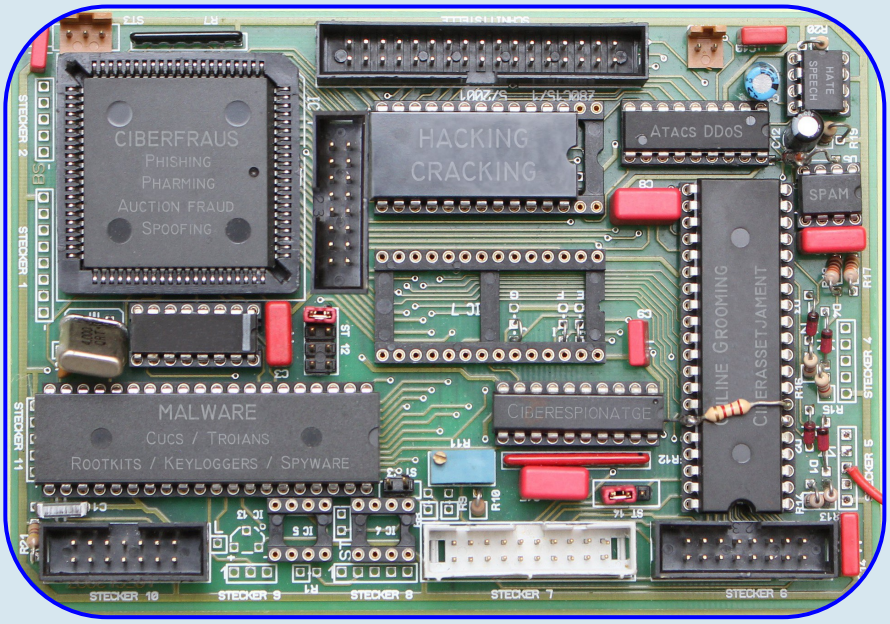
4 — 2022

AGS PUBLICATIONS

ISSN: 2696-1083

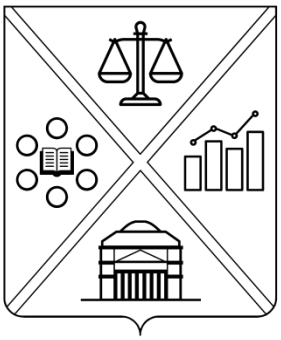
www.ags.cat



Taxonomia penal dels ciberdelictes

Anàlisi jurídic del crim digital

ARNAU GUIX SANTANDREU



AGS Publications / Arnau Guix Santandreu
No. 4 / Setembre 2022
ISSN: 2696-1083
Website: https://ags.cat

Cita recomanada:

GUIX SANTANDREU, Arnau (2022): "Taxonomia penal dels ciberdelictes. Anàlisi jurídic del crim digital". *AGS Publications*, No. 4, pp. 1-33. Accessible en línia a: www.ags.cat

La present publicació és fruit de l'adaptació parcial a la llengua catalana i ampliació del Treball de Fi de Màster en Dret Processal titulat "Las diligencias de investigación y la prueba electrónica del cibercrimen", elaborat pel mateix autor l'any 2022 a la Universidad de Salamanca.
El citat document és accessible a l'enllaç següent: http://hdl.handle.net/10366/150877

Taxonomia penal dels ciberdelictes

Anàlisi jurídic del crim digital

ARNAU GUIX SANTANDREU

RESUM / ABSTRACT

[*Català*] La digitalització a la nostra vida quotidiana és un fenomen innegable, de la mateixa manera que la irrupció dels ciberdelictes en aquesta pot arribar a suposar un impacte considerable sobre la nostra estabilitat financera i emocional. Cada dia, particulars, empreses i institucions són víctimes del cibercrim a tot el planeta, amb una tendència cada cop més a l'alça. La primera qüestió que convindria plantejar-nos és: *Què entenem per ciberdelicte?* A partir d'aquí, el present anàlisi descobreix les tipologies principals dels il·lícits penals digitals, identificant els preceptes del Codi Penal que hi són d'aplicació, com la doctrina jurídica els descriu i trobant exemples il·lustratius d'actualitat per arribar a definir-los de forma més completa. Finalment, el present estudi es complementa amb l'observança dels obstacles que impedirien una persecució òptima dels ciberdelictes des de la perspectiva del Dret Processal.

Paraules clau: ciberdelicte, cibercrim, pirateig informàtic, ciberfrau, ciberassetjament.

***

[*Castellano*] La digitalización en nuestra vida cotidiana es un fenómeno innegable, al igual que la irrupción de los ciberdelitos en ésta puede llegar a suponer un impacto considerable sobre nuestra estabilidad financiera y emocional. Todos los días, particulares, empresas e instituciones son víctimas del cibercrimen en todo el planeta, con una tendencia cada vez más al alza. La primera cuestión que convendría plantearnos es: *¿Qué entendemos por ciberdelito?* A partir de aquí, el presente análisis descubre las principales tipologías de los ilícitos penales digitales, identificando los preceptos del Código Penal que son de aplicación, como la doctrina jurídica los describe y encontrando ejemplos ilustrativos de actualidad para llegar a definirlos de forma más completa. Por último, el presente estudio se complementa con la observancia de los obstáculos que impedirían una persecución óptima de los ciberdelitos desde la perspectiva del Derecho Procesal.

Palabras clave: ciberdelito, cibercrimen, pirateo informático, ciberfraude, ciberacoso.

***

[*English*] Digitisation in our daily life is an undeniable phenomenon, in the same way that the emergence of cybercrimes in it can have a considerable impact on our financial and emotional stability. Every day, individuals, companies and institutions are victims of cybercrime all over the planet, with an ever-increasing trend. The first question we should ask ourselves is: *What do we mean by cybercrime?* From here, the present analysis discovers the main typologies of digital criminal offences, identifying the precepts of the Penal Code that can be applied, how the legal doctrine describes them and finding illustrative current examples to define them more completely. Finally, the present study is complemented by observing the obstacles that would prevent an optimal prosecution of cybercrimes from the perspective of the Procedural Law.

Keywords: cybercrime, hacking, cyberfraud, cyberharassment.

***

[*Français*] La numérisation dans notre quotidien est un phénomène indéniable, au même titre que l'émergence de la cybercriminalité dans celle-ci peut avoir un impact considérable sur notre stabilité financière et émotionnelle. Chaque jour, des particuliers, des entreprises et des institutions sont victimes de la cybercriminalité partout sur la planète, avec une tendance croissante sans cesse. La première question que nous devons nous poser est : *Qu'entend-on par cybercriminalité ?* À partir d'ici, la présente analyse découvre les principales typologies d'infractions pénales numériques, en identifiant les préceptes du Code Pénal pouvant être appliqués, comment la doctrine juridique les décrit et en trouvant des exemples illustratifs actuels pour les définir plus complètement. Enfin, la présente étude est complétée par l'observation des obstacles qui empêcheraient une poursuite optimale des cybercrimes du point de vue du Droit Procédural.

Mots-clés : cyberdélit, cybercriminalité, piratage informatique, cyberfraude, cyberharcèlement.

***

[*Italiano*] La digitalizzazione nella nostra vita quotidiana è un fenomeno innegabile, così come l'emergere di crimini informatici al suo interno può avere un impatto considerevole sulla nostra stabilità finanziaria ed emotiva. Ogni giorno, individui, aziende e istituzioni sono vittime della criminalità informatica in tutto il pianeta, con una tendenza in costante aumento. La prima domanda che dovremmo porci è: *Cosa intendiamo per criminalità informatica?* Da qui, la presente analisi scopre le principali tipologie di reato digitale, individuando i precetti del Codice Penale applicabili, come la dottrina giuridica li descrive e trovando esempi illustrativi attuali per definirli più completamente. Infine, il presente studio è completato dall'osservazione degli ostacoli che impedirebbero un perseguimento ottimale dei crimini informatici dalla prospettiva del Diritto Processuale.

Parole chiave: ciberreato, cibercrimine, pirataggio informatico, cibertruffa, cibermolestia.

***

[*Gascon/Occitan*] La digitalizacion ena nòsta vida vidanta ei un fenomèn innegable, de la madeisha manièra que l'arribada des ciberdelictes en aguesta pòt arribar a supausar un impacte considerable sus la nòsta estabilitat financèra e emocionau. Cada jorn, particulars, enterpresas e institucions son victimes deu cibercrime a tota la planeta, damb ua tendéncia cada viatge de mès nautada. La prumèra question que auríem de posar ei: *Qué comprenem per ciberdelicte?* A partir d'aquiu, lo presènt analisi descorbís les tipologies principaus des illicits penaus digitaus, en tot identificar los precèptes deu Code Penau que son d'aplicacion, coma la doctrina juridica ac descriu e en tot trapar exemples illustraires actuaus entà arténher a definir-los mès completament. Fin finau, lo present estudi ei complementat damb l'observacion des obstàcles que poderien empedir ua persecucion optimala sus los ciberdelictes segon la perspectiva deu Dret Processau.

Mots clau: ciberdelicte, cibercrime, piratatge informatic, ciberfrauda, ciberassautada.

ÍNDEX GENERAL

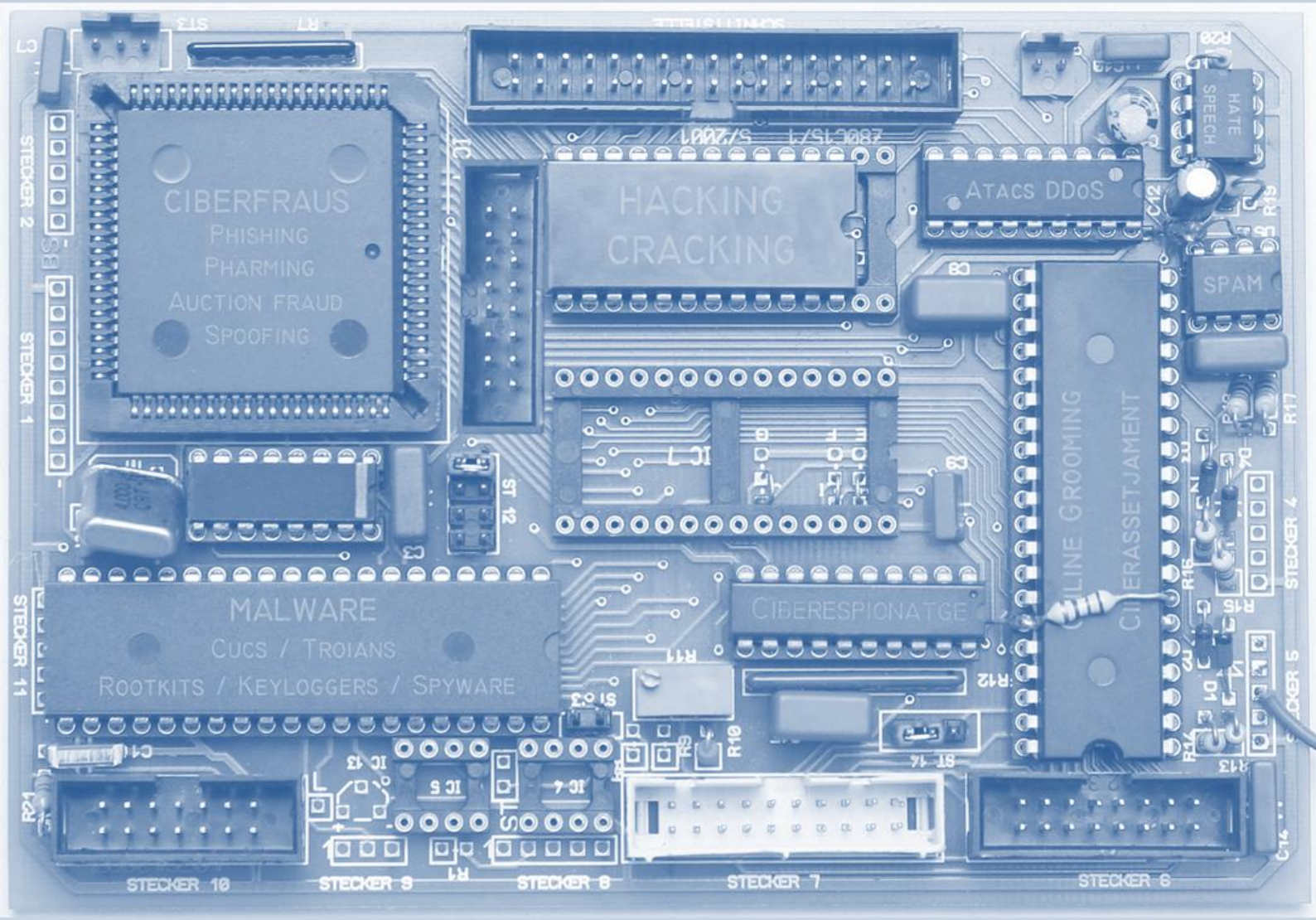
ABREVIATURES

Art.	Article
CE	Constitució Espanyola
CP	Codi Penal
CEDH	Conveni Europeu de Drets Humans
FGE	Fiscalia General de l'Estat
FJ	Fonament Jurídic
IA	Intel·ligència Artificial
LAJ	Lletrat de l'Administració de Justícia
LEC	Llei d'Enjudiciament Civil
LECRIM	Llei d'Enjudiciament Criminal
LO	Llei Orgànica
OTAN	Organització del Tractat de l'Atlàntic Nord
RD	Reial Decret
Rec.	Nombre de recurs
SAN	Sentència de l'Audiència Nacional
STC	Sentència del Tribunal Constitucional
STEDH	Sentència del Tribunal Europeu de Drets Humans
STS	Sentència del Tribunal Suprem
TICs	Tecnologies de la Informació i la Comunicació

Æquam memento rebus in arduis servare mentem.

(Recorda conservar la ment serena en els moments difícils)

QUINTUS HORATIUS FLACCUS,
Carmina, Liber II, III



Introducció

INTRODUCCIÓ

A) UN NOU ORDRE DIGITAL

Actualment, en els països desenvolupats la majoria de les interaccions humanes tenen lloc a l'entorn virtual. Més enllà de la revolució de les xarxes socials de l'última dècada, ja fa anys que treballem amb equips informàtics i les empreses utilitzen sistemes electrònics per a fer les seves transaccions diàries. Les compres en línia s'han democratitzat i de la mateixa manera l'accés a continguts d'entreteniment i actualitat és ampli. A aquest escenari d'oportunitats inèdit s'ha articulat un sector d'amenaces també mai vist, que aprofita les vulnerabilitats dels sistemes per a lucrar-se i causar estralls. Per tant, aquí rau la necessitat d'establir una regulació punitiva que resulti efectiva i no quedi obsoleta per la rapidesa en la qual avança la tecnologia. S'estima que l'any 2021 la cibercriminalitat tingué un impacte planetari de 5,7 bilions d'euros. El continent europeu va estar exposat a una cinquena part dels atacs[1]. A Espanya, s'estima que el 15,6% del total d'infraccions penals comeses al país l'any 2021 van ser ciberdelictes[2]. Un dels atacs més greus va ser el que afectà a la UNIVERSITAT AUTÒNOMA DE BARCELONA (UAB) el passat 11 d'octubre de 2021, en què un virus de tipus *ransomware* encriptà les dades de 10.000 ordinadors[3].

B) OBJECTIUS I ESTRUCTURA

La finalitat del present anàlisi radica en descobrir quins són els principals ciberdelictes i il·lustrar-ne una classificació pragmàtica, mostrant la regulació penal que es troba en vigor actualment a l'ordenament jurídic hispànic. Per aquest motiu, el nucli de l'estudi desenvolupa la mencionada classificació de forma exhaustiva. El treball quedaria incomplet si no es contemplessin els obstacles processals que existeixen per a una persecució efectiva dels ciberdelictes; d'aquesta manera, abans de concloure es presentaran de forma sintètica aquelles dificultats que obstrueixen una acció més efectiva de l'Estat de Dret.

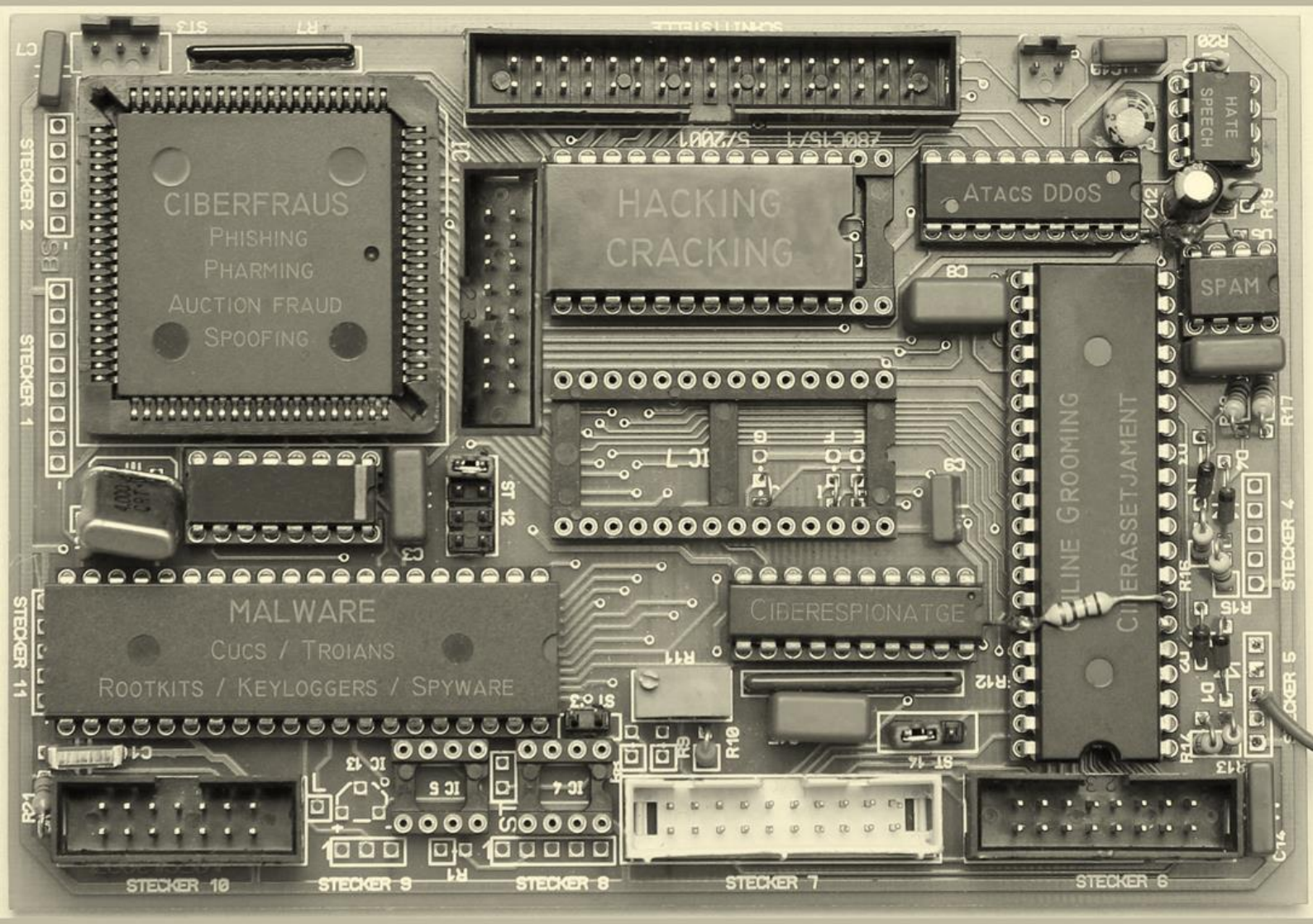
C) METODOLOGIA

La metodologia emprada es recolza en la revisió bibliogràfica i l'anàlisi crític de la literatura existent sobre el tema. Per aquest motiu, s'han consultat diverses fonts documentals primàries, entre la legislació espanyola (destacant el Codi Penal i la Llei d'Enjudiciament Criminal), la normativa dimanant d'organitzacions internacionals i les notícies de premsa relacionades. A nivell de fonts secundàries, s'han estudiat les monografies i publicacions científiques especialitzades en Dret sobre la temàtica en qüestió, establint una major prioritat pels continguts més recents, dins de l'última dècada a causa de l'entorn jurídic i tecnològic més variable.

[1] FRANCE 24 (10.05.2022): *La cibercriminalidad costó más de 6 billones de dólares en 2021*. Accessible a: https://www.france24.com/es/minuto-a-minuto/20220510-la-cibercriminalidad-cost%C3%B3-m%C3%A1s-de-6-billones-de-d%C3%B3lares-en-2021 [Última consulta realitzada el 25.08.2022].

[2] GOBIERNO DE ESPAÑA. MINISTERIO DEL INTERIOR (2022): *Informe sobre la cibercriminalidad en España 2021*. Madrid, Secretaría de Estado de Seguridad, Dirección General de Coordinación y Estudios, p. 23.

[3] LA VANGUARDIA (23.11.2021): *El Govern destina 3,5 millones a la UAB para recuperarse del ciberataque*. Accesible a: https://www.lavanguardia.com/vida/20211123/7883348/govern-destina-3-5-millones-uab-recuperarse-ataque-informatico.html [Última consulta realitzada el 25.08.2022].



La classificació dels ciberdelictes i els seus obstacles processals

LA CLASSIFICACIÓ DELS CIBERDELICTES

1. MARC GENERAL DE LA CLASSIFICACIÓ

La doctrina ha fet diverses aproximacions per tal de sistematitzar la cibercriminalitat de forma recent. En efecte, el Dret penal i processal penal clàssic, juntament amb els principis de garantia dels Drets Fonamentals, s'han construït sobre un model de criminalitat física, de tipus marginal i en què l'infractor és un o pocs individus. Sense cap dubte, la revolució digital de la segona meitat del segle XX fins ara ha suposat un canvi de paradigma[4]. Així, la doctrina es va referir primer als *delictes informàtics* i posteriorment, com una evolució o segona generació dels mateixos, als *ciberdelictes* o *delictes 2.0*, com a comportaments desviats, realitzats a través dels sistemes informàtics i que tenen una repercussió social nociva; estan completament determinats per l'ús de la xarxa i l'existència de les TIC[5].

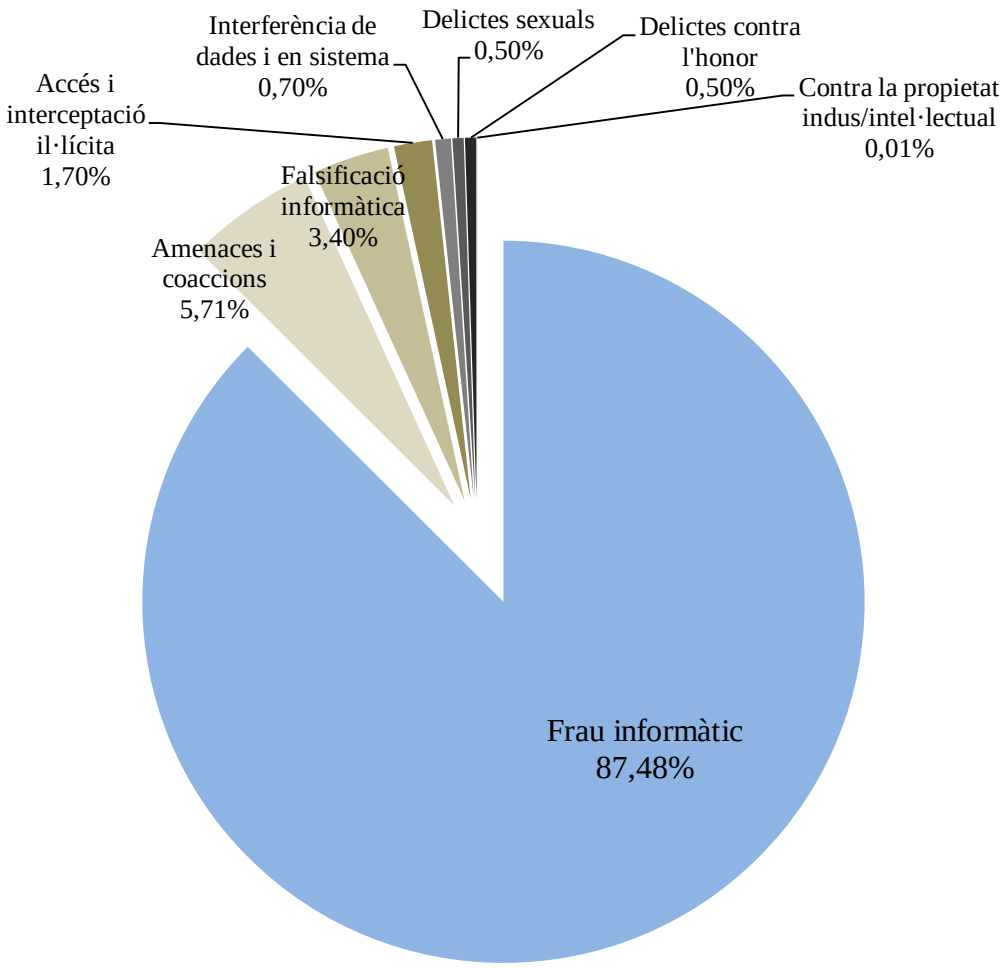
El concepte de *Dret penal informàtic* podria arribar a induir a una perspectiva errònia, de pensar fins i tot que estem davant d'un sector de tal branca de l'ordenament jurídic que agrupa certs tipus penals que tenen elements tècnics configuradors comuns que obliguen a fer una distinció respecte d'altres figures del Codi Penal. Segons GALÁN MUÑOZ, no existeix un bé jurídic comú, per exemple, la seguretat dels sistemes informàtics, que obligui a realitzar aquesta separació[6], fet que és refutat per BARRIO ANDRÉS, que qualifica la seguretat a la Societat de la Informació de *bé jurídic de primer ordre*, però no es posiciona a favor de seccionar el Dret penal[7]. No es pot prescindir del pes real dels ciberdelictes, ja que amb ells es poden consumar una llarga llista de tipus penals, des de delictes contra els consumidors, homicidis[8] i fins i tot supòsits de terrorisme.

És fonamental comprendre el paper que tenen les TIC per a la consecució del delicte. Així, inicialment la posició era considerar la distinció en què els sistemes informàtics eren o bé un instrument per a perpetrar el delicte (*computer assisted crimes*) o bé l'objectiu del ciberatac (*computer focused crimes*). Actualment aquesta classificació ha estat superada: moltes vegades les tecnologies ja són simultàniament l'eina (*tool*) i l'objectiu (*target*) de l'il·lícit penal i hauríem de cenyir-nos únicament a aquests supòsits múltiples per arribar a definir el cibercrim satisfactòriament.

Actualment, el Sistema Estadístic de Criminalitat, integrat en el MINISTERI DE L'INTERIOR, classifica els ciberdelictes a través de la tipologia següent*: accés i interceptació il·lícita, amenaces i coaccions, delictes contra l'honor, delictes contra la propietat industrial i intel·lectual, delictes sexuals* (amb exclusions), *falsificació informàtica, frau informàtic, i interferència de dades i en sistema*. L'any 2021, la categoria delictiva que tingué un impacte major va ser la dels fraus informàtics, amb 267.011 fets coneguts, representant un 87,4% del total (305.477 fets delictius registrats). Aquesta proporció dominant s'ha mantingut al llarg del temps[9].

[4] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*. Las Rozas (Madrid), Wolters Kluwer, p. 29.
[5] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op.* cit.), pp. 35-36.
[6] GALÁN MUÑOZ, Alfonso (2019): *Los ciberdelitos en el ordenamiento español*. Barcelona, Editorial UOC, p. 16.
[7] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op.* cit.), p. 92.
[8] Pensem per aquest supòsit, per exemple, el *pirateig* d'un vehicle amb sistemes de conducció autònoms.
[9] GOBIERNO DE ESPAÑA. MINISTERIO DEL INTERIOR (2022): *Informe sobre la cibercriminalidad (...) (op. cit.*), p. 43.

El present gràfic mostra les categories delictives del cibercrim segons el MINISTERI DE L'INTERIOR, tenint en compte la proporció de fets coneguts respectius durant l'any 2021[10]:



A efectes d'anàlisi, BARRIO ANDRÉS ha representat els ciberdelictes a partir de la proposta següent, seguint la ubicació dels preceptes al Codi Penal[11]:

Ciberdelicte	***Article del CP***
Descobriment i revelació de secrets	197
Intrusisme informàtic i intercepció de les comunicacions (*hacking*)	197 bis
Utilització no autoritzada d'imatges prèviament obtingudes amb consentiment (*revenge pornography*)	197.7
Danys informàtics i sabotatges (*cracking*)	264 i ss.
Establiment d'obstacles o interrupció d'un sistema informàtic	264 bis
Estafes	248
Abús de sistemes informàtics (*phreaking*)	256
Calúmnies	205
Injúries	208
Ciberassetjament (*cyberstalking*)	172 ter
Pornografia infantil	187 i ss.
Apropament y entabanament a menors (*online grooming*)	183 ter
Delictes contra la propietat intel·lectual	270 i ss.
Ciberterrorisme	571 i ss.

[10] GOBIERNO DE ESPAÑA. MINISTERIO DEL INTERIOR (2022): *Informe sobre la cibercriminalidad (...) (op. cit.*), p. 43.
[11] Taula adaptada de BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. (...) (op.* cit.), pp. 71-72.

En canvi, MIRÓ LLINARES ha optat per il·lustrar la següent classificació pràctica dels ciberdelictes, de forma entrecreuada, que és la que serà estudiada amb major deteniment[12]:

	Ciberatacs purs	***Ciberatacs rèplica***	***Ciberatacs de contingut***
Cibercrims econòmics	• *Hacking* • *Malware* intrusiu • *Malware* destructiu • Ataques de *insiders* • Ataques DoS • *Spam* • Ciberocupació xarxa • *Antisocial networks*	• Ciberfraus(*phishing, pharming, scam, auction fraud*, etc.) • *Cyberspyware* • *Identity theft* • *Spoofing* de ARP, DNS, IP y web • Ciberblanqueig de capitals • Ciberextorsió • Ciberocupació	• Distribució de pornografia infantil a Internet • Ciberpirateria intel·lectual
Cibercrims socials	-	• *Spoofing* • *Cyberstalking* • *Cyberbullying* • *Online harassment* • *Sexting* • *Online grooming*	-
Cibercrims polítics	• Ataques DoS (*cyberwar*) • Ataques DoS (*cyberhacktivism*) • *Malware* intrusiu	• Ciberespionatge terrorista • Ciberguerra	• *Online hate speech* • Ciberterrorisme (difusió de missatges radicals amb fins terroristes)

En alguns supòsits, el ciberespai és l'únic escenari viable per perpetrar la infracció, i es produeixen crims que mai abans s'haguessin pogut fer: són els anomenats *ciberatacs purs*. En altres casos, no s'han generat il·lícits nous, sinó que s'han reproduït les característiques bàsiques de tipus penals ja existents a les nostres societats a l'entorn de la xarxa: es tracta dels *ciberatacs rèplica*. Per concloure, el ciberespai s'ha convertit en un àmbit privilegiat per a la difusió en massa de continguts, i ha amplificat significativament el dany d'aquests il·lícits cap a una esfera global: són els anomenats *ciberatacs de contingut*.

El primer tipus de ciberatacs planteja problemes per incriminar els presumptes criminals i concloure un procés penal amb èxit. La segona categoria també presenta característiques de ràpida evolució i no està exempta de dificultats per aplicar els preceptes penals vigents. I la tercera categoria presenta obstacles a la prevenció, amb riscos d'afectar Drets Fonamentals exercits lliurement, i naturalment en l'atribució de les responsabilitats penals als autors.

Així mateix, com es pot apreciar a la taula anterior, el cibercrim pot ser analitzat des d'una altra perspectiva creuada, diferenciant entre els ciberatacs *econòmics*, *socials* i *polítics*, segons el seu particular àmbit d'incidència. És una classificació més pragmàtica, procedent dels tres grans àmbits funcionals d'utilització de les tecnologies de la informació i la comunicació. Especialment, els dos primers entorns són més clars: el ciberespai es visualitza en una àrea de desenvolupament econòmic i també d'expansió de relacions socials i el contacte interpersonal

[12] Taula adaptada de MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid, Marcial Pons, p. 50.

entre individus[13]. Seguidament analitzarem separadament aquestes tres categories de ciberatacs, descobrint-ne els seus subgrups principals.

2. CIBERDELICTES ECONÒMICS I PATRIMONIALS

Els *ciberatacs econòmics* tenen la raó de ser en la voluntat de l'autor d'obtenir beneficis patrimonials, ja siguin directes o indirectes a partir de les conductes delictives a la xarxa. És indubtable que aquesta és la principal categoria de ciberatacs pel seu impacte diari als països desenvolupats i les seves implicacions contra les pràctiques mercantils. La digitalització ha suposat que diners, dades de valor elevat i nous serveis s'ofereixen mitjançant les xarxes. Aquest fet exposa empreses i particulars, aquests darrers entesos més aviat com a clients o consumidors, al cibercrim de tipus econòmic i patrimonial, en què els atacants pretenen lucrar-se de les activitats legítimes d'altres subjectes. En la majoria de supòsits, els cibercriminals encadenaran diferents atacs per aconseguir el seu propòsit últim. Els *cibercrims econòmics purs* troben en el *hacking* i l'ús de *malware* o codi maliciós els seus principals supòsits.

2.1. *Hacking* i *Cracking*, una distinció no contemplada per la llei

El *hacking* o *pirateig* és una conducta per la qual un atacant accedeix a un sistema informàtic sense autorització del seu titular. Amb aquesta posició privilegiada, està en condicions d'utilitzar-lo o aprofitar les dades que s'hi troben contingudes. Es pot diferenciar entre el *white hat hacking*, és a dir, el *hacking blanc*, que no té un propòsit de sabotejar o utilitzar la informació més tard, únicament entrar al sistema informàtic, i el *black hat hacking*, en altres paraules, el *cracking*, en el qual el *cracker* busca malmetre el sistema, causar un perjudici al titular, o apropiar-se, modificar o eliminar les dades contingudes en aquest[14]. El *hacking blanc* ha estat qualificat de *hacking ètic*. La demanda d'especialistes i les seves recompenses van en augment[15].

És important tenir present que en certes ocasions els *hackers* informen de les vulnerabilitats que han detectat als titulars mateixos dels equips informàtics, de manera que s'aconsegueix avançar en la millora dels estàndards de seguretat; no obstant això, la conducta sancionada com a il·lícit penal a l'article 197 bis CP[16] i sota el qualificatiu de ciberatac es basa en el simple accés[17]; aquí no preval la distinció entre *hackers* i *crackers*[18]. El precepte és fruit de la reforma del 2015 i preveu a l'article 197 ter la sanció per a actes preparatoris destinats a la comissió dels delictes de l'article 197 bis[19].

[13] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (...) (op. cit.)*, pp. 116-118.
[14] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (...) (op. cit.)*, pp. 53-54.
[15] LA VANGUARDIA (15.08.2022): *¿Quieres ser hacker ético? Los ciberataques disparan la demanda de sombreros blancos*. Accessible a: https://www.lavanguardia.com/vida/formacion/20220815/8466693/hacker-etico-ciberataques.html [Última consulta realitzada el 25.08.2022].
[16] *Vid.* STS 494/2020, de 8 de octubre, rec. 10018/2020, FJ 6, en què s'aplica el precepte citat al supòsit d'un accés no autoritzat a una base de dades d'antecedents policials.
[17] Així, l'article 197 bis del Codi Penal condemna a qui *por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información, o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo*.
[18] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (...) (op. cit.)*, pp. 55-56.
[19] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op.* cit.), pp. 90-91.

2.2. Les múltiples cares del *malware*

Un altre dels instruments del *cibercrim econòmic pur* és l'anomenat *malware*, és a dir, un programa maliciós que té com a objectiu malmetre, controlar o modificar un sistema informàtic[20]. Hi ha dins d'aquesta àmplia categoria de *software* un ampli ventall de tècniques, des dels clàssics virus, que pretenen destruir el sistema o la informació emmagatzemada en ell, als *worms* (cucs; saturen els ordinadors i xarxes mitjançant la seva replicació constant i consumeixen la capacitat de processament), els *trojans* (troians, infecten els sistemes sota una aparença benèvola i proporcionen un accés remot als atacants), els *rootkits* (s'introdueixen al nucli del sistema informàtic per evitar ser detectats i permeten a l'agressor prendre el control de la màquina), els *keyloggers* (capturen les pulsacions realitzades al teclat i envien les dades a l'atacant) i el *spyware* (programa espia; transfereix dades de l'operativa del sistema capturat[21]).

Amb les capacitats del codi maliciós és possible que l'autor exigeixi a la víctima un rescat per tal de tornar a restablir el sistema informàtic al seu estat original, o que s'acontenti a destruir les dades o pertorbar el funcionament dels equips, provocant pèrdues quantioses en el cas de les empreses i administracions afectades. El *malware* és normalment l'avantsala del *hacking*, on els experts cibercriminals disposaran d'elements de control dels terminals infectats per expandir-ne l'atac i multiplicar-ne el seu poder devastador. En altres casos, existeixen els anomenats *insiders*, és a dir, treballadors o persones vinculades que sabotegen els sistemes de les seves pròpies organitzacions aprofitant la seva posició privilegiada a l'interior[22].

Dins dels *cibercrims econòmics purs* és important esmentar els atacs *DoS* (de l'anglès *denial of service*, denegació de servei), que provoquen una saturació del servidor del sistema de la víctima i impedeixen que pugui atendre altres peticions que no siguin les del propi agressor. Aquest fet pot arribar a incapacitar llocs web comercials amb un alt nombre de visites, perjudicant les activitats de les empreses i institucions que representen i malmetent la seva reputació. És més, hi ha una evolució encara més invasiva dels atacs *DoS*, els *DDoS* (*distributed denial of service*, denegació de servei distribuïda).

Els atacs *DDos* realitzen una saturació del servidor mitjançant peticions procedents de múltiples atacants alhora o xarxes de bots que actuen de forma coordinada, fins i tot treballant des de diversos terminals infectats. En aquests casos és més difícil distingir els visitants il·lícits dels lícits. Davant d'aquests danys, s'ha arribat a articular un veritable mercat del ciberdelicte[23], en què es lloguen *botnets* a ciberdelinqüents per un preu reduït de 60 dòlars al dia, que poden causar estralls a una sola empresa per la quantiosa xifra de 580.000 euros[24].

[20] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (…) (op. cit.)*, p. 59.
[21] Sobre el programari espia, també es podria inserir a dins de la categoria dels *cibercrims econòmics rèplica*, ja que l'espionatge naturalment també és una pràctica anterior a l'existència del mateix ciberespai.
[22] És el cas de Hervé Falciani, la *llista* del qual va ser validada com a prova per part del Tribunal Suprem l'any 2017. *Vid.* CONSEJO GENERAL DEL PODER JUDICIAL (24.02.2017): *El Tribunal Supremo avala la 'lista Falciani' como prueba de cargo del delito fiscal*. Accessible a: https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Tribunal-Supremo/Noticias-Judiciales/El-Tribunal-Supremo-avala-la--lista-Falciani--como-prueba-de-cargo-del-delito-fiscal [Última consulta realitzada el 25.08.2022].
[23] En altres termes, el *ciberdelicte com a servei* (CaaS – *cybercrime as a service*, en anglès).
[24] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (…) (op.* cit.), p. 37.

El Codi Penal espanyol ha tipificat a l'article 264 CP un tipus bàsic per punir els danys derivats de la interferència il·legal en dades informàtiques[25] una conducta assimilable a la introducció de codi maliciós o la realització d'atacs *DoS*. L'articulat pretén respondre a les especificacions de l'article 5 de la Directiva 2013/40/UE, del Parlament europeu i el Consell, de 12 d'agost de 2013, relativa als atacs contra els sistemes d'informació (DAI), encara que en aquesta no s'especifica la necessitat de cobrir supòsits greus en la definició del delicte, de manera que el legislador hispànic ha optat per crear un concepte jurídic indeterminat que s'haurà d'actualitzar a través de la praxi dels òrgans jurisdiccionals[26]. No obstant això, hi ha poques resolucions condemnatòries als repertoris de jurisprudència que permetin delimitar la gravetat dels atacs amb caràcter general[27].

2.3. Els ciberfraus i la ciberextorsió

Els *cibercrims econòmics rèplica* tenen als ciberfraus la seva major representativitat. Aquests es caracteritzen perquè els autors del delicte aconsegueixin un lucre a partir d'un perjudici patrimonial de la víctima. Van centrar l'atenció del legislador fins i tot abans que aquest comprengués la necessitat de castigar els danys informàtics i els accessos il·legítims als sistemes, donada la tendència expansiva de tractament automatitzat de dades bancàries en Administracions Públiques i grans corporacions als anys setanta i vuitanta als països tecnològicament més avançats[28]. Aproximadament dos terços dels ciberdelictes que es produeixen a tot el món estan quantificats sota la categoria dels fraus informàtics, una xifra elevada que s'ha mantingut relativament estable al llarg de la darrera dècada[29].

Per arribar a cometre'ls s'han dissenyat infinitat de tècniques que s'han perfeccionat al llarg del temps, coincidint amb les millores en seguretat i divulgació pública de les pràctiques d'estafa: fraus de xecs i targetes de crèdit, estafes d'inversió amb productes financers falsos, *ponzi frauds* o estafes piramidals, enganys amb falsos premis o presumptes loteries, *auction frauds* a les subhastes en línia en què no es lliura el producte o s'enganya sobre les seves propietats, els *scam* o ciberfraus rudes com les anomenades *cartes nigerianes*, etc.[30]. Actualment, l'article 248.2 a) del Codi Penal comprèn el tipus penal bàsic de l'anomenada *estafa informàtica*.

El cas paradigmàtic després de la irrupció de la banca electrònica i les aplicacions financeres és l'anomenat *phishing*[31], una tècnica de suplantació d'identitat d'una entitat bancària o una empresa per extreure posteriorment les dades personals dels clients i lucrar-se amb operacions fraudulentes, fonamentalment a mitjançant missatges de correu electrònic enganyosos que redireccionen els usuaris a llocs web falsos. Un exemple recent s'ha produït el febrer del 2022,

[25] Tal precepte estableix que *El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años.*

[26] GALÁN MUÑOZ, Alfonso (2019): *Los ciberdelitos en el ordenamiento español (...) (op. cit.)*, p. 172.

[27] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op.* cit.), p. 113.

[28] GALÁN MUÑOZ, Alfonso (2019): *Los ciberdelitos en el ordenamiento español (...) (op. cit.)*, p. 139.

[29] PONS GAMÓN, Vicente (2017): "Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad". Quito, *URVIO - Revista Latinoamericana de Estudios de Seguridad*, nº 20, p. 84.

[30] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (...) (op. cit.)*, pp. 69-71.

[31] Es tracta d'un terme procedent de l'anglès *fishing*, pesca, per a referir-se metafòricament a les víctimes com si fossin els peixos que *mosseguen a l'ham*. A l'argot informàtic resulta habitual trobar termes que comencen amb l'arrel *ph*, com per exemple un altre tipus de ciberfrau, el *pharming*.

quan l'Ajuntament de Barcelona ha fet un pagament de vora 350.000 euros a uns estafadors que havien suplantat la identitat d'una empresa de sistemes informàtics amb un certificat fals de canvi de número de compte[32]. Així, s'utilitza l'enginyeria social per aparentar la identitat d'una organització aliena (*spoofing*), alhora que es pot arribar a fer un seguiment exhaustiu del comportament de la víctima a través del lloc web veritable (*pharming*)[33]. A més, si la incursió cap als sistemes es realitza per missatge de SMS en lloc de correu electrònic, per exemple, rebent un enllaç que en obrir-lo infecta el dispositiu, rep el nom de *smishing*[34].

Els diners robats es transferiran als comptes de *mulers*[35], que retindran un percentatge i reenviaran els fons a altres comptes bancaris, molts d'ells situats a l'estranger per dificultar la traçabilitat de les operacions[36]. Altres vegades, l'objectiu dels atacants no són els perfils del consumidor típic sinó els directius de grans corporacions o Administracions Públiques, per arribar a obtenir les seves credencials (*whaling*, caça de balenes)[37].

Tot i que els atacants de *phishing* ja fa anys que intenten trobar mètodes òptims per aprofitar-se de les distraccions de les seves víctimes sense poder ser perseguits, hi ha alguns indicis generalitzats que permeten detectar-los. Entre aquests indicis es troben: utilitzar adreces de correu electrònic no oficials, realitzar una salutació no personalitzada, sol·licitar dades de l'usuari que el remitent veritable no demanaria perquè ja li consten, requerir fer gestions amb urgència, proferir amenaces de desactivació de comptes, contenir faltes d'ortografia i fins i tot adjuntar fitxers amb codi maliciós perquè els sistemes informàtics s'infectin en executar-los[38]. Fins i tot s'arriben a aprofitar d'emocions humanes com l'afany de lucre (regals, ofertes i premis) o la compassió envers les persones vulnerables (peticions de fons davant de guerres, crisis o calamitats naturals).

A la mateixa categoria de *cibercrims econòmics rèplica* també trobaríem a la ciberextorsió. Algunes organitzacions criminals amenacen les víctimes de fer atacs informàtics i exigeixen el pagament de sumes importants de diners per no arribar a executar-los. Algunes cases d'apostes i jocs d'atzar en línia han cedit aquestes pressions perquè els seus sistemes no fossin paralitzats i perdessin el seu potencial recaptatori, especialment durant dates assenyalades[39].

[32] EL PERIÓDICO (27.05.2022): *'Hackers' estafen 350.000 euros a l'Institut d'Informàtica de Barcelona*. Accessible a: https://www.elperiodico.cat/ca/barcelona/20220527/hackers-institut-informatica-barcelona-estafa-phising-13717094 [Última consulta realitzada el 25.08.2022].
[33] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (...) (op. cit.)*, p. 72.
[34] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op.* cit.), p. 128.
[35] Els anomenats *muleros* (en castellà) també participen del ciberblanqueig de capitals. Normalment seran captats a través de les seccions d'ocupació de portals d'anuncis classificats, sota denominacions aparentment innòcues com *treballar* o bé *guanyar diners des de casa*.
[36] LA GACETA DE SALAMANCA (24.05.2022): *Alerta por nuevos casos de estafas bancarias a través del correo electrónico*. Accessible a: https://www.lagacetadesalamanca.es/virales/alerta-por-nuevos-casos-de-estafas-bancarias-a-traves-del-correo-electronico-EE11262262 [Última consulta realitzada el 25.08.2022].
[37] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (...) (op. cit.)*, pp. 76-77.
[38] EL PERIÓDICO (23.05.2022): *Phishing: ¿Qué es y cómo evitarlo?* Accessible a: https://www.elperiodico.com/es/tecnologia/20220523/phishing-que-es-dv-13695404 [Última consulta realitzada el 25.08.2022].
[39] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (...) (op. cit.)*, pp. 83-84.

2.4. La distribució de pornografia infantil

Finalment, hi ha *cibercrims econòmics de contingut*, en els quals podem identificar la distribució de pornografia infantil a Internet i els ciberdelictes relatius a la propietat intel·lectual. Pel que fa a la primera, en primer lloc resulta difícil fer una definició socialment acceptada d'aquest fenomen[40]. La pornografia infantil es recull a l'ordenament espanyol a l'article 189 CP.

La pornografia infantil no té un origen purament cibernètic, encara que l'ús s'ha multiplicat exponencialment a partir de la irrupció de les noves tecnologies. Inicialment, la divulgació d'aquests continguts a Internet es feia a llocs web accessibles pel públic i indexats en motors de cerca, fet que va provocar la seva ràpida detecció per les autoritats i el bloqueig en el seu ús. Més tard, es va traslladar a fòrums de menor exposició pública, en què els pedòfils xatejaven per intercanviar-se els arxius, i en plataformes de descàrrega, en què el traspàs de dades resulta immediat[41]. El fet que hi hagués agents encoberts fent un seguiment d'aquestes activitats il·lícites va motivar la translació cap a comptes de correu electrònic compartits, la deslocalització de diferents fases de la producció de continguts a diferents països[42] i l'ús de l'anomenada *dark web*, on no és possible rastrejar als cibercriminals. La Comissió Europea va iniciar el 2020 un pla per combatre aquests delictes, que els ha qualificat d'abusos sexuals a través de la xarxa[43].

2.5. La pirateria contra la propietat intel·lectual

En una altra esfera dels *cibercrims econòmics de contingut*, la ciberpirateria intel·lectual ha afectat sens dubte els creadors de continguts, ja sigui dins de la indústria musical o l'editorial. El valor estimat del lucre cessant és considerable i des de les administracions públiques dels països occidentals s'ha procurat limitar les activitats de portals de descàrregues[44] i de visualització de vídeos en *streaming*, i alhora incentivar els ciutadans perquè adquireixin els productes únicament en negocis legítims.

A Espanya, l'article 270.1 del Codi Penal comprèn el tipus bàsic de delicte contra la propietat intel·lectual, en què és un requisit fonamental de l'injust que aquest es cometi *amb ànim d'obtenir un benefici econòmic directe o indirecte i en perjudici de tercer*, a la vegada que el precepte atorga protecció envers les obres o prestacions literàries, artístiques o científiques, o la seva transformació, interpretació o execució artística. D'aquesta manera, com a requisits de les obres, cal matisar que en primer lloc, les creacions han de ser innovacions o manifestació de l'enginy o la creativitat humana; en segon lloc, les creacions han de ser originals, és a dir, que es

[40] Segons la Decisió Marc 2004/68/JAI, de 22 de desembre de 2003, del Consell (ara derogada), que va ser pionera en el Dret comunitari, s'entén per pornografia infantil qualsevol material pornogràfic que descrigui o representi de manera visual: *un nen real practicant o participant en una conducta sexualment explícita, inclosa l'exhibició lasciva dels genitals o de la zona púbica d'un nen, (...) a una persona real que sembli ser un nen practicant o participant en la conducta mencionada (...) o (...) imatges realistes d'un nen inexistent practicant o participant en la conducta mencionada (...)* (art. 1). La legislació que va substituir a la citada Decisió Marc va ser la Directiva 2011/92/UE, de 13 de desembre de 2011, del Parlament Europeu i del Consell, que a l'article 2 manté la definició mostrada.

[41] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (...) (op. cit.)*, pp. 109-110.

[42] Seria el cas, per exemple, de filmacions de menors d'edat realitzades a les Filipines, enviades posteriorment a la xarxa des de Tailàndia i allotjades a un servidor d'un país situat a l'Àfrica Occidental, permetent-ne un accés global.

[43] COMISSIÓ EUROPEA (2020): *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones*. *Estrategia de la UE para una lucha más eficaz contra el abuso sexual de menores*. Brussel·les, COM(2020) 607 final.

[44] Com el cas del portal *Megaupload*, que va ser clausurat per la FBI l'any 2012.

puguin diferenciar d'altres creacions o produccions anteriors; i en tercer lloc, aquesta creació o producte s'ha de poder qualificar d'artístic, literari o científic[45].

3. CIBERDELICTES SOCIALS

Els *cibercrims socials* tenen el seu punt de partida en la translació a Internet dels vincles i tractes socials existents a la vida real. Concretament, es reflecteixen en els crims ja tipificats que sorgeixen de les relacions i els conflictes entre les persones. La pandèmia de coronavirus, que va afectar amb força els països occidentals a partir del març del 2020, va suposar un abans i un després en l'ús de les TICs per evitar les trobades presencials, ja fos des d'una perspectiva laboral (teletreball), com d'una òptica d'amistat i afectiva, incrementant la incidència dels *cibercrims socials*. Els *millennials* o nadius digitals, que usen els dispositius electrònics per a gran part de les activitats diàries, són la generació amb una exposició més elevada per patir les repercussions d'aquesta categoria de ciberdelictes i a la vegada són els que tenen menys propensió a denunciar haver estat víctimes del cibercrim en general[46].

3.1. L'assetjament en línia i les seves variants

Com és ben sabut, les persones es poden assetjar a través de mitjans digitals. El ciberespai ofereix la possibilitat d'efectuar, a milers de quilòmetres de distància, injúries, calúmnies, amenaces, coaccions i altres agressions a un cost mínim, propulsades fàcilment a través de les xarxes socials. En aquests casos, hi concorren dos elements bàsics: que l'autor del delicte atempti contra la dignitat o la llibertat de la víctima i que aquestes accions tinguin lloc a través de les TICs[47]. El ciberassetjament es pot diferenciar entre el *cyberstalking* (fustigació, persecució o amenaces digitals, és a dir, una successió d'actes de l'anomenat *online harassment*), el ciberassetjament sexual (qualificant-lo d'atemptat a la llibertat sexual d'una altra persona) i el *cyberbullying* (és a dir, el ciberassetjament escolar o entre menors, en què per definició no intervenen adults).

L'article 172 ter del Codi Penal ha previst al tipus bàsic de *stalking* o assetjament el supòsit en què l'agressor estableixi o intenti establir contacte amb la víctima *a través de qualsevol mitjà de comunicació, o per mitjà de terceres persones*[48]. En canvi, l'assetjament laboral o *mobbing* està cobert de forma generalista a l'article 173.1 CP, sense una especificació per als ciberdelictes. Més silenciat, el *bullying* no disposa d'una tipificació particular i la jurisprudència s'ha hagut de remetre al precepte esmentat[49], entre d'altres. Això no obstant, la creació d'un tipus penal

[45] Fins a la data actual, la tendència ha estat que els creadors de continguts s'han dirigit cap a una selecta llista de plataformes considerades vàlides per a difondre els seus continguts i obtenir així una remuneració en base al nombre de visites o reproduccions, com el cas dels serveis de YOUTUBE o de SPOTIFY. L'ús d'aquests gegants com a intermediaris acaba derivant en una uniformització global de les preferències culturals.

[46] ESCUDO DIGITAL (05.11.2021): *Los centennials y millennials son los menos proclives a denunciar un ciberdelito*. Accessible a: https://www.escudodigital.com/ciberseguridad/centennials-millennials-no-denuncia-ciberdelito_50099_102.html [Última consulta realitzada el 25.08.2022].

[47] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (...) (op. cit.)*, pp. 84-85.

[48] També si l'agressor *adquirís productes o mercaderies, o contractés serveis, o fes que terceres persones es posin en contacte amb ella* mitjançant l'ús indegut de les seves dades personals, una possibilitat amplificada per l'ús de les TICs. Així, el *cyberstalking* es basa en dues característiques principals.

[49] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op.* cit.), p. 143.

específic no necessàriament milloraria la resposta penal a aquestes agressions, ja que hi ha béns jurídics diferents de protegir; per exemple, l'honor, la llibertat, la intimitat i la integritat moral[50].

3.2. Del *sexting* a la *revenge pornography*

Un dels comportaments que més s'ha expandit en el context pandèmic és l'anomenat *sexting*, una pràctica que consisteix en la captació pròpia i l'enviament d'imatges de contingut eròtic o sexual a altres persones, juntament amb textos suggeridors[51]. Algunes anàlisis distingeixen entre *sexting actiu* (la realització de fotos o vídeos propis) i el *sexting passiu* (la recepció de fotos o vídeos d'una altra persona)[52]. Evidentment, hi ha un risc elevat que les imatges o vídeos siguin difoses a tercers fins al punt que la reputació personal sigui malmesa de manera incontrolable i irreversible.

És per això que el Codi Penal ha contemplat un tipus qualificat a l'article 197.7 CP, després de l'explosió d'un cas mediàtic relacionat amb la filtració pública d'un vídeo íntim d'una regidora d'un municipi situat a la província de Toledo[53] i la necessitat d'incorporar el contingut de la Directiva 2013/40/UE (DAI) a la reforma del 2015[54]. El legislador també ha volgut fer front al fenomen de la *revenge pornography* o pornografia venjativa, en què el cònjuge o persones relacionades per anàloga relació d'afectivitat perjudiquen a la intimitat de l'altra persona, agreujant la pena a la meitat superior per a aquests supòsits[55].

Segons un estudi realitzat per un conegut portal de contactes íntims a Espanya, el 59% dels usuaris enquestats han declarat que un any després del confinament total se sentien més inclinats a fer *sexting*, majoritàriament cap a persones desconegudes[56] [57]. Evidentment, no són fenòmens exclusius del context ibèric. Sobre l'ús no autoritzat d'imatges íntimes d'altres persones, la LAW COMMISSION del Regne Unit ha publicat el juliol de 2022 un informe en el qual proposa la penalització de l'anomenat *downblousing*[58], que consisteix en la captura i difusió d'imatges dels pits de les dones, normalment des d'un angle vertical. Així, el legislador britànic vol recuperar la política criminal anteriorment realitzada contra l'*upskirting*[59].

[50] MIRÓ LLINARES, Fernando (2013): "Derecho penal, «cyberbullying» y otras formas de acoso (no sexual) en el ciberespacio". Barcelona, *Revista de Internet, Derecho y Política*, nº 16, p. 65.
[51] D'aquí prové l'origen del terme: es tracta d'un anglicisme procedent de fusionar els mots *sex* i *texting*.
[52] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (...) (op. cit.)*, p. 93.
[53] GALÁN MUÑOZ, Alfonso (2019): *Los ciberdelitos en el ordenamiento español (...) (op. cit.)*, p. 101.
[54] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op.* cit.), p. 98.
[55] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op.* cit.), pp. 100-101.
[56] NOTICIAS SALAMANCA (04.05.2021): *El "sexting" crece con la pandemia: el 59% asegura que ahora se siente más motivado a practicarlo*. Accessible a: https://noticiassalamanca.com/sociedad/el-sexting-crece-con-la-pandemia/ [Última consulta realitzada el 25.08.2022].
[57] Els adolescents no valoren de forma suficient els riscs associats a la pràctica del *sexting*, duent-la a terme per a impressionar a altres, divertir-se o senzillament autoafirmar-se en una etapa decisiva i a la vegada convulsa de la formació de la personalitat d'un mateix.
[58] GREEN, Justice; HOPKINS, Nick; PAINES, Nicholas; GREEN, Sarah; LEWIS, Penney (2022): *Intimate image abuse: a final report*. Londres, The Law Commission of the United Kingdom, nº 407, p. 56.
[59] El *upskirting* es basa en la realització no consentida de fotografies de les natges i genitals femenins per sota de la faldilla.

3.3. El *grooming* de persones menors d'edat

Per finalitzar la visió dels cibercrims socials convé referir-nos a l'anomenat *online grooming*, *childgrooming* o *cybergrooming*, és a dir, la captació de menors d'edat a través d'Internet per consumar un abús o agressió sexual (art. 183 CP), o la realització de pornografia i delictes de corrupció de menors (art. 189 CP)[60]. De forma general, el tipus penal recollit per l'anglicisme es podria qualificar d'*apropament i entabanament de persones menors d'edat*. El bé jurídic protegit és la indemnitat sexual del menor, però també es preserva la formació i desenvolupament de la seva personalitat i sexualitat[61]. L'abusador detecta els perfils més febles, que es projecten a les xarxes com a joves incompresos familiarment i socialment, i s'hi aproximen simulant que són un interlocutor confiable i proper[62]. El *groomer* estudia detalladament el seu perfil, contactes, fotografies i opinions, per després enviar preguntes d'aparença innocent i començar el tracte nefast amb la víctima[63].

El Codi Penal recull el *cybergrooming* a l'article 183 ter CP, fixant el contacte cap a un menor de 16 anys, a través de qualsevol TIC, proposant-lo de concertar una trobada amb aquest per a les finalitats exposades. Es tracta d'un *delicte de perill* que no requereix que hi hagi contacte físic entre la persona agressora i l'agredida[64]. El bé jurídic protegit és doble: d'una banda, l'individual en relació amb el menor afectat; de l'altra, supraindividual, sobre la protecció de la infància en general contra l'actuació de pederastes[65]. Amb aquest objectiu, l'ONG en defensa dels drets dels menors TERRE DES HOMMES i l'EUROPOL van crear el perfil virtual d'una nena filipina de deu anys d'edat mitjançant la intel·ligència artificial, anomenada *Sweetie*[66], que per l'elevat realisme de la imatge en vídeo va atreure l'atenció de més de 20.000 pedòfils a tot el món entre 2013 i 2014 mitjançant una estratègia coordinada per l'EUROPEAN CYBERCRIME CENTRE (EC3)[67].

4. CIBERDELICTES POLÍTICS O CONTRA INTERESSOS GENERALS

4.1. El ciberespionatge i la ciberguerra creixen

El conflicte recent a Ucraïna ha destacat, encara més, l'ús de les xarxes per causar estralls en infraestructures i serveis estratègics d'altres Estats. Segons l'empresa MICROSOFT, Rússia hauria realitzat ciberatacs i intents de ciberespionatge a institucions de 42 països que haurien donat suport a Ucraïna des de l'inici de la intervenció de març de 2022, situades principalment als

[60] Les persones menors d'entre 12 i 14 anys són especialment vulnerables, per trobar-se en una fase primerenca de l'adolescència, disposar d'un accés ampli a les TICs i fer-ne un ús intensiu, i a la vegada no comprendre el caire sexual de moltes de les converses que es puguin arribar a desenvolupar.

[61] DE LA MATA BARRANCO, Norberto (2017): "El contacto tecnológico con menores del art. 183 ter 1 CP como delito de lesión contra su correcto proceso de formación y desarrollo personal sexual". Granada, *Revista Electrónica de Ciencia Penal y Criminología*, nº 19-10, p. 5.

[62] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (...) (op. cit.)*, p. 97.

[63] GRANJA, Pedro Javier (2020): "«Grooming»: el minotauro en Internet. El derecho penal del enemigo frente al pederasta de la era digital". Bogotá, *Revista de Derecho Penal y Criminología*, vol. 41, nº 111, p. 81.

[64] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op. cit.)*, p. 154.

[65] GRANJA, Pedro Javier (2020): "«Grooming»: el minotauro en Internet *(...)*" *(op. cit.)*, p. 82.

[66] BBC NEWS (05.11.2013): *Computer-generated 'Sweetie' catches online predators*. Accessible a: https://www.bbc.com/news/uk-24818769 [Última consulta realitzada el 25.08.2022].

[67] BUENO DE MATA, Federico (2022): "Novas tendências na investigação de crimes complexos em um contexto europeu globalizado". Rio de Janeiro, *Revista Eletrônica de Direito Processual*, vol. 23, nº 1, pp. 440-441.

Estats Units, Polònia, les Repúbliques Bàltiques i els països membres del Consell Nòrdic. En un 29% dels casos els atacants haurien aconseguit el seu propòsit i fins i tot s'haurien apoderat d'informacions privades[68].

És en aquests escenaris on es produeixen els anomenats *cibercrims polítics*. En la seva naturalesa cibernètica pura, es tractarà d'atacs de denegació de servei en el marc de les anomenades *cyberwar* i el *cyberhacktivism*, juntament amb l'ús de codi maliciós intrusiu per afectar el funcionament dels sistemes clau. Cal no oblidar que l'*ius ad bellum* desenvolupat en el context de la Carta de les Nacions Unides considera que els ciberatacs són una expressió de l'ús de la força, de manera que en legítima defensa els Estats podrien respondre amb armament convencional[69]. Els *cibercrims polítics* també representen, de forma general, una manifestació d'una modalitat delictual tan antiga com l'existència de grups cohesionats d'éssers humans; la guerra i l'espionatge han existit des de sempre.

En el context pre-bèl·lic del març del 2022 i advertida, com altres institucions públiques, de possibles ingerències informàtiques procedents de l'Est europeu, la UNIVERSITAT DEL PAÍS BASC va ordenar el canvi de contrasenya urgent a 7.800 treballadors dels cossos docents i d'administració per a evitar les greus conseqüències que un ciberatac de gran envergadura podria arribar a comportar a la institució[70] [71]. Aquest mateix any 2022 la UNIVERSITAT OBERTA DE CATALUNYA ja havia patit una agressió de tipus *ransomware* que havia bloquejat el campus virtual durant 20 hores, coincidint amb el període d'exàmens telemàtics[72].

Malgrat la recent conflagració a Ucraïna, l'ús de les TIC en el marc de la *ciberguerra* no és nou al segle XXI. L'any 2007, Estònia va patir una onada de ciberatacs considerable[73] [74]. Posteriorment, l'OTAN va instaurar el CENTRE D'EXCEL·LÈNCIA DE CIBERDEFENSA COOPERATIVA a Tallinn per assistir els Estats membres en situacions assimilables i ajudar a empreses i institucions[75]. Un any després, presumptes *hackers* russos van produir un atac de denegació de servei múltiple a llocs web oficials de l'Administració de Geòrgia després de l'inici del conflicte d'Ossètia del Sud.

[68] 20 MINUTOS (22.06.2022): *Microsoft asegura que Rusia ha lanzado ciberataques contra 42 países aliados de Ucrania desde que empezó la guerra*. Accessible a: https://www.20minutos.es/noticia/5020016/0/microsoft-asegura-que-rusia-ha-lanzado-ciberataques-contra-42-paises-aliados-de-ucrania-desde-que-empezo-la-guerra/ [Última consulta realitzada el 25.08.2022].

[69] PONS GAMÓN, Vicente (2017): "Internet, la nueva era del delito *(...)*" *(op. cit.)*, p. 87.

[70] EL MUNDO (03.03.2022): *La Universidad vasca ordena a toda su plantilla proteger sus cuentas electrónicas ante un "ciberataque inminente"*. Accessible a: https://www.elmundo.es/pais-vasco/2022/03/03/622115d3fc6c83ed028b457f.html [Última consulta realitzada el 25.08.2022].

[71] La Universitat era conscient que s'hauria produït una venda de credencials dels usuaris interns a tercers, després d'un presumpte ciberatac inicial, i va decidir d'adoptar una decisió prudent.

[72] 20 MINUTOS (03.01.2022): *La Universitat Oberta de Catalunya vuelve a la normalidad tras el ataque de ransomware que había dañado los servidores centrales de su Campus Virtual*. Accessible a: https://www.20minutos.es/tecnologia/ciberseguridad/la-universitat-oberta-de-catalunya-vuelve-a-la-normalidad-tras-el-ataque-de-ransomware-que-habia-danado-los-servidores-centrales-de-su-campus-virtual-4935636/ [Última consulta realitzada el 25.08.2022].

[73] Després que les autoritats estonianes retiressin una estàtua amb càrrega simbòlica al port de Tallin, es va produir una seqüència de ciberatacs en tot el país, que va saturar el ciberespai i requerí un mes per a recuperar-se. Entre les institucions més afectades hi hagué el parlament, els ministeris, entitats financeres i mitjans de comunicació.

[74] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op.* cit.), p. 107.

[75] PONS GAMÓN, Vicente (2017): "Internet, la nueva era del delito: *(...)*" *(op. cit.)*, p. 90.

Un altre exemple remarcable és el virus tipus *worm* anomenat *Stuxnet*[76], que ha estat considerat la primera arma digital de la història[77]. En aquest camp especialment, la informatització comporta greus riscos per a la gestió de les amenaces nuclears i l'ús de la capacitat dissuasòria de les grans potències, ja que podria provocar l'esclat d'una escalada involuntària de *destrucció mútua assegurada*, ja sigui només entre Estats o amb la intromissió d'agents no nacionals. Així, en matèria d'armament nuclear és fonamental conservar els sistemes de control analògics i la desconnexió total d'Internet[78].

4.2. El ciberterrorisme es projecta globalment

Els *cibercrims polítics* també adopten la forma de conductes de *ciberterrorisme*. *Ab initio*, es pot tractar de *ciberatacs directes*, com les infeccions amb codi maliciós intrusiu i destructiu, o els ja esmentats atacs *DoS*. Aquest és el supòsit que ha estat contemplat a l'article 573.2 del Codi Penal, que estableix per remissió que tindran la consideració de delictes terroristes, els supòsits de danys informàtics contemplats als articles 264 a 264 *quater* CP quan concorrin finalitats terroristes. En el cas de desestabilització greu en el funcionament de les estructures econòmiques o socials d'un país (article 573.1.1 CP), l'article 573.2 CP no es podria aplicar conjuntament amb el precepte anterior per identitat de fonament i s'hauria de fer un concurs de lleis, a ser resolt per alternativitat[79].

El tipus bàsic del delicte de terrorisme es recull a l'article 573.1 del Codi Penal i es tracta d' *un tipus mixt alternatiu*[80]. Així, serà considerada terrorista la conducta de qui busqui subvertir l'ordre constitucional, obligar els poders públics a fer un acte o abstenir-se de fer-ho, alterar la pau pública, desestabilitzar una organització internacional o provocar terror en una part de la població.Així mateix, la noció d'*infraestructures crítiques* és essencial. Aquestes comprenen el conjunt de béns jurídics, de caràcter tangible o intangible, que són necessaris per desenvolupar les activitats bàsiques de governs, organitzacions de tipologia diversa i ciutadans, pertanyents a una determinada zona geogràfica i temps.

Les *infraestructures crítiques en línia* haurien de rebre un tractament i tutela jurídics diferenciats, d'acord amb el seu impacte real a la vida de les persones o les activitats d'institucions[81]. No es pot obviar que les TICs es poden fer servir per difondre propaganda i incitar a la comissió d'actes terroristes[82], al mateix temps que permetrien demanar dades clau, obtenir finançament, reclutar

[76] Després d'infiltrar-se en el portàtil d'un especialista l'any 2010, possiblement a través d'una memòria USB, el virus alterà la programació de les centrifugadores d'enriquiment del programa nuclear iranià, concentrat aleshores a la planta de Natanz. El *cuc* va modificar la velocitat normal de rotació dels sistemes i aquest fet causà grans dificultats al país per a la producció d'un arsenal nuclear propi.

[77] WIRED (11.03.2014): *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*. Accessible a: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ [Última consulta realitzada el 25.08.2022].

[78] FUTTER, Andrew (2022): "La ciberseguridad de los sistemas de armas nucleares. Amenazas, vulnerabilidades y consecuencias". Barcelona, *Vanguardia Dossier*, nº 84, pp. 86-90.

[79] GALÁN MUÑOZ, Alfonso (2019): *Los ciberdelitos en el ordenamiento español (...) (op. cit.)*, p. 197.

[80] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op.* cit.), p. 182.

[81] COAQUIRA FLORES, Ángel Jeancarlo (2020): *Aproximación a la naturaleza jurídica de las infraestructuras críticas: delineando las bases para la ciberseguridad peruana*. A BUENO DE MATA, Federico (Dir.); GONZÁLEZ PULIDO, Irene (Coord.) (2020): *Fodertics 8.0. Estudios sobre tecnologías disruptivas y justicia*. Granada, Editorial Comares, p. 339.

[82] Efectivament, el Codi Penal preveu condemnes pels tipus d'enaltiment del terrorisme de l'article 578 CP, amb unes penes superiors si els continguts son difosos a través de mitjans de comunicació, Internet, o per mitjà de serveis

participants per realitzar les accions i instruir-los en la fabricació d'artefactes, per exemple[83]. La xarxa és un mitjà de gran utilitat per crear un sentiment de pertinença entre individus molt distants geogràficament i coordinar cèl·lules aïllades[84].

És en aquest escenari virtual que proliferen els discursos d'odi o *online hate speech*, que també són ciberdelictes de caire polític. Inicialment s'han format entorn de la persecució de grups ètnics concrets, tot difonent missatges d'odi i violència contra ells que s'amplifiquen per l'abast transnacional d'Internet i la facilitat amb què s'amaguen els agressors, amb molts més recursos per aprofitar-se de l'anonimat[85].

A la darrera dècada els autors del discurs d'odi s'han decantat també en contra d'altres col·lectius significatius, com les persones LGTBIQ+, les que tenen algun tipus de discapacitat o les que manifesten tenir unes preferències polítiques diferents. Per camuflar-se sota una aparença legítima s'han creat les anomenades *cloaked websites*, que són llocs web amb aspecte de diaris, ONG o associacions per a la defensa dels drets civils que difonen missatges discriminatoris encoberts. El disseny d'algunes xarxes socials com TWITTER, que són plataformes de *microblogging* o difusió de missatges curts, dificulta l'expressió de sentits de comunicació diferents i afavoreix la identificació d'un sentit únic. Els missatges d'aquestes xarxes són pobres en matisos i reforcen l'ús de la comunicació violenta[86].

5. OBSTACLES PROCESSALS A LA PERSECUCIÓ DEL CIBERCRIM

5.1. Indeterminació de la competència judicial

El lloc de comissió dels ciberdelictes és una noció fonamental però a la vegada difusa, amb un impacte decisiu a l'esfera internacional. Per exemple, podria resultar que un ciberatacant introdueix un perillós *malware* o codi maliciós en un país, aquest virus circula per servidors ubicats en altres Estats i finalment causa estralls en terceres nacions, com va acabar sent el cas de l'esmentat virus *Stuxnet*, que malgrat estar orientat cap a els sistemes iranians va afectar a infraestructures d'Indonèsia i altres països asiàtics. Aquí sorgeix la dificultat de determinar el Dret aplicable i quins òrgans judicials estaran en condicions de perseguir el delicte[87].

La *teoria de l'activitat* defensa que serà competent l'Estat en què l'acció va ser executada, és a dir, on es va dur a terme la conducta delictiva (*forum loci delicti comissi*). Hi ha arguments

de comunicacions electròniques o mitjançant l'ús de les TICs. Es justifica aquesta previsió per tal de punir la major rapidesa amb la qual es difonen aquestes actuacions.

[83] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (...) (op. cit.)*, p. 129.

[84] Com en el cas de l'autoproclamat ISIS, que ha dut a terme un ús extraordinari dels mitjans audiovisuals i les xarxes socials a Internet per a captar joves de països occidentals que se sentien frustrats i discriminats pels seus propis orígens familiars. *Vid.* SAN 3/2017, de 17 de febrer, rec. 6/2016. En aquest aspecte, resultà interessant la ponència presentada per un membre investigador de la Policia Nacional en el *Fórum de Expertos y Jóvenes Investigadores en Derecho y Nuevas Tecnologías – Fodertics 11.0*, que es desenvolupà a la UNIVERSIDAD DE SALAMANCA el passat 5 i 6 de maig de 2022.

[85] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (...) (op. cit.)*, p. 114.

[86] MIRÓ LLINARES, Fernando (2016): "Taxonomía de la comunicación violenta y el discurso del odio en Internet". Barcelona, *Revista de Internet, Derecho y Política*, nº 22, p. 97.

[87] CÁRDENAS ARAVENA, Claudia (2008): "El lugar de comisión de los denominados ciberdelitos". Talca, *Política Criminal. Revista Electrónica Semestral de Políticas Públicas en Materias Penales*, nº 6, p. 2.

raonables al respecte: el Tribunal disposa de més facilitats per obtenir proves i probablement per detenir i condemnar els presumptes autors. No obstant això, poden ser Estats fallits o *ciberparadisos*, sense cap interès a perseguir els criminals, o llocs que l'autor ha visitat temporalment i abandona al cap de poc temps[88]. En canvi, la *teoria del resultat* postula que serà competent l'Estat on es produeixi el resultat típic que acaba consumant la infracció. En el cas dels anomenats *delictes de resultat*, aquest és senzill de determinar. També cal apreciar que és un lloc més proper a la víctima, on es lesiona el bé jurídic[89], però per contra és significativament més difícil arribar a condemnar l'autor.

Per superar les dificultats anteriors, es va crear la *teoria de la ubiqüitat*, amb ànim d'obtenir el millor dels dos mons. Així, només cal que hagi esdevingut la conducta o el resultat a l'Estat respectiu i puguin ser competents dos o més Estats, a títol d'exemple. Aquest mecanisme garanteix que els buits de punició es poden superar, en el cas hipotètic que l'Estat del lloc de comissió considerés la teoria del resultat, i l'Estat del lloc del resultat optés per la teoria del lloc de la comissió.

Amb el concepte de la ubiqüitat es produeix una major seguretat jurídica[90]. El Dret internacional ha acceptat aquesta postura al Conveni de Budapest de 2001, però amb la problemàtica de considerar que els òrgans judicials s'han de cenyir a investigar únicament els dispositius situats al propi país, excloent-ne la cerca transfronterera a l'article 19.2, fet que limita les capacitats incriminatòries[91]. El Ple del TRIBUNAL SUPREM ha acceptat la *teoria de la ubiqüitat* en un acord no jurisdiccional de 3 de febrer de 2005, indicant que el delicte es comet a totes les jurisdiccions en què s'hagi realitzat algun element del tipus i que l'òrgan judicial que primer hagi iniciat actuacions processals serà el competent per instruir la causa[92].

5.2. Nombre de perjudicats indeterminat

Els delictes cibernètics poden afectar a un gran nombre de ciutadans, en alguns casos de molt difícil determinació[93] i per raons òbvies de posterior personació en un procés judicial. De manera il·lustrativa, s'estima que els estralls causats per un virus *ransomware* actiu des de l'abril del 2022 contra una trentena d'institucions públiques a Costa Rica han suposat unes pèrdues per al país equivalents a 30 milions de dòlars diaris. El MINISTERIO DE HACIENDA d'aquest país i la CAJA COSTARRICENSE DEL SEGURO SOCIAL són alguns dels organismes més afectats, amb un impacte remarcable sobre tota la població[94]. En altres casos, les persones perjudicades pretendran evitar personar-se per por o vergonya de revelar la seva pròpia identitat. A títol d'exemple, l'any 2019 el portal de cites canadenc *Ashley Madison*, que compta amb una elevada implantació a països occidentals i es caracteritza per promoure trobades sexuals entre persones casades, va patir

[88] CÁRDENAS ARAVENA, Claudia (2008): "El lugar de comisión *(...) (op. cit.)*, pp. 6-7.
[89] CÁRDENAS ARAVENA, Claudia (2008): "El lugar de comisión *(...) (op. cit.)*, pp. 8.
[90] CÁRDENAS ARAVENA, Claudia (2008): "El lugar de comisión *(...) (op. cit.)*, pp. 10-11.
[91] BLANCO, Hernán (2021): "El hackeo con orden judicial en la legislación procesal española a partir de la Ley Orgánica 13/2015 del 5 de octubre". Barcelona, *InDret*, nº 1/2021, p. 489.
[92] MARTÍN CANO, Ángel (2020): *Investigación penal de delitos tecnológicos*. A BUENO DE MATA, Federico (Dir.); GONZÁLEZ PULIDO, Irene (Coord.) (2020): *Fodertics 8.0. (...) (op. cit.)*, p. 287.
[93] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op.* cit.), p. 53.
[94] LA VANGUARDIA (17.06.2022): *Costa Rica sigue enfrentando las consecuencias de dos meses de ciberataques*. Accessible a: https://www.lavanguardia.com/vida/20220618/8349187/costa-rica-sigue-enfrentando-consecuencias-dos-meses-ciberataques.html [Última consulta realitzada el 25.08.2022].

un ciberatac a gran escala i es van filtrar les dades personals i financeres corresponents a més de 37 milions d'usuaris[95].

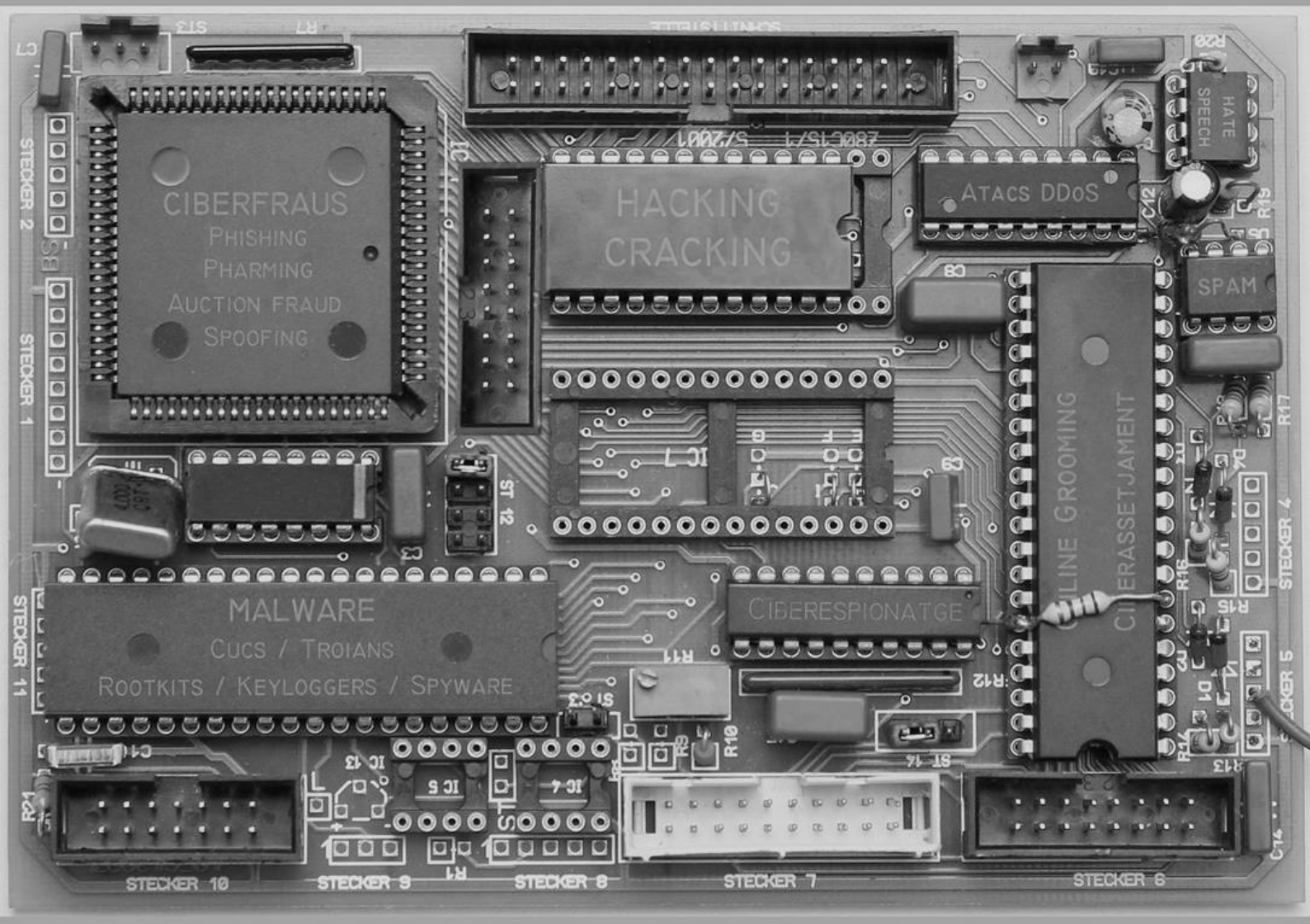
5.3. Anonimat i dificultats per descobrir l'autoria delictiva

L'autoria dels ciberdelictes és, en la majoria de casos, un aspecte difícil de ser determinat. L'ús de determinades *personalitats virtuals* encobreix la identificació dels delinqüents i en permet la impunitat, causant un escenari de *macrovictimització*. Així, sistemes com la xarxa TOR (*The Onion Router*) impedeixen la traçabilitat dels autors a la *Internet profunda* o *dark web*, creant capes superposades assimilables a una ceba que interrompen qualsevol possibilitat de seguiment. Inclús, el fet de ser titular d'una adreça IP no determina l'autoria del delicte[96]. Cal tenir en compte que a l'entorn digital les proves poden resultar fàcilment alterables, o senzillament destruïbles i inutilitzables per impossibilitar la identificació dels autors[97].

Pel que fa a l'autoria delictiva, resulta fonamental l'exegesi del TRIBUNAL SUPREM, concretament d'una reconeguda resolució de maig de 2015, qualificada generalment de la *sentència de les captures de pantalla*, per acreditar el contingut de missatges instantanis en xarxes socials i aplicacions de missatgeria[98]. L'Alt Tribunal expressa que *la impugnació de l'autenticitat de qualsevol d'aquestes converses, quan són aportades a la causa mitjançant arxius d'impressió, desplaça la càrrega de la prova cap a qui pretén aprofitar-ne la idoneïtat probatòria. Serà indispensable en tal cas la pràctica d'una prova pericial que identifiqui el veritable origen d'aquesta comunicació, la identitat dels interlocutors i, en fi, la integritat del contingut*[99]. No obstant això, com encertadament assenyala BUENO DE MATA, la resolució podia haver proporcionat recomanacions més extenses per a l'aportació de proves electròniques, com els segells de temps (*time stamping*), la cooperació amb les plataformes digitals o l'obligatorietat de practicar proves pericials a l'enjudiciament per instàncies superiors[100].

Alguns aspectes podran ser acreditats fàcilment davant de l'òrgan judicial mitjançant una navegació amb la presència del Lletrat de l'Administració de Justícia, que podrà proveir fe pública de la manera com s'han extret els documents basats en impressions de pantalla. Ara bé, aquest fet no exclou que es produeixin falsificacions o fraus, i aquí és interessant acreditar la veracitat del contingut mitjançant la declaració de testimonis i el desenvolupament d'una prova pericial informàtica. Hi ha elements que només es poden percebre a través d'una comprovació d'experts, per exemple, l'existència real del lloc web, qui n'és el titular, un anàlisi de metadades informatives sobre els accessos realitzats, etc.[101].

[95] LA GACETA DE SALAMANCA (11.01.2019): *Millones de adúlteros al descubierto gracias al hackeo de una web*. Accessible a: https://www.lagacetadesalamanca.es/hemeroteca/millones-adulteros-descubierto-gracias-hackeo-web-IRGS149634 [Última consulta realitzada el 25.08.2022].
[96] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op.* cit.), pp. 44-45.
[97] BARRIO ANDRÉS, Moisés (2011): "La ciberdelincuencia en el derecho español". Madrid, *Revista de las Cortes Generales*, nº 83, pp. 278-279.
[98] La resolució es pronuncia sobre la xarxa social TUENTI, malgrat que els arguments formen una doctrina que es pot extrapolar a plataformes com ara WHATSAPP o el mateix correu electrònic.
[99] STS 300/2015, de 19 de mayo, rec. 2387/2014, FJ 4.
[100] BUENO DE MATA, Federico (2015): "Acerca de la validez de los pantallazos como prueba electrónica en juicio". Salamanca, *Ars Iuris Salmanticensis*, vol. 3, p. 324.
[101] RICHARD GONZÁLEZ, Manuel (2017): *Investigación y prueba mediante medidas (...) (op. cit.),* p. 50.



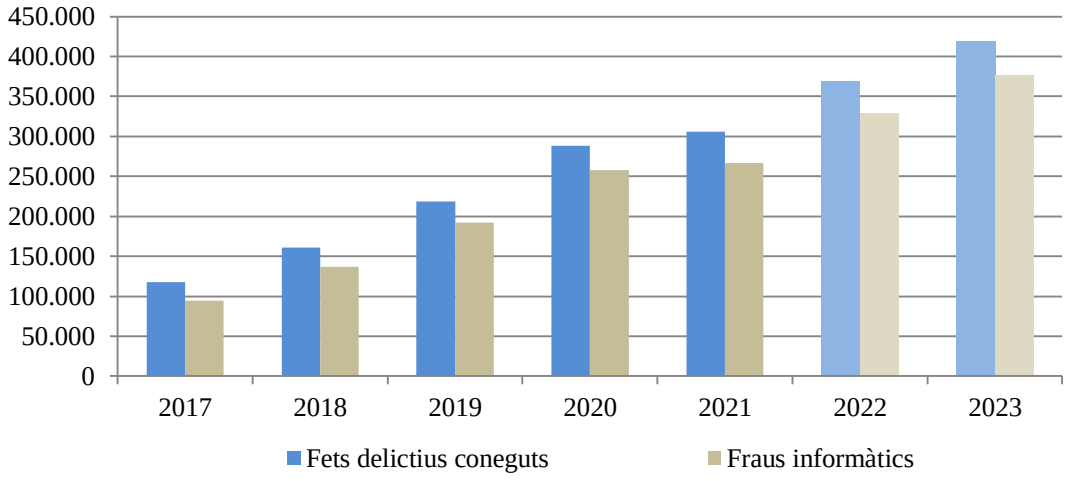
Conclusions

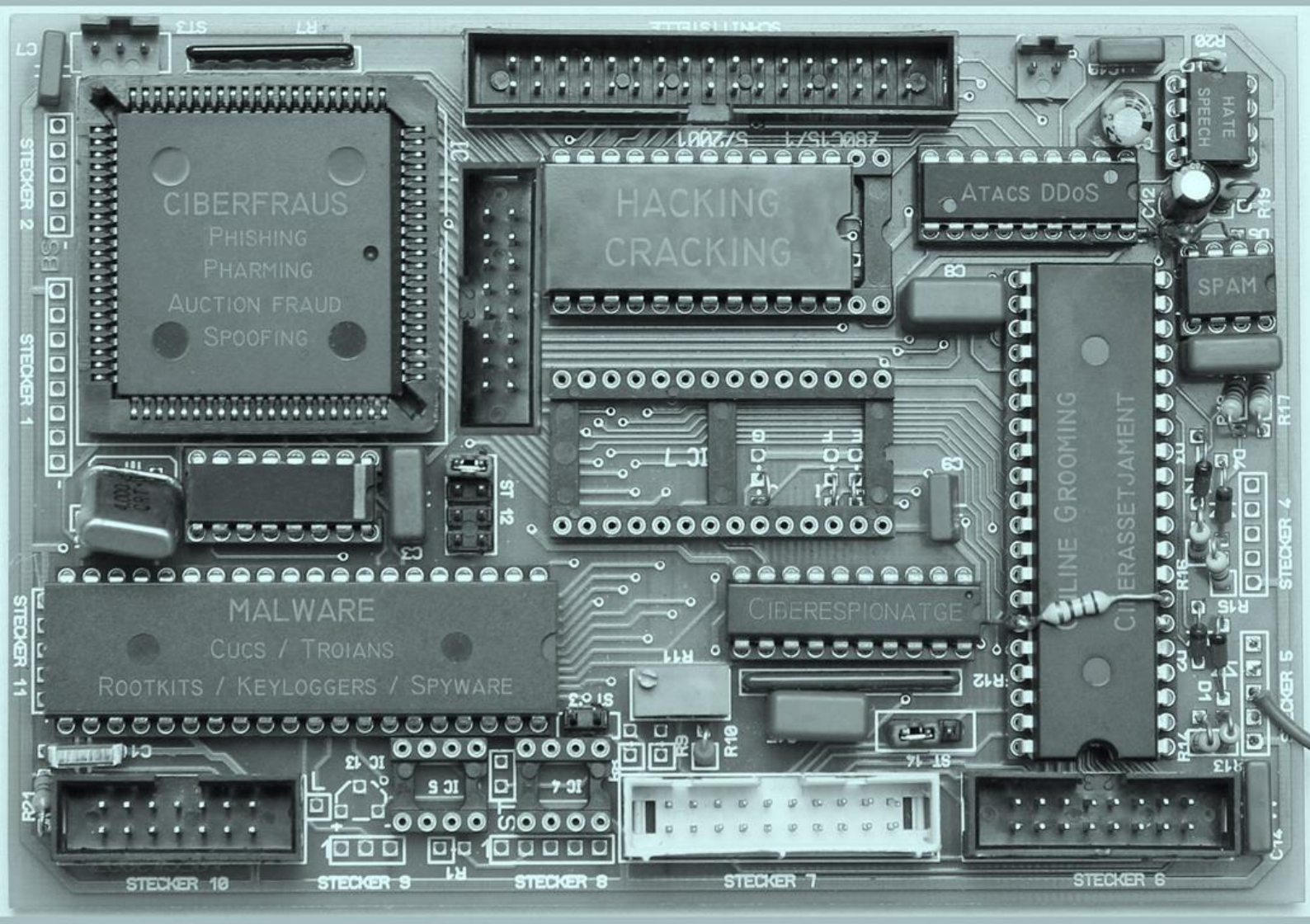
CONCLUSIONS

El present treball s'ha centrat en el cibercrim, un fenomen de difícil perseguibilitat. Actualment, molts dels ciberdelictes que es cometen no són denunciats i no es pot conèixer amb precisió l'envergadura real del fenomen. I en cas que el sistema processal penal aconsegueixi rebre la notícia de la seva perpetració, resulta extremadament difícil determinar-ne l'autoria delictiva, ja que existeixen nombrosos artificis per a encobrir-la de forma exitosa. Es pot dir que l'Estat de Dret es troba davant d'una problemàtica per a la qual té pocs instruments per a intervenir-hi, amb el risc que s'acabi centrant en lluitar contra tipus penals de poca entitat. De la mateixa manera, una pluralitat indeterminada de persones perjudicades dificulta la seva personació en un procés penal amb totes les garanties. Finalment, l'existència de *ciberparadisos* en Estats fallits o tolerants amb aquestes conductes delictives és un obstacle determinant per acabar obstruint el dret a la tutela judicial efectiva i determinar la impunitat en la seva forma més extrema.

L'anàlisi ha versat sobre les categories del cibercrim, adoptant les classificacions més acceptades per la doctrina actual. Les categories principals s'han diferenciat en tres blocs amplis, concretament: els *ciberdelictes econòmics i patrimonials*, els *ciberdelictes socials* i els *ciberdelictes polítics o contra els interessos generals*. Els primers ocupen la proporció més elevada dels fets denunciats i inclouen el *hacking* o *pirateig* i el *cracking*, la introducció de *malware* o codi maliciós, els ciberfraus, la ciberextorsió, la distribució de pornografia infantil i la pirateria contra la propietat intel·lectual. Els segons es corresponen a la translació a la xarxa de les relacions i interaccions humanes, i inclouen l'assetjament en línia i les seves múltiples variants, el *sexting* i la *revenge pornography* i el *grooming* de persones menors d'edat. Finalment, el tercer tipus de ciberdelictes abasta al ciberespionatge, la ciberguerra i el ciberterrorisme.

Les reformes aplicades al Codi Penal i la Llei d'Enjudiciament Criminal durant l'any 2015 han suposat que la legislació espanyola ha entrat en un escenari institucional més favorable per a atendre les necessitats de la societat, però malgrat aquest esforç no existeixen solucions màgiques per a afrontar un problema que va en augment. El gràfic inferior mostra una evolució del nombre de ciberdelictes registrats pel MINISTERI DE L'INTERIOR des de l'any 2017 fins al 2021, comprenent també la categoria principal d'il·lícits penals, és a dir, els fraus informàtics. La representació s'acompanya d'una estimació elaborada per l'autor de la incidència que podrien tenir properament en el 2022 i el 2023, en cas que es mantingui la mateixa evolució.





Referències

REFERÈNCIES

Bibliografia

1. BARRIO ANDRÉS, Moisés (2011): "La ciberdelincuencia en el derecho español". Madrid, *Revista de las Cortes Generales*, nº 83, pp. 273-305.

2. BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*. Las Rozas (Madrid), Wolters Kluwer.

3. BLANCO, Hernán (2021): "El hackeo con orden judicial en la legislación procesal española a partir de la Ley Orgánica 13/2015 del 5 de octubre". Barcelona, *InDret*, nº 1/2021, pp. 431-501.

4. BUENO DE MATA, Federico (2015): "Acerca de la validez de los pantallazos como prueba electrónica en juicio". Salamanca, *Ars Iuris Salmanticensis*, vol. 3, pp. 322-324.

5. BUENO DE MATA, Federico (2022): "Novas tendências na investigação de crimes complexos em um contexto europeu globalizado". Rio de Janeiro, *Revista Eletrônica de Direito Processual*, vol. 23, nº 1, pp. 434-457.

6. CÁRDENAS ARAVENA, Claudia (2008): "El lugar de comisión de los denominados ciberdelitos". Talca, *Política Criminal. Revista Electrónica Semestral de Políticas Públicas en Materias Penales*, nº 6, pp. 1-14.

7. COAQUIRA FLORES, Ángel Jeancarlo (2020): *Aproximación a la naturaleza jurídica de las infraestructuras críticas: delineando las bases para la ciberseguridad peruana*. A BUENO DE MATA, Federico (Dir.); GONZÁLEZ PULIDO, Irene (Coord.) (2020): *Fodertics 8.0. Estudios sobre tecnologías disruptivas y justicia*. Granada, Editorial Comares, pp. 333-343.

8. COMISSIÓ EUROPEA (2020): *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Estrategia de la UE para una lucha más eficaz contra el abuso sexual de menores*. Brussel·les, COM(2020) 607 final.

9. DE LA MATA BARRANCO, Norberto (2017): "El contacto tecnológico con menores del art. 183 ter 1 CP como delito de lesión contra su correcto proceso de formación y desarrollo personal sexual". Granada, *Revista Electrónica de Ciencia Penal y Criminología*, nº 19-10, pp. 1-28.

10. FUTTER, Andrew (2022): "La ciberseguridad de los sistemas de armas nucleares. Amenazas, vulnerabilidades y consecuencias". Barcelona, *Vanguardia Dossier*, nº 84, pp. 86-90.

11. GALÁN MUÑOZ, Alfonso (2019): *Los ciberdelitos en el ordenamiento español*. Barcelona, Editorial UOC.

12. GOBIERNO DE ESPAÑA. MINISTERIO DEL INTERIOR (2022): *Informe sobre la cibercriminalidad en España 2021*. Madrid, Secretaría de Estado de Seguridad, Dirección General de Coordinación y Estudios.

13. GRANJA, Pedro Javier (2020): "«Grooming»: el minotauro en Internet. El derecho penal del enemigo frente al pederasta de la era digital". Bogotá, *Revista de Derecho Penal y Criminología*, vol. 41, nº 111, pp. 61-108.

14. GREEN, Justice; HOPKINS, Nick; PAINES, Nicholas; GREEN, Sarah; LEWIS, Penney (2022): *Intimate image abuse: a final report*. Londres, The Law Commission of the United Kingdom, nº 407.

15. MARTÍN CANO, Ángel (2020): *Investigación penal de delitos tecnológicos*. A BUENO DE MATA, Federico (Dir.); GONZÁLEZ PULIDO, Irene (Coord.) (2020): *Fodertics 8.0. Estudios sobre tecnologías disruptivas y justicia*. Granada, Editorial Comares, pp. 285-297.

16. MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid, Marcial Pons.

17. MIRÓ LLINARES, Fernando (2013): "Derecho penal, «cyberbullying» y otras formas de acoso (no sexual) en el ciberespacio". Barcelona, *Revista de Internet, Derecho y Política*, nº 16, pp. 61-75.

18. MIRÓ LLINARES, Fernando (2016): "Taxonomía de la comunicación violenta y el discurso del odio en Internet". Barcelona, *Revista de Internet, Derecho y Política*, nº 22, pp. 93-118.

19. PONS GAMÓN, Vicente (2017): "Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad". Quito, *URVIO - Revista Latinoamericana de Estudios de Seguridad*, nº 20, pp. 80-93

Notícies de premsa

1. BBC NEWS (05.11.2013): *Computer-generated 'Sweetie' catches online predators*. Accessible a: https://www.bbc.com/news/uk-24818769 [Última consulta realitzada el 25.08.2022].

2. WIRED (11.03.2014): *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*. Accessible a: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ [Última consulta realitzada el 25.08.2022].

3. CONSEJO GENERAL DEL PODER JUDICIAL (24.02.2017): *El Tribunal Supremo avala la 'lista Falciani' como prueba de cargo del delito fiscal*. Accessible a: https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Tribunal-Supremo/Noticias-Judiciales/El-Tribunal-Supremo-avala-la--lista-Falciani--como-prueba-de-cargo-del-delito-fiscal [Última consulta realitzada el 25.08.2022].

4. LA GACETA DE SALAMANCA (11.01.2019): *Millones de adúlteros al descubierto gracias al hackeo de una web*. Accessible a: https://www.lagacetadesalamanca.es/hemeroteca/millones-adulteros-descubierto-gracias-hackeo-web-IRGS149634 [Última consulta realitzada el 25.08.2022].

5. NOTICIAS SALAMANCA (04.05.2021): *El "sexting" crece con la pandemia: el 59% asegura que ahora se siente más motivado a practicarlo*. Accessible a: https://noticiassalamanca.com/sociedad/el-sexting-crece-con-la-pandemia/ [Última consulta realitzada el 25.08.2022].

6. ESCUDO DIGITAL (05.11.2021): *Los centennials y millennials son los menos proclives a denunciar un ciberdelito*. Accessible a: https://www.escudodigital.com/ciberseguridad/centennials-millennials-no-denuncia-ciberdelito_50099_102.html [Última consulta realitzada el 25.08.2022].

7. LA VANGUARDIA (23.11.2021): *El Govern destina 3,5 millones a la UAB para recuperarse del ciberataque*. Accesible a: https://www.lavanguardia.com/vida/20211123/7883348/govern-destina-3-5-millones-uab-recuperarse-ataque-informatico.html [Última consulta realitzada el 25.08.2022].

8. 20 MINUTOS (03.01.2022): *La Universitat Oberta de Catalunya vuelve a la normalidad tras el ataque de ransomware que había dañado los servidores centrales de su Campus Virtual*. Accessible a: https://www.20minutos.es/tecnologia/ciberseguridad/la-universitat-oberta-de-catalunya-vuelve-a-la-normalidad-tras-el-ataque-de-ransomware-que-habia-danado-los-servidores-centrales-de-su-campus-virtual-4935636/ [Última consulta realitzada el 25.08.2022].

9. EL MUNDO (03.03.2022): *La Universidad vasca ordena a toda su plantilla proteger sus cuentas electrónicas ante un "ciberataque inminente"*. Accessible a: https://www.elmundo.es/pais-vasco/2022/03/03/622115d3fc6c83ed028b457f.html [Última consulta realitzada el 25.08.2022].

10. FRANCE 24 (10.05.2022): *La cibercriminalidad costó más de 6 billones de dólares en 2021*. Accessible a: https://www.france24.com/es/minuto-a-minuto/20220510-la-cibercriminalidad-cost%C3%B3-m%C3%A1s-de-6-billones-de-d%C3%B3lares-en-2021 [Última consulta realitzada el 25.08.2022].

11. EL PERIÓDICO (23.05.2022): *Phishing: ¿Qué es y cómo evitarlo?* Accessible a: https://www.elperiodico.com/es/tecnologia/20220523/phishing-que-es-dv-13695404 [Última consulta realitzada el 25.08.2022].

12. LA GACETA DE SALAMANCA (24.05.2022): *Alerta por nuevos casos de estafas bancarias a través del correo electrónico*. Accessible a: https://www.lagacetadesalamanca.es/virales/alerta-por-nuevos-casos-de-estafas-bancarias-a-traves-del-correo-electronico-EE11262262 [Última consulta realitzada el 25.08.2022].

13. EL PERIÓDICO (27.05.2022): *'Hackers' estafen 350.000 euros a l'Institut d'Informàtica de Barcelona*. Accessible a: https://www.elperiodico.cat/ca/barcelona/20220527/hackers-institut-informatica-barcelona-estafa-phising-13717094 [Última consulta realitzada el 25.08.2022].

14. LA VANGUARDIA (17.06.2022): *Costa Rica sigue enfrentando las consecuencias de dos meses de ciberataques*. Accessible a: https://www.lavanguardia.com/vida/20220618/8349187/costa-rica-sigue-enfrentando-consecuencias-dos-meses-ciberataques.html [Última consulta realitzada el 25.08.2022].

15. 20 MINUTOS (22.06.2022): *Microsoft asegura que Rusia ha lanzado ciberataques contra 42 países aliados de Ucrania desde que empezó la guerra*. Accessible a: https://www.20minutos.es/noticia/5020016/0/microsoft-asegura-que-rusia-ha-lanzado-ciberataques-contra-42-paises-aliados-de-ucrania-desde-que-empezo-la-guerra/ [Última consulta realitzada el 25.08.2022].

16. LA VANGUARDIA (15.08.2022): *¿Quieres ser hacker ético? Los ciberataques disparan la demanda de sombreros blancos*. Accessible a: https://www.lavanguardia.com/vida/formacion/20220815/8466693/hacker-etico-ciberataques.html [Última consulta realitzada el 25.08.2022].

Taxonomia penal dels ciberdelictes

Anàlisi jurídic del crim digital

ARNAU GUIX SANTANDREU

RESUM

La digitalització a la nostra vida quotidiana és un fenomen innegable, de la mateixa manera que la irrupció dels ciberdelictes en aquesta pot arribar a suposar un impacte considerable sobre la nostra estabilitat financera i emocional. Cada dia, particulars, empreses i institucions són víctimes del cibercrim a tot el planeta, amb una tendència cada cop més a l'alça.

La primera qüestió que convindria plantejar-nos és: *Què entenem per ciberdelicte?* A partir d'aquí, el present anàlisi descobreix les tipologies principals dels il·lícits penals digitals, identificant els preceptes del Codi Penal que hi són d'aplicació, com la doctrina jurídica els descriu i trobant exemples il·lustratius d'actualitat per arribar a definir-los de forma més completa. Finalment, el present estudi es complementa amb l'observança dels obstacles que impedirien una persecució òptima dels ciberdelictes des de la perspectiva del Dret Processal.

Paraules clau: ciberdelicte, cibercrim, pirateig informàtic, ciberfrau, ciberassetjament.

AGS PUBLICATIONS

ISSN: 2696-1083

www.ags.cat

4 — 2022