serveis que després analitzarem, la situació en el sistema del *hosting* o allotjament de webs malicioses dedicades al blanqueig de diners, la realització de fraus per mitjà de *phishing* o la distribució de pornografia infantil, la realització d'activitats d'escaneig de sistemes i webs vulnerables per a la realització d'altres conductes delictives, o l'enviament d'un gran nombre de correus electrònics no sol·licitats (*spam*).

Una altra forma de sabotatge però que no s'inclouria en l'anomenat *grup de delictes cibernètics* és el sabotatge d'*insiders*. Es tracta de la conducta que duu a terme un treballador o extreballador amb accés a l'empresa o institució que aprofita aquesta posició per a danyar, destruir o distribuir tanta informació com sigui possible.

Els atacs de denegació de serveis o DoS (*denial of services*) és una altra forma de sabotatge que consisteix a utilitzar tècniques per a carregar els recursos de l'ordinador objectiu i produir la negació d'accés del servidor a altres sistemes informàtics.

Se sol dur a terme mitjançant la saturació del sistema després d'efectuar un enviament massiu d'informació que produeix una sobrecàrrega dels recursos del sistema i la inutilització conseqüent del servei amb els danys econòmics que això comporta, i es converteix en *distributed DoS* (DDoS) quan es realitza per mitjà de molts terminals gràcies o bé a una infecció *botnet* o bé a la col·laboració de múltiples usuaris que duen a terme l'atac alhora.

Atacs DoS

Aquest tipus d'atac es va popularitzar l'any 2000 quan es van produir els atacs a pàgines web comercials molt conegudes (Yahoo, Ebay, Etrade, etc.), l'objectiu dels quals era danyar la reputació de les empreses que ofereixen serveis a Internet impedint el funcionament correcte de les seves activitats, tot i que, en els darrers anys, també s'ha utilitzat aquest tipus d'atac amb finalitats de hacktivisme polític, és a dir, de difusió de missatges de protesta a Internet generalment adreçats contra organismes o estats.

L'*spam* és el següent atac destacable als terminals, en aquest cas, als sistemes informàtics consistents en ordinadors, i que es duu a terme per mitjà del correu electrònic.

L'*spam* és un *e-mail* no sol·licitat que se sol enviar a un gran nombre d'adreces electròniques per mitjà d'una adreça electrònica de les que ofereixen els serveis de correu gratuït, com per exemple Hotmail, o bé des d'un sistema informàtic infectat, convertit en *botnet* i utilitzat per l'*spammer* que adquireix les adreces de correu "hackejant" sistemes informàtics o utilitzant *spyware* o altres sistemes de cerca d'adreces electròniques per mitjà de la Xarxa.

L'*spam* té diverses finalitats, entre les quals, l'enviament il·lícit de publicitat, l'intent d'infecció del sistema per mitjà de *malware* i l'intent de *phishing*. En tot cas, l'enviament de *spam*, a més de la recollida prèvia de l'adreça electrònica, ja es pot considerar un atac al terminal informàtic.

Malgrat que el principal risc que comporta la recepció de correus *spam* rau en la possibilitat de ser infectat per algun tipus de *malware* que posteriorment s'utilitzi per a defraudar la víctima, no s'ha de menysprear l'enorme gravetat que representa el simple fet de rebre correus no volguts fins i tot en el cas de no ser infectats per ells.

Costos econòmics de l'*spam*

Segons un estudi sobre els costos econòmics de l'*spam*, representa un cost per a les empreses dels Estats Units d'Amèrica de gairebé nou milions de dòlars per any, 2,5 bilions per a les d'Europa i 500 milions per als prestadors de serveis. Aquestes macroxifres encara criden més l'atenció quan es concreten en el cost que comporta per a les empreses la neteja de *spam*: d'uns 600 $ a uns 1.000 $ de pèrdues per any en productivitat per usuari, amb una mitjana de 874 $ de pèrdua de rendiment per persona a causa dels deu correus de *spam* diaris rebuts per compte de correu en l'àmbit de l'empresa.

3.1.3. Ocupació o ús de xarxes sense autorització

També considerem un ciberatac pur l'atac directe a les xarxes, de forma concreta a la utilització d'un terminal de comunicació que és titularitat d'un altre subjecte, i que comença a ser habitual ja no solament en xarxes de comunicació de televisió per cable, sinó també en les mateixes xarxes telemàtiques com Internet, a causa de la popularització del sistema Wi-Fi i de la facilitat de connectar-se a aquestes xarxes. Finalment, l'altre element de les TIC, els serveis, concretament els serveis generals de comunicació i difusió de continguts de telecomunicació, també es veuen avui dia greument afectats per tot un seguit de comportaments de pirateria de senyals d'emissió radiofònica, televisiva i d'Internet que, mitjançant la creació de *software* específic que s'instal·la en un sistema informàtic perquè amb la connexió a l'antena ja es pugui "piratejar el senyal digital de què es tracti" o bé mitjançant altres sistemes més arcaics com la duplicació de claus o similars, posen realment en perill els interessos comercials dels que han aprofitat la mundialització d'Internet per crear un nou model de negoci basat en la comunicació digital de continguts.

3.1.4. *Anti-social networks*

Per acabar, en relació amb els ciberatacs purs cal fer referència a una de les formes més noves de conducta criminal en el ciberespai que alguns autors han batejat com a *anti-social networks* o xarxes socials antisocials.

L'***anti-social networks*** és un comportament preparatori de les conductes criminals posteriors, que tracta d'assegurar-les i facilitar-les, i consisteix en la manipulació de xarxes socials o de grups d'aquestes amb la finalitat d'utilitzar-les després per al frau o per a qualsevol altre tipus de ciberdelicte.

Al cap i a la fi, i com han assenyalat diversos autors, les xarxes socials tenen algunes propietats intrínseques que les fan ideals perquè les aprofitin adversaris o perquè les utilitzin els que volen defraudar altres persones: en primer lloc, tenen una gran i àmpliament distribuïda base d'usuaris; en segon lloc, estan formades per grups d'usuaris que comparteixen interessos socials semblants, la qual cosa comporta un desenvolupament de la confiança entre ells i l'ús de recursos compartits; en tercer lloc, la plataforma permet als usuaris la instal·lació d'aplicacions pensades contra el frau i altres cibercrims semblants. Totes aquestes característiques donen l'oportunitat als cibercriminals de ma-

nipular els comptes d'Internet dels usuaris o a ells mateixos directament i de portar-los a executar conductes antisocials contra la resta de persones en el ciberespai sense el consentiment que l'estan duent a terme.

3.2. Ciberatacs rèplica

En aquesta categoria s'inclouen tots els delictes en què el ciberespai s'ha convertit en un nou mitjà des del qual es duen a terme delictes tradicionals.

En el cas dels **ciberatacs rèplica**, l'atac no es realitza a un terminal informàtic, ni tampoc el contingut no és l'objecte de la il·licitud, sinó que la Xarxa és el nou mitjà utilitzat per a cometre una infracció que abans se servia d'altres mitjans. Es tracta, per tant, de rèpliques, dutes a terme en el ciberespai, de crims que ja es realitzaven, d'una altra manera, a l'espai físic.

Tanmateix, els trets especials d'aquest nou àmbit de realització criminal que és el ciberespai confereixen a la conducta una singularitat tal que sembla pràcticament una conducta nova.

3.2.1. Els ciberfraus

Entre els **ciberfraus** trobem, de primer, els fraus d'Internet, en què les xarxes telemàtiques esdevenen l'instrument mitjançant el qual s'aconsegueix un benefici patrimonial derivat d'un perjudici patrimonial a una víctima.

Hi ha moltes maneres d'aconseguir accedir al patrimoni de terceres persones, utilitzant les nombroses modalitats de relació comercial existents en el ciberespai, i també les debilitats de seguretat dels sistemes informàtics que donen accés al patrimoni de manera indirecta o indirecta, ja que contenen les claus o dades bancàries dels usuaris.

Exemples de ciberfraus

Així, entre els ciberfraus més coneguts trobem els fraus de targetes de crèdit, els fraus de xecs, les estafes d'inversió, les estafes piramidals realitzades per Internet, les conegudes estafes de la loteria, les vendes *online* defraudadores en què no s'envia el producte que s'ha comprat (o s'envia amb unes altres característiques, com en el frau en les subhastes, o no es paga el rebut o es cobren serveis no establerts prèviament, les estafes d'inversió en què es cobren despeses no previstes o no s'expliquen pèrdues inesperades, a més dels atacs de *scam* en què es prometen quantitats importants de diners a canvi de petites transferències relacionades amb ofertes de treball, loteries, premis o d'altres, entre una varietat de fraus que es va transformant (o adaptant, segons la terminologia que utilitzarem més endavant) d'una manera constant.

Frau en les subhastes

Un dels fraus més comuns i que es manté com a habitual els últims anys és l'anomenat *auction fraud* o *frau en les subhastes*, consistent en la tergiversació d'un producte o el no lliurament conforme als pactes en els sistemes de subhasta *online*, del tipus eBay.

Dins d'aquest grup també s'inclou l'enviament de correus electrònics anomenats *scam*. Es tracta de l'estafa tradicional, però, en aquest cas, la forma de comunicació entre les persones per a realitzar l'engany sobretot és Internet, mitjançant correu electrònic o l'ús de les xarxes socials. És més aviat una categoria genèrica que pot comprendre gairebé tots els fraus, si bé se sol utilitzar per a referir-se als fraus menys fins, en què l'engany és poc elaborat i en què l'error de la víctima pot anar més enllà del que és habitual.

Cartes nigerianes

En aquest cas podríem integrar el conegut cas de les "cartes nigerianes", estafa clàssica semblant a la famosa "estafa de l'estampa", en què l'engany s'aconsegueix explotant l'ànim de lucre de la víctima, a banda de moltes altres que han sorgit posteriorment, com la de la loteria o la de treballar des de casa, sempre caracteritzades perquè tracten d'interessar la víctima o guanyar-se'n la confiança perquè finalment realitzi l'acte de disposició patrimonial que la perjudica. En aquest tipus d'estafes, el factor humà, més concretament la vulnerabilitat de la persona, és l'element essencial perquè l'engany tingui èxit.

El ***phishing*** és una altra modalitat de ciberfrau que es defineix com el mecanisme criminal que utilitza tant enginyeria social com subterfugis tècnics per a robar les dades d'identitat personals dels consumidors i les dades de les targetes de crèdit o comptes bancaris que tenen.

L'ús de l'enginyeria social es produeix quan s'utilitza la identitat personal d'un altre individu (*spoofing*) mitjançant la falsificació de llocs web, per a portar els consumidors a confiar en la veracitat del missatge i divulgar les dades objectiu. Quan s'utilitzen altres artificis tècnics, com ara redireccionar un nom de domini d'una pàgina web real situada en la memòria cau del subjecte o d'una altra manera, a una pàgina web falsa, o monitorar la intervenció del subjecte en la pàgina web real, s'utilitza el terme *pharming*.

3.2.2. *Identity theft* i cibersuplantació de la identitat

El robatori d'identitat o *identity theft* és el següent grup de conductes de què cal tractar, ja que, encara que no sigui nou, adquireix una nova dimensió en el ciberespai.

El **robatori d'identitat** es pot definir com l'adquisició total o parcial per part d'un individu de les dades d'un altre individu per a usar-les com si li pertanyessin, si bé, en general, quan es parla d'*identity theft* s'utilitza ja pressuposant el futur ús delictiu de la suplantació, és a dir, com la utilització o explicació de les dades d'identificació personal o un altre tipus d'informació de la persona com ara el nom o el número de DNI, per a cometre frau o participar en altres activitats il·legals.

Tot i que la suplantació de personalitats també es produeix fora del món virtual, en el ciberespai és més fàcil d'executar i potencialment molt més perillosa perquè, en primer lloc, l'eliminació de la immediatesa física i les possibilitats tècniques per a obtenir informació personal i per a simular fan que sigui possible tant obtenir dades privades necessàries per a suplantar la persona com actuar directament fent-se passar per ella i, en segon lloc, hi ha moltes persones connectades en el ciberespai que efectuen operacions financeres i de qualsevol altre tipus. En definitiva, Internet no solament és el mitjà que permet realitzar l'*identity theft*, sinó que a més és la raó del gran risc que comporta aquest delicte actualment, ja que en el ciberespai ha augmentat de manera significativa la necessitat d'utilitzar les dades personals per a realitzar transaccions, operacions o accions, no sempre comercials, per part dels titulars d'aquesta identitat.

D'altra banda, cal tenir en compte que si bé generalment el robatori d'identitat es duu a terme com un primer pas per a l'execució posterior d'algun tipus de frau informàtic, el *phishing*, atesa la importància actual de l'anomenada *identitat digital*, aquesta suplantació no solament comporta un risc per al patrimoni de les persones, sinó també per a molts altres béns jurídics. El **robatori d'identitat a Internet** es pot dur a terme de moltes maneres, des de les més senzilles, en què s'utilitza l'enginyeria social per a suplantar la personalitat, fins a les més complexes, en què s'**usa l'enginyeria informàtica per a aconseguir amb els diversos mecanismes existents la identificació dels sistemes que actuen en el ciberespai**. En aquestes darreres cal situar l'*spoofing*, que, al seu torn, també pot ser poc o molt elaborat.

Actualment, es diferencien com a mínim cinc formes de ***spoofing***:

- ***IP spoofing***, en què mitjançant la utilització de programes específicament destinats a això, se substitueix l'adreça IP original per una altra.

- ***ARP spoofing***, en què es falsegen les anomenades *taules ARP* d'una víctima per a portar el seu sistema MAC a enviar els paquets a l'hoste atacant i no a la destinació corresponent.

- ***DNS spoofing***, en què es modifica el nom de domini IP d'un servidor DNS, aprofitant alguna vulnerabilitat, cosa que se sol utilitzar per al *pharming*, en què el subjecte posa l'adreça web d'una entitat bancària oficial i se'l remet a una web falsa.

- ***Web spoofing***, potser el més comú de tots aquests atacs, en què, per mitjà d'un enllaç o altres formes d'engany, es fa passar una pàgina web, imitada i allotjada en un altre servidor, per la real, mitjançant un codi que sol·licita la informació requerida pel sistema víctima a cada servidor original i remet a la pàgina web falsa.

- ***Mail spoofing***, consistent en la suplantació de l'adreça de correu electrònic d'altres persones o entitats, utilitzada generalment per a enviar *spam* o com a començament de la dinàmica d'atac del *phishing*.

3.2.3. El ciberespionatge

L'espionatge informàtic o *snooping* és una altra modalitat de cibercriminalitat en què les xarxes són el nou instrument des del qual s'ha d'interceptar la comunicació. Es pot realitzar per mitjà d'un *insider* que aprofita la situació que té en l'empresa o amb la persona de confiança per danyar-la, per mitjà d'un *hacker* que accedeix directament al sistema informàtic o bé per mitjà de tot un conjunt de *software* la finalitat principal del qual és l'obtenció de dades de tipus molt divers i amb objectius diferents. Aquest *software* s'anomena *spyware* i pot ser enviat per correu electrònic per part de l'atacant, o bé pot ser descarregat inconscientment per la víctima quan descarrega algun altre tipus de *software*.

L'***spyware*** és un *software* que s'instal·la en un sistema informàtic i en recopila una determinada informació que després envia a un altre sistema. Per mitjà de l'*spyware* es pot accedir a informació personal o a secrets d'empresa obtinguts en correus electrònics i un altre tipus de missatges, tot i que generalment aquest tipus de *software* el que recapta és un conjunt de dades necessàries per a realitzar altres atacs posteriors a la intimitat o al patrimoni del subjecte, com les seves claus informàtiques o bancàries, l'adreça IP o els números de telèfon.

Dins l'*spyware* té una importància especial l'ús de programes *sniffers* i *keylogger*, que en darrer terme pretenen captar informació per a l'espionatge industrial o bé per a la utilització posterior en atacs de *spam*, *phishing*, *botnet*, etc.

Els ***sniffer*** són programes de captura de trames d'informació que no hi estan destinades.

En realitat, els *packet sniffer* capturen tot el trànsit que viatja d'una determinada manera o amb unes característiques concretes per la Xarxa, i això pot ser utilitzat amb la finalitat de detectar fallades en xarxes o sistemes o fins i tot *hackers*, o bé amb finalitat maliciosa, per a capturar de manera automàtica contrasenyes de sistemes informàtics o noms d'usuari de la Xarxa per al posterior accés informàtic o enviament de *spam*, respectivament, o per a tractar d'interceptar missatges de correu electrònic o espiar converses de xat, etc.

Quant als ***keylogger***, es tracta d'un tipus de *hardware* o *software*, el que més ens interessa aquí, que es dedica a enregistrar les pulsacions que es realitzen en el teclat amb la finalitat de memoritzar-les i després enviar-les al subjecte, que posteriorment les utilitzarà per a accedir a la informació o al patrimoni de la víctima.

Per bé que en l'àmbit de l'empresa o fins i tot en les relacions personals, en la família mateixa, es pot començar a produir l'ús de *hardware keylogger*, el que més ens interessa aquí són els casos en què per mitjà d'un troià o una *backdoor* s'instal·la en un sistema informàtic aliè un *software* que, gràcies a l'enregistrament de pulsacions, aconsegueix que el cibercriminal accedeixi a contrasenyes del sistema o a claus bancàries entre altres informacions.

Finalment, també es poden esmentar altres formes de *snooping* o captació de dades d'un altre sistema sense modificar-les i sense autorització, com per exemple l'anomenat *DNS snooping*, en què s'obtenen noms de domini resolts per un servidor DNS.

Cookies

Finalment, alguns autors situen dins de l'*spyware*, encara que com a conductes invasores de la intimitat amb menys lesivitat, les anomenades *cookies*, arxius que emmagatzemen informació de l'usuari en el seu propi sistema i que serveixen perquè els llocs web identifiquin el visitant. La tecnologia de les *cookies* permet que una pàgina web, per defecte, insereixi amb dissimulació el seu propi identificador en el terminal d'una manera permanent per tal de poder rastrejar el comportament de l'individu a Internet.

3.2.4. Ciberblanqueig de capitals i ciberextorsió

D'altra banda, la relació entre el crim organitzat i la cibercriminalitat que hem comentat anteriorment fa que actualment el ciberespai i els diferents serveis que ofereix s'utilitzin per al blanqueig de capitals derivats, generalment, de les activitats cibercriminals d'aquests grups. Malgrat que hi ha tècniques molt diverses per a blanquejar els diners virtuals, les més comunes avui són l'**ús de mules** per a l'enviament de diners i l'assoliment de divises per mitjà dels jocs *online*. Quan es parla de les mules, especialment en l'àmbit del *phishing*, es fa referència als **usuaris d'Internet que tenen (o obren) comptes bancaris**, i que són reclutats via web sota l'aparença d'un contracte de treball realitzat des de casa, i que consisteix en la recepció en els seus comptes bancaris de diners i l'enviament d'aquests, generalment per mitjà de sistemes com el de Western Union, o també per transferència bancària, als comptes corrents dels cibercriminals a canvi d'una petita comissió. Pel que fa als webs de joc *online*, impliquen la creació d'una economia virtual en què s'intercanvien els diners reals per diners virtuals per a participar en els jocs. Això és aprofitat per les organitzacions criminals per a, primer, intercanviar els diners reals per diners virtuals i, després, tornar-los a recuperar com a reals, amb la qual cosa compliquen la perseguibilitat dels béns il·lícits.

També en relació amb les bandes organitzades trobem el següent comportament criminal, en què l'únic que canvia és el ciberespai com a nou mitjà utilitzat, en aquest cas, l'element amb què s'amenaça. Ens referim a l'extorsió realitzada per cibercriminals, generalment per bandes organitzades, consistent en la sol·licitud de quantitats econòmiques importants a canvi de cessar en la realització d'algun tipus de ciberatac o fins i tot de començar a executar-lo.

Igual que en els casos d'extorsió "normal", el criminal aprofita el fet que per a la víctima pot ser més senzill, i fins i tot beneficiós, atendre la sol·licitud del criminal i no rebre l'atac que ser-ne víctima i tractar de defensar-se posteriorment. En el cas dels comportaments cibercriminals, aquestes conductes sembla que proliferen en relació amb les pàgines web dedicades a les apostes i als jocs d'atzar *online*, interessades a pagar quantitats no gaire grans a les màfies a canvi de no patir un atac de denegació de serveis o d'altres en dates concretes que els pot paralitzar la pàgina web i fer-los perdre una quantitat de diners significativament superior.

3.2.5. El ciberassetjament

Finalment, el ciberespai també és un mitjà d'intercomunicació personal, per la qual cosa dins d'aquesta categoria d'infraccions tradicionals en què el que canvia és el mitjà de realització de les infraccions trobem les conductes d'atac a béns personalíssims com les amenaces, les coaccions, les injúries, les calúmnies i altres agressions a l'honor o a la llibertat. Algunes d'aquestes pràctiques destaquen per la transcendència especial que tenen, ja que afecten menors d'edat, com el *cyberbullying* i el *child grooming*.

El ***cyberbullying*** ha estat definit com la conducta que consisteix a "infligir dany d'una manera voluntària i repetida per mitjà de text electrònic", i és un comportament que, si no substitueix, sí que complementa moltes conductes de *bullying* entre menors, a causa de la popularització també en aquest espectre de la població de l'ús de les TIC en general, i de les xarxes socials, en particular.

En aquest cas, i respecte del *bullying* tradicional, el poder que s'exerceix sobre la víctima ja no és físic ni (solament, ja que també ho pot ser) social, sinó que es tracta d'un poder en línia que es deriva de la unió entre la crueltat associada a aquest tipus d'intimidació i l'habilitat: és el jove capaç de navegar i dominar el món electrònic, el que està en una posició de poder en relació amb una víctima i pot utilitzar les TIC per a assetjar les víctimes.

S'inclou també dins de la modalitat d'assetjament en el ciberespai el ciberassetjament sexual, tant a menors com a majors d'edat, en què s'aprofita l'ús de diferents instruments de comunicació com el Messenger, el correu electrònic, el sistema de comunicació oral Skype o les xarxes socials com Twitter o Facebook per a atemptar contra la llibertat sexual d'una altra persona. Cal tenir en compte que l'atemptat pot ser de tot tipus, ja que la popularització de l'ús de les *webcams* amplia profundament el catàleg de comportaments relacionats amb la llibertat sexual que es poden realitzar per mitjà d'Internet; ja no es tracta únicament de la possibilitat de realitzar un assetjament sexual per mitjà de paraules, sinó que ara és possible la difusió directa de contingut sexual per

mitjà de paraules, la difusió directa de contingut sexual a un menor o, fins i tot, la visualització d'una actitud sexual de la víctima coaccionada per una amenaça.

El comportament més conegut d'atac relacionat amb la indemnitat i la llibertat sexual en el ciberespai és el ***child grooming***, que consisteix a contactar amb menors per mitjà de les xarxes socials o d'altres formes de comunicació com les sales de xat, els canals de Messenger o similars, per apropar-s'hi i posteriorment intentar un assetjament sexual.

Un altre comportament de moda relacionat amb aquest àmbit és l'anomenat ***sexting***, que consisteix en la realització, per part de menors, de fotografies pròpies de nus complets o de parts nues i l'enviament d'aquestes fotografies, generalment per mitjà del telèfon mòbil, a altres persones, juntament amb textos obscens i amb la finalitat de conèixer persones o d'enviar missatges d'amor o d'odi.

Finalment, cal destacar una altra conducta d'assetjament per mitjà de la Xarxa, el ***cyberstalking***, entès com l'ús d'Internet o una altra tecnologia de la comunicació per a assetjar, perseguir o amenaçar algú. Se substitueixen les trucades de telèfon a hores en què la persona no és a casa, o les visites a la feina i a casa, a més dels seguiments no volguts, per altres conductes com l'enviament de desenes de correus o de missatges per mitjà de les xarxes socials, la posada a disposició del públic de fotografies, missatges o correu de la víctima en pàgines web, etc. Habitualment, el *cyberstalker* selecciona la víctima per mitjà de xats, fòrums, etc. i una vegada seleccionada realitza una o diverses formes de persecució, com ara intentar contactar-hi unes quantes vegades, amenaçar-la amb violència física, sol·licitar-li sexe de manera explícita o enviar-li imatges obscenes, sempre tenint en compte el caràcter repetitiu de l'acció. El mitjà més comú que utilitzen els *cyberstalkers* és el correu electrònic, per mitjà del qual envien missatges d'assetjament, d'amenaça, d'odi, obscens o imatges feridores. Altres formes de *cyberstalking*, menys usades, són instar altres usuaris d'Internet a assetjar o amenaçar la víctima mitjançant fòrums o el xat, enviar arxius infectats amb la intenció de danyar el sistema informàtic de la víctima i el robatori d'identitat; aquestes dues darreres conductes es consideren *cyberstalking* únicament si l'objectiu de l'agressor és intimidar la víctima.

3.3. Ciberatacs de contingut

L'últim grup, les conductes de contingut, fa referència a una forma concreta dels atacs anomenats *rèplica*, però amb una singularitat i amb problemàtiques jurídiques tan especials que requereixen un tracte separat.

Els **ciberatacs de continguts** aglutinen totes les conductes en què el centre de la infracció és el contingut que es comunica o es transmet per Internet.

La facilitat amb què avui es pot digitalitzar qualsevol tipus d'informació i amb què es pot comunicar aquesta informació a un gran nombre de receptors de manera simultània i situats en llocs diversos d'arreu del món converteix la Xarxa en un mitjà obert en què els continguts il·lícits, igual que els lícits, també poden viatjar amb facilitat. Cal tenir en compte, a més, que a diferència de la resta de mitjans de comunicació Internet funciona simultàniament com un mitjà d'edició i com un mitjà de comunicació, en el sentit que la dicotomia entre emissor i receptor es difumina en el ciberespai, on un usuari pot passar de ser receptor a ser també comunicador i productor de continguts. Si a això se suma la popularització d'Internet i la facilitat per a accedir-hi i enviar-hi informació, a més de la utilització progressiva per part dels menors d'aquest sistema de comunicació, aleshores es pot entendre que des de fa ja més d'una dècada sorgís una preocupació pels continguts, davant l'aparició de tot un conjunt de conductes que comparteixen la il·legalitat esdevinguda no del mitjà utilitzat, sinó del contingut distribuït per Internet.

3.3.1. Pornografia infantil a Internet

Un dels problemes clàssics amb caràcter internacional és la difusió de pornografia infantil, de manera que s'aprofita la capacitat de comunicació transnacional i l'anonimat que aporta Internet per a difondre material pornogràfic en què s'usen infants per a realitzar-lo, o bé s'utilitzen imatges figurades representatives de menors d'edat mantenint relacions sexuals.

El grup Interpol especialitzat en crims contra els infants ha definit la pornografia infantil com "tota forma de representació o promoció de l'explotació sexual dels infants, incloent-hi els materials escrits i d'àudio, que es concentrin en la conducta sexual o en els òrgans genitals dels infants".

Aquest fenomen està cada vegada més vinculat a l'ús de les noves tecnologies de la informació, fins al punt que, actualment, des d'una perspectiva criminològica, es pot dir que la majoria d'aquests comportaments es perpetren bàsicament per mitjà d'Internet.

La **pornografia infantil** ha passat per diverses **fases** al llarg dels anys:

1) En una primera fase, s'empraven **pàgines web allotjades en servidors d'Internet**, en què el traficant comerciava amb el material pornogràfic que posava a disposició dels usuaris, els quals prèviament accedien a pagar una contraprestació que se satisfeia per mitjà d'un càrrec en la targeta de crèdit de l'adquirent.

Dins d'aquesta primera fase es poden diferenciar dues modalitats: d'una banda, la de l'usuari que decideix navegar amb l'objectiu d'accedir a una pàgina web concreta el contingut de la qual sap amb certesa que conté material pornogràfic infantil, i de l'altra, la del que crea la pàgina web mateixa. No obstant això, com que aquest sistema era fàcil de detectar es va abandonar i es van utilitzar altres modalitats.

2) La segona fase es desenvolupa en els **xats a temps real** en què els pedòfils dialoguen entre ells i acorden l'intercanvi per mitjà del correu electrònic del material en qüestió, la compra directa d'aquest element per mitjà d'alguna pàgina web o la simple descàrrega d'arxius, en què l'intercanvi de fotografies de pornografia infantil és qüestió de segons. Una altra d'aquestes noves modalitats conductuals que van sorgir són els **grups de notícies** i **fòrums** com a mitjà de comunicació, a més del **camuflatge de les pàgines web** de pornografia infantil, no accessibles per mitjà de cercadors i només localitzables per a iniciats. Posteriorment, com que els pedòfils eviten els *chat rooms* quan s'adonen que poden estar infiltrats per agents encoberts, la figura del traficant de pornografia infantil és substituïda en gran mesura per la dels consumidors-que informalment s'associen sense ànim de lucre. Aquests **socis**, que actuen de manera coordinada, es poden descarregar a l'ordinador una gran quantitat de fotografies en poca estona a partir de tècniques d'intercanvi per mitjà de correu electrònic o de fórmules com ***send to receive***.

En aquesta evolució accelerada, els programes de globalització d'arxius individuals han habilitat noves vies comissives, que permeten a l'usuari la possibilitat de compartir una part del contingut del seu ordinador amb les persones que estiguin connectades a la xarxa i utilitzin aquest mateix programa (programes tipus Napster), de manera que els usuaris dels programes d'arxius compartits posen en comú el seu material pornogràfic, sense cap necessitat d'establir contacte directe, realitzar adquisicions individualitzades o mantenir conversa. Així, l'**intercanvi mutu de material substitueix la compra al traficant**. Dins d'aquesta modalitat, hem de fer referència a dos tipus de protocols, l'**FTP** i el **P2P**, que donen lloc a dues classes de comportaments molt diferents.

3.3.2. La ciberpirateria intel·lectual

La ciberpirateria intel·lectual és una altra forma de ciberatac de contingut que comprèn des de la d'obres digitalitzades fins a la comunicació pública de les obres per mitjà de *streaming* a canvi d'una quantitat de diners, entre moltes altres. Internet ha donat lloc a diverses conductes que es caracteritzen per la infracció de drets de propietat intel·lectual i que inclourien el que s'ha ano-

menat ***ciberpirateria***. La major part d'aquestes formes, però, han desaparegut a causa de l'impacte del comportament que, sens dubte, més mal ha fet a la indústria de l'entreteniment però sobre el qual més es podria discutir la consideració com a pirateria digital, l'intercanvi gratuït d'arxius.

L'ús compartit d'arxius es va iniciar amb el protocol IRC[1] a mitjan dècada dels noranta, i en el canvi de mil·lenni va assolir l'apogeu, primer, amb Napster i, després, amb un nou sistema d'intercanvi d'arxius amb un protocol P2P[2]. Aquest sistema va estar a dalt de tot amb programes com eMule o Ares que va compartir amb els sistemes de *streaming*, fins que s'ha posat en voga el **sistema de descàrrega directa**, de manera que han sorgit programes com Megaupload, RapidShare o MediaFire, que si bé aparentment servien per a guardar arxius i codificar-los, es relacionaven amb un gran nombre de blogs i pàgines que enllaçaven els noms dels continguts protegits amb els dels codis de baixada en pàgines web d'aquest tipus.

(1)Sigla que correspon a *Internet relay chat*.

(2)Sigla que correspon a *peer-to-peer*.

Megaupload

Si bé el tancament de Megaupload per part de l'FBI va poder significar un atac aparent al sistema de descàrregues a Internet, la substitució immediata d'aquest sistema per altres webs i altres sistemes d'intercanvi gratuït d'arxius fa que difícilment sigui una opció real per al consumidor de béns culturals en el ciberespai el fet de pagar per això. De fet, a més de la proliferació de llocs de baixada gratuïta d'arxius i de noves formes d'explotació, en alguns casos lícites, però contràries a la configuració tradicional de la propietat intel·lectual, s'uneix el fet que en els motors de cerca com Google i Yahoo! i Bing, molts dels resultats principals que ofereixen les seves pàgines proporcionen enllaços a continguts no autoritzats o a llocs que infringeixen els drets d'autor. Aquestes empreses, no obstant això, tracten de respondre immediatament a les demandes i sol·licituds dels titulars dels drets.

3.3.3. Difusió d'altres continguts il·lícits

La possibilitat d'introduir informació a la Xarxa amb continguts il·lícits diversos i d'utilitzar-la per a difondre aquests continguts ha convertit la Xarxa en un mitjà potent per a cometre delictes com l'apologia i altres actes preparatoris del terrorisme.

Dins d'aquesta última categoria trobem l'anomenat ***cyberhate speech*** o ***incitació a l'odi racial***. El ciberespai incrementa el risc que implica aquesta activitat: com a àmbit transnacional i mundial, és un lloc perillós per a difondre missatges racistes i violents, que s'aboquen amb més facilitat a Internet davant la dificultat de perseguir la cibercriminalitat i les facilitats més grans per a l'anonimat que ofereix el medi. Internet permetia substituir prospectes i fullets racistes que eren difosos localment per webs i blogs fàcils de fer i que resultaven molt més eficaços per a transmetre idees odioses a milions de persones arreu del món. Malgrat que no es disposa de xifres fiables, es calcula que són milers les pàgines web que, provinents sobretot dels Estats Units d'Amèrica, fomenten i difonen idees racistes, generalment relacionades amb la supremacia blanca, si bé també n'hi ha que difonen missatges feixistes similars sota altres aparences ideològiques.

També podríem integrar dins d'aquest tipus de cibercriminalitat altres pàgines web en què el missatge d'odi i d'incitació a la violència i de difusió d'idees racistes és menys abstracte i molt més localitzat contra partits polítics, governants o associacions concretes i determinades. Certament, però, aquestes conductes amb prou feines es poden delimitar de la incitació que representen algunes formes de terrorisme.

Exemples de difusió de contiguts il·lícits

En són dos exemples ben coneguts, d'una banda, la campanya, focalitzada a Internet, d'amenaces i incitació a la violència realitzada des de sectors islamistes radicals contra Dinamarca i el dibuixant d'un diari que en les vinyetes identificava Mahoma i els musulmans amb els terroristes, i de l'altra, la campanya duta a terme per mitjà de vídeos a YouTube en què es promocionava la crema d'exemplars de l'Alcorà com una forma de protesta davant la decisió de construir a Nova York, en l'anomenada *zona zero*, una mesquita.

Tots dos comportaments comparteixen no solament el fet de ser missatges d'incitació a l'odi i a la violència, sinó també el fet que malgrat que es realitzen en un àmbit localitzat molt concret (un humorista a Dinamarca i davant d'ell diversos estudiants musulmans des de les universitats a Síria o l'Iran, o un sacerdot d'una petita església d'un petit poble dels Estats Units d'Amèrica), com que s'utilitza Internet per a difondre el missatge, aquest arriba a moltes persones i genera un clima d'odi amb conseqüències difícils de mesurar.

Resum

El fenomen de la delinqüència associada a les TIC és una realitat que està adquirint protagonisme en els darrers anys. No obstant això, en molts casos s'exagera l'amenaça que comporta i en d'altres no es percep el risc real i en part derivat per l'altíssima xifra negra d'aquest tipus de delinqüència.

Cal tenir en compte que l'ús d'Internet ha evolucionat des que va ser creada, de manera que ha passat de ser un mitjà utilitzat per uns quants a convertir-se en el mitjà més usat per a efectuar operacions econòmiques i per a establir relacions socials. De la mateixa manera que ha evolucionat Internet, paral·lelament ho ha fet la cibercriminalitat, i amb aquests elements els seus actors principals, de manera que s'ha passat dels primers atacs destinats als terminals als atacs que tenen com a objectiu altres béns personalíssims com la integritat, la indemnitat sexual o la dignitat personal. Així, en la primera època de la cibercriminalitat era característic l'ús d'ordinadors per a cometre el delicte, precedit per una altra època en què la característica central és que el delicte es comet per mitjà d'Internet fins a una tercera època en què els delictes estan absolutament determinats per l'ús d'Internet i les TIC.

En definitiva, aquesta evolució ens ha permès establir una classificació dels delictes segons la incidència que tenen les TIC en la comissió d'aquests delictes. Així, hem vist que el ciberespai en alguns casos ha esdevingut un generador de noves conductes que tan sols es pot realitzar per mitjà de les TIC i que hem anomenat *ciberatacs purs*. En altres casos, l'evolució de les TIC ha servit per a realitzar delictes que ja es cometien en el món físic, per la qual cosa s'han anomenat *ciberatacs rèplica*, tot i que els trets especials d'aquest nou àmbit els confereix una singularitat tal que els fa semblar conductes noves. I, finalment, hem estudiat els anomenats *ciberatacs de contingut*, que inclouen tots els delictes en què la infracció és determinada per la informació il·lícita que es transmet i que, tenint en compte la difusió que pot oferir Internet, comporta un gran perill.

Exercicis d'autoavaluació

1. La infecció per *malware* és...

a) un ciberatac pur.
b) un ciberatac rèplica.
c) un ciberatac de contingut.
d) Cap de les respostes anteriors no és correcta.

2. El ciberatac que consisteix a adaptar al món virtual comportaments delictius que ja es feia per altres mitjans és...

a) un ciberatac econòmic.
b) un ciberatac rèplica.
c) un ciberatac pur.
d) un ciberatac de contingut.

3. El comportament que duu a terme un adult per mitjà d'Internet per guanyar-se la confiança de menors amb la finalitat de concretar trobades per obtenir concessions de caràcter sexual s'anomena...

a) *child grooming.*
b) *grooming.*
c) *cyberstalking.*
d) *cyberbullying.*

4. La persona que roba informació d'una empresa aprofitant-se de la situació que hi té és...

a) un *hacker.*
b) un *cracker.*
c) un *insider.*
d) un ciberterrorista.

5. El terme *cibercrim* entès des d'un sentit ampli comprèn...

a) qualsevol comportament delictiu realitzat en el ciberespai.
b) només comportaments il·lícits des del punt de vista tradicional en què l'únic canvi és que ara es duen a terme a Internet.
c) conductes el contingut il·lícit de les quals es relaciona directament amb béns existents en el ciberespai.
d) Cap de les respostes anteriors no és correcta.

6. El tipus de ciberfrau que consisteix en propostes de negoci enganyoses s'anomena...

a) *pharming.*
b) *phishing.*
c) *spoofing.*
d) *scam.*

7. El *cyberhate* és...

a) assetjament a menors aprofitant les possibilitats de les càmeres web.
b) incitació a l'odi racial en el ciberespai.
c) inflicció de dany de manera voluntària o repetida per mitjà de text electrònic.
d) realització de fotografies de nus totals o parcials per a penjar-les a les xarxes socials.

8. Des d'un concepte emprat de manera restringida per al cibercrim, només s'hi inclou un comportament delictiu en què...

a) s'utilitzin mitjans tecnològics.
b) s'aprofita el ciberespai per a poder-lo executar.
c) l'essència de l'injust no es pot produir fora d'ell.
d) Cap de les respostes anteriors no és correcta.

9. Quin dels cibercrims següents es pot categoritzar com un ciberatac de contingut?

a) Assetjar algú per mitjà de les xarxes socials.

b) Introduir-se sense permís per mitjà d'Internet en el terminal d'un altre subjecte.
c) Robar les dades d'accés als comptes bancaris.
d) Crear una pàgina web amb missatges que inciten a la violència.

10. El motiu pel qual la xifra negra de la cibercriminalitat és superior a altres formes de delinqüència es deu al fet que...

a) és molt difícil determinar-ne l'autor.
b) els afectats no ho denuncien.
c) la conducta passa inadvertida.
d) Totes les opcions anteriors són correctes.

Solucionari

Exercicis d'autoavaluació

1. a

2. b

3. a

4. c

5. a

6. d

7. b

8. c

9. d

10. d

Glossari

cibercrim *m* Qualsevol delicte dut a terme en el ciberespai.

ciberespai *m* Espai d'intercomunicació social transnacional, universal, popularitzat i en evolució permanent derivat de l'ús de les tecnologies de la informació i la comunicació.

cuc *m* Programa que realitza còpies de si mateix i les allotja en diferents ubicacions de l'ordinador amb la finalitat de col·lapsar els ordinadors i les xarxes informàtiques, de manera que impedeix que els usuaris puguin treballar.

cyberbullying *m* Dany repetit i intencionat per mitjans electrònics com ara telèfons mòbils o Internet realitzat per un grup o individu contra el qual la víctima no es pot defensar de si mateixa.

cybergrooming *m* Ciberassetjament sexual a menors.

cyberhate *m* Difusió de missatges d'odi racial en el ciberespai.

cyberstalking *m* Ús d'Internet o una altra tecnologia de la comunicació per a assetjar, perseguir o amenaçar algú de manera repetida.

denial of services *f* Denegació de serveis consistent en un ciberatac mitjançant el qual se satura el servidor del sistema de manera que només es pot centrar en la petició que realitza l'atacant sense que pugui atendre'n cap més.
sigla **DOS**

DOS *f* Vegeu ***denial of services***.

hacking *m* Qualsevol conducta per la qual un subjecte accedeix a un sistema o equip informàtic sense l'autorització del titular d'aquest, de manera que té capacitat potencial d'utilitzar-lo o d'accedir a qualsevol tipus d'informació que hi hagi en el sistema.

hacktivisme *m* Difusió de missatges de protesta a Internet generalment adreçats contra organismes o estats en relació amb la voluntat de mantenir el ciberespai lliure de normes.

hardware *m* Conjunt de components que integren la part material d'una computadora.

insider *m i f* Cibercriminal que pertany o treballa per a la institució o empresa que és víctima de la infracció.

Internet *f* Xarxa informàtica mundial, descentralitzada, formada per la connexió directa entre computadores mitjançant un protocol especial de comunicació.

keylogger *m* Tipus de *hardware* o *software* que enregistra les pulsacions que s'efectuen en el teclat amb la finalitat de memoritzar-les i posteriorment enviar-les al subjecte que les utilitzarà per a accedir a la informació o al patrimoni de la víctima.

malware *m* *Software* maliciós destinat a danyar, controlar o modificar un sistema informàtic.

nadiu -a digital *m i f* Persona pertanyent a la generació nascuda amb la implantació total d'Internet.

phishing *m* Mecanisme criminal que empra tant enginyeria social com subterfugis tècnics per a robar les dades d'identitat personals dels consumidors i les dades de les targetes de crèdit o dels comptes bancaris que tenen.

protocol FTP *m* Protocol de transferència de fitxers.

protocol IP *m* Protocol d'Internet per a enviar i rebre dades per mitjà d'una xarxa de paquets commutats.

protocol P2P *m* Protocol que permet l'intercanvi directe d'informació, d'igual a igual.
sin. compl. **protocol *peer-to-peer***

protocol *peer-to-peer* *m* Vegeu **protocol P2P**.

scam *m* Concepte que podria incloure gairebé tots els fraus en el ciberespai, si bé se sol utilitzar per a referir-se als fraus menys fins, en què l'engany és poc elaborat i en què l'error de la víctima pot anar més enllà del que és habitual.

sexting *m* Realització, per part de menors, de fotografies pròpies de nus complets o de parts nues i l'enviament d'aquestes fotografies, generalment per mitjà del telèfon mòbil, a altres individus, juntament amb textos obscens i amb la finalitat de conèixer persones o d'enviar missatges d'amor o d'odi.

snooping *m* Accés no autoritzat a dades d'altres persones.

software *m* Conjunt de programes, instruccions i regles informàtiques per a executar certes tasques en una computadora.

spam *m* *E-mail* no sol·licitat que se sol enviar a un gran nombre d'adreces electròniques o bé per mitjà d'una adreça electrònica de les que ofereixen els serveis de correu gratuïts, com ara Hotmail, o bé des d'un sistema informàtic infectat, convertit en *botnet* i utilitzat per l'*spammer* que adquireix les adreces de correu "hackejant" sistemes informàtics o utilitzant *spyware* o altres sistemes de cerca d'adreces electròniques per mitjà de la Xarxa.

spoofing *m* Suplantació de la identitat.

spyware *m* *Software* que s'instal·la en un sistema informàtic, en recull una informació determinada i després l'envia a un altre sistema.

TIC *f pl* Tecnologies de la informació i la comunicació.

troià *m* Programa maliciós que, mitjançant finestres emergents, recull claus; i en general qualsevol altra tècnica que, per mitjà de *software*, permet perfeccionar l'engany fent creure a la víctima que està fora de perill.

Wi-Fi *f* Tecnologia de comunicació sense fil.

Bibliografia

Agustina Sanllehí, J. R. (2010). "¿Menores infractores o víctimas de pornografía infantil? Respuestas legales e hipótesis criminológicas ante el Sexting". *RECPC* (núm. 12-11).

Agustina Sanllehí, J. R. (2009). "La arquitectura digital de Internet como factor criminógeno". *IEJCS* (art. 4, núm. 3).

Álvarez Vizcaya, M. (2001). "Consideraciones político criminales sobre la delincuencia informática: el papel del Derecho penal en la Red". *CDJ* (núm. 10). Madrid.

Bocij, P. (2003). "Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet". *FMPRJI* (vol. 8, núm. 10).

Chawki, M.; Abdel Wahab, M. (2006, primavera-estiu). "Identity Theft in Cyberspace: Issues and Solutions". *LE* (vol. 11, núm. 1).

Chiu, C.; Ku, Y.; Lie, T.; Chen, Y. (2011). "Internet Auction Fraud Detection Using Social Network Analysis and Classification Tree Approaches". *IJEC* (vol. 15, núm. 3).

Choo, K. K. R. (2007). "Zombies and Botnets". *TICCJ* (núm. 233). Canberra.

Chua, C. E. H.; Wareham, J. (2004, octubre). "Fighting Internet Auction Fraud: An Assessment and Proposal". *IEEE Computer* (núm. 10).

Cilli, C. (2005). "Identity Theft: A New Frontier for Hackers and Cybercrime". *Information Systems Control Journal* (vol. 6).

Marco Marco, J. J. (2010). "Menores, ciberacoso y derechos de la personalidad". A: J. García González (coord.). *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet*. València: Tirant lo Blanch.

Morillas Fernández, D. L. (2005). *Análisis dogmático y criminológico de los delitos de pornografía infantil. Especial consideración de las modalidades comisivas relacionadas con Internet*. Madrid: Dykinson ("Colección Monografías de Derecho Penal", 4).

Patchin, J. W.; Hinduja, S. (2006). "Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying". *YVJJ* (vol. 4).

Pathé, M.; Mullen, P. E. (1997). "The impact of stalkers on their victims". *BJP*. A. Pérez Martínez i A. Ortigosa Blanch. "Una aproximación al ciberbullying". A: J. García González (coord.) (2010). *Ciberacoso: La tutela penal de la intimidad, la integridad y la libertad sexual en Internet*. València: Tirant lo Blanch.

Pinguelo, F. M.; Muller, B. W. (2011, primavera). "Virtual Crimes, Real Damages: A Primer On Cybercrimes In The United States and Efforts to Combat Cybercriminals". *VJLT* (vol. 16, núm. 1).

Pittaro, M. L. (2007). "Cyber stalking: An Analysis of Online Harassment and Intimidation". *IJCC* (vol. 1, núm. 2).

Pollock, E. T. (2010). "Understanding and Contextualising Racial Hatred on the Internet: A Study of Newsgroups and Websites". *Internet Journal of Criminology*.

Poullet, Y. (2007). "Hacia nuevos principios de protección de datos en un nuevo entorno TIC". *IDP* (núm. 5).

Prensky, M. (2001, octubre). "Digital Natives, Digital Immigrants". *On the Horizon* (vol. 9, núm. 5). Lincoln: NCB University Press.

Romeo Casabona, C. M. (coord.) (2006). *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*. Granada: Comares.

Sommer, P.; Brown, I. (2011). "Reducing Systemic Cybersecurity Risk". Oxford University Press.*Contribution to the OECD project Future Global Shocks*

Thomas, D.; Loader, B. (eds.) (2000). *Cybercrime: Law enforcement, security and surveillance in the information age*. Londres: Routledge.

Villacampa Estiarte, C. (2010). "La respuesta jurídico-penal frente al stalking en España: presente y futuro". *Revista del Instituto Universitario de Investigación en Criminología y Ciencias Penales de la UV* [en línia]. <http://www.uv.es/recrim/recrim10/recrim10a03.pdf>

Wall, D. S. (2005). "What are Cybercrimes?". *CJR*.

Wall, D. (2007). *Cybercrime: the transformation of crime in the information age*. Cambridge: Polity Press.

Williams, P. (2001, agost). "Organized Crime and Cybercrime: Synergies, Trends, and Responses". *ATC* (vol. 6).

Yar, M. (2005). "The novelty of «cybercrime»: an assessment in light of routine activity theory". *EJC* (núm. 2).

Yar, M. (2006). *Cybercrime and society*. Londres: Sage.