INSTRUMENTS DE COOPERACIÓ ENTRE ELS ESTATS MEMBRES DE LA UNIÓ EUROPEA EN MATÈRIA DE CIBERDELINQÜÈNCIA

TREBALL FINAL DE GRAU

Paula Colprim Doñate

Tutora: Dra. Sílvia Pereira Puigvert

Universitat de Girona · Facultat de Dret · Grau en Dret · Curs Acadèmic 2020-2021

Primera convocatòria

If crime crosses borders, so must law enforcement. If the rule of law is undermined not only in one country, but in many, then those who defend it cannot limit themselves to purely national means. If the enemies of progress and human rights seek to exploit the openness and opportunities of globalization for their purposes, then we must exploit those very same factors to defend human rights and defeat the forces of crime, corruption and trafficking in human beings... Criminal groups have wasted no time in embracing today's globalized economy and the sophisticated technology that goes with it. But our efforts to combat them have remained up to now very fragmented and our weapons almost obsolete.... With enhanced international cooperation, we can have a real impact on the ability of international criminals to operate successfully and can help citizens everywhere in their often bitter struggle for safety and dignity in their homes and communities.

Kofi A. Annan

Pròleg de la Convenció de les Nacions Unides
contra la delinqüència organitzada transnacional

ÍNDEX DE CONTINGUTS

ABREVIATURES

CSIRT	Equip de resposta a incidents de seguretat informàtica. De l'anglès *Computer Security Incident Response Team.*
EC3	Centre Europeu de Ciberdelinqüència. De l'anglès *European Cybercrime Centre*.
EEMM	Estats Membres.
EJCN	La Xarxa Judicial Europea contra la Ciberdelinqüència. De l'anglès *European Judicial Cybercrime Network.*
ENISA	Agència de la Unió Europea de Ciberseguretat. De l'anglès *European Union Agency for Cybersecurity.*
EUROJUST	Agència de la Unió Europea per la Cooperació Judicial Penal.
EUROPOL	Agència Policial de la Unió Europea.
INTERPOL	Organització Internacional de Policia Criminal.
IOCTA	Informe avaluatiu de les amenaces de la delinqüència organitzada a internet. De l'anglès *The Internet Organised Crime Threat Assessment.*
J-CAT	Grup d'Acció Conjunta contra la Ciberdelinqüència. De l'anglès *Joint Cybercrime Action Taskforce.*
OEI	Ordre Europea d'Investigació.
SIS	Sistema d'Informació Schengen.
UE	Unió Europea.

INTRODUCCIÓ

Els canvis produïts per la globalització i digitalització de la societat les últimes dècades han millorat la qualitat de vida dels ciutadans, però també han fet sorgir una nova modalitat delictiva: la ciberdelinqüència.

Aquesta modalitat delictiva, que va aparèixer a la dècada dels vuitanta, és tan singular que exigeix un tractament especial per part del Dret, ja que els mètodes tradicionals no se li poden aplicar en molts casos. La seva singularitat rau en que, en gairebé tots els casos, té dimensió supranacional, i aquesta característica juga un paper crucial en el seu tractament. La ciberdelinqüència s'aprofita dels avantatges que li proporcionen les noves tecnologies, i treballa a partir d'un instrument molt potent: Internet. El ciberespai té abast global, s'hi pot accedir des de qualsevol part del món de manera instantània i precisament això és el que permet que els delinqüents puguin actuar, buscar víctimes i efectuar atacs des de qualsevol punt del món, dificultant-ne la persecució.

Mentre les lleis nacionals generalment només s'apliquen a un territori específic, la ciberdelinqüència creua fronteres. Precisament per això els problemes que comporta s'han de resoldre pel Dret Internacional, amb el requeriment d'adopció d'instruments legals adequats que evitin la impunitat. S'han d'executar polítiques conjuntes, generals, que integrin tots els Estats i sectors de la societat. Les disposicions d'assistència mútua entre Estats, és a dir, la cooperació, és un dels elements més rellevants que envolten aquesta modalitat delictiva. Per evitar la frustració de la persecució dels crims, es requereix un alt nivell de cooperació. La Unió Europea, com molts altres organismes a àmbit internacional, també ha de fer front a aquesta problemàtica.

Aquest treball té la finalitat d'analitzar quins són els diferents instruments de cooperació que té la Unió Europea per lluitar contra la ciberdelinqüència. És per això que el treball engloba diferents disciplines, com ara el dret processal, el dret comunitari i el dret internacional públic.

Per complir amb els objectius del treball, primerament al Capítol I introduirem l'objecte d'estudi explicant els orígens de la ciberdelinqüència, establint-ne una definició i analitzant les característiques i realitats que fan que requereixi un tracte tan especial.

Continuarem analitzant al Capítol II, genèricament, la cooperació judicial penal a la Unió Europea. En particular, farem èmfasi a tres instruments que són de gran utilitat en procediments que inclouen la ciberdelinqüència. En primer lloc analitzarem l'Agència de la Unió Europea per la Cooperació Judicial Penal, també coneguda com l'EUROJUST, i el paper que desenvolupa concretament en la lluita contra la ciberdelinqüència. En segon lloc farem un estudi de l'instrument que permet la detenció i entrega de sospitosos i condemnats quan es troben a diferents Estats Membres, l'Ordre de Detenció i Entrega. Finalment, analitzarem l'instrument que permet obtenir proves transfrontereres, l'Ordre Europea d'Investigació.

Acotant més l'anàlisi a l'objecte del treball, procedirem al Capítol III amb l'estudi dels instruments que ha implementat la Unió Europea específicament en l'àmbit de ciberdelinqüència. Farem una valoració de la seva implicació en l'assumpte a través de comunicacions i recomanacions, analitzarem els instruments normatius que ha aprovat en aquest àmbit i estudiarem actors creats específicament amb l'objectiu de lluitar ciberdelinqüència.

Per obtenir una visió més àmplia, i perquè tots els Estats Membres hi estan adherits, també farem un anàlisi al Capítol IV de l'instrument més rellevant existent actualment en el pla internacional en aquest àmbit, el Conveni sobre Ciberdelinqüència.

Finalitzarem amb el Capítol V, després d'un anàlisi de l'estat actual de la cooperació a nivell de la Unió Europea, amb un conjunt de crítiques al sistema i propostes per millorar-lo.

Per complir amb l'objectiu principal del treball i dur a terme l'anàlisi hem utilitzat una pluralitat de metodologia.

Pel que fa a la doctrina que hem consultat - tant espanyola com de caràcter comunitari i internacional - hem utilitzat manuals, monografies i articles doctrinals per entendre el concepte de ciberdelinqüència i els instruments de la Unió Europea que la combaten. La legislació consultada ha estat majoritàriament de caràcter comunitari però també internacional i espanyola. Així mateix, hem consultat una pluralitat de Comunicacions de la Comissió Europea i Comunicats de Premsa i Conclusions del Consell de la Unió Europea per entendre quina és la posició i estratègia de la Unió en aquest àmbit. A més, en aquesta investigació també hem fet ús d' informes de diferents fonts. Entre els autors dels informes consultats trobem institucions com la Comissió Europea o EUROJUST, però també informes particulars d'empreses especialitzades en la matèria. Finalment, també hem consultat pàgines web, principalment amb l'objectiu d'adquirir més informació de diferents organismes a través dels seus portals oficials.

CAPÍTOL I -CONSIDERACIONS GENERALS SOBRE CIBERDELINQÜÈNCIA

1.1 - La societat de la informació i els orígens de la ciberdelinqüència

Tot el progrés tecnològic que està transformant la societat actual i està fent sorgir noves formes de delinqüència, dins les quals la ciberdelinqüència, s'emmarca en el que es denomina la Societat d'Informació. L'evolució des de la Societat Industrial fins la Societat d'Informació és un procés de expansió constant, que afecta tota la societat en forma de xarxa. La base d'aquesta Societat d'Informació rau, no tant en la riquesa material, si no en els recursos intel·lectuals de les persones i la seva capacitat de processar informació i projectar innovació. Es pot definir com una societat en la que els ciutadans siguin capaços de fer ús dels diversos serveis de telecomunicacions avançades per millorar els diferents aspectes de la seva vida quotidiana. [1] La Unió Europea ha sigut un dels principals promotors de la Societat d'Informació, adoptant als anys noranta els plans d'actuació anomenats "Europa en marxa cap a la Societat d'Informació" i "Europa a la Vanguardia de la Societat d'Informació".

La Societat d'Informació té potencia per millorar la qualitat de vida dels ciutadans i a reforçar la cohesió social, però també pot tenir efectes devastadors si no s'utilitza amb la mesura, responsabilitat i prudència necessaris. Aprofitant els avantatges que proporciona la Societat d'Informació i les noves tecnologies, ha aparegut la ciberdelinqüència, i ha anat augmentant constantment en la mateixa mesura que els avenços informàtics.

La ciberdelinqüència no existiria sense la informàtica, i és per això que per explicar-ne els seus orígens hem de començar amb la invenció de la màquina desxifradora dels codis alemanys encriptats *Engima*. Alan Turing es va convertir el 1939 en el pare de la ciència de la computació i trenta anys més tard, al 1969, es va crear el sistema operatiu *UNIX*, que es va acabar convertint en l'eix principal de la infraestructura en la informàtica.

A principis de la dècada dels anys setanta, els delinqüents cometien delictes a través de les línies telefòniques i s' autoanomenaven *Phreakers*, però no va ser fins a la dècada dels anys vuitanta en que es va començar a parlar de ciberdelinqüència com a tal. Al 1981 es va condemnar a Ian Murpy per piratejar la xarxa d'una companyia multinacional de telecomunicacions i es va convertir en el primer condemnat d'un delicte cibernètic. Un any més tard, al 1982, es va crear el primer virus informàtic, i al 1989 el primer codi maligne informàtic (també anomenat *worm*) i el primer atac de segrest de dades (també anomenat *ransomware*).

[1] José Enrique Anguita Osuna "Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea" *Revista de Estudios en Seguridad Internacional*, Vol. 4, No.1, 2018. Pg. 107-126 http://dx.doi.org/10.18847/1.7.7

Davant els danys cada cop més elevats de la ciberdelinqüència, i veient que s'estava convertint en quelcom recurrent, Estats Units d'Amèrica va aprovar la primera legislació relacionada amb aquest àmbit, la Llei Federal d'Abús i Frau Informàtic de 1986. Al 1990, amb l'objectiu de respondre a les amenaces dels drets civils que es produïen a través d'aquesta pràctica delictiva, el mateix país va crear l' *Electronic Frontier Foundation (EFF)*, la primera organització creada a aquests efectes i encara activa actualment. Aquesta fundació té al seu servei informàtics, advocats i altres professionals que, ja des del seus inicis, tenen el deure de defensar i protegir els consumidors dels ciberatacs. Amb la tecnologia molt més avançada, al 1999 es va dur a terme per primera vegada un enviament en massa de correus electrònics que contenen virus. Amb el canvi de segle, i també l'avanç cada cop més ràpid de la tecnologia, les tècniques de ciberdelinqüència van anar en augment i van seguir un creixement que fins a l'actualitat avança a una velocitat que en dificulta el seu estudi i la seva prevenció.

1.2 - Què significa el terme ciberdelinqüència

1.2.1 Definició

El *Conveni sobre Ciberdelinqüència del Consell d'Europa de 8 de Novembre de 2001*, també conegut com el Conveni de Budapest, és un referent internacional per definir què es considera que és la ciberdelinqüència, ja que un dels seus objectius és l'harmonització de la tipificació d'aquests actes per millorar l'eficiència en la persecució de delinqüents tecnològics més enllà de les fronteres de cada país.

El conveni ens explica què és la ciberdelinqüència a través d'una llista de conductes delictives que s'identifiquen com a tal: la falsificació informàtica, el frau informàtic, els delictes relacionats amb la pornografia infantil i els delictes relacionats amb infraccions de la propietat intel·lectual i dels drets afins. No podem extreure a través d'aquest text legislatiu una definició concreta del terme, però el preàmbul ens dóna a entendre que es tracta de:

> " Aquells actes dirigits contra la confidencialitat, integritat i disponibilitat dels sistemes informàtics, xarxes i dades informàtiques, així com l'abús d'aquests sistemes, xarxes i dades"

La Unió Internacional de Telecomunicacions considera que el Ciberdelicte es defineix com[2]:

[2] Unión Internacional de Telecomunicaciones, Divisón de Aplicaciones TIC y Ciberseguridad. *El Ciberdelito: Guía para Países en Desarollo.* 2009. https://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf

> ”Qualsevol activitat delictiva en la que s’utilitzen com a eina els ordinadors o xarxes, o aquests son la víctima de la mateixa, o bé el medi des del que s’efectua l’activitat delictiva.”

La doctrina ens dóna altres definicions i reflexions entorn la seva definició. Lira Arteaga [3] va més enllà d’una simple definició i fa una reflexió interessant al distingir entre els ciberdelictes i aquelles conductes antijurídiques que utilitzen com a medi o fi les tecnologies de la informació i comunicació. És a dir, diferencia entre els termes anglosaxons que relacionem directament amb la paraula ciberdelinqüència (*phishing, ransmoware, grooming...*) i la tècnica que s’utilitza per cometre un delicte, la pròpia conducta delictiva. Considera que els esforços s’han de centrar en identificar la conducta delictiva comesa a través del cibercrim, en comptes que crear nous tipus penals que ja s’han realitzat molt anteriorment abans de que hi haguessin ordinadors. Per exemple: el *phishing* no deixa de ser una forma de frau, el *ransmoware* d’ extorsió, el *grooming* d’assetjament sexual a menors...Les conductes antijurídiques han existit molt anteriorment que les seves vessants informàtiques, l’únic que amb l’aparició d’informàtica aquestes s’han dut a terme amb diferents mitjans. Lira Arteaga acaba definint la ciberdelinqüència com:

> “la conducta delictiva que utilitza com a fi o mitjà les tecnologies de la informació i comunicació i que es troba tipificada en els diferents codis penals.”

Així ho veu també Fernández Bermejo[4], al definir-la com:

> “Tot aquell il·lícit penal que s’ha dut a terme a través de mitjans informàtics.”

Fernández Bermejo també defensa que al Codi Penal Espanyol no hi ha un títol específic que contengui els delictes tecnològics o informàtics ja que senzillament són aquells que es cometen a través del mitja telemàtic i que tenen via probatòria a través de la prova informàtica. És per això que normalment aquests delictes estan regulats a la seva forma tradicional als codis penals, i la informàtica acaba sent només el mitjà a través del qual es duen a terme. Per tant, la ciberdelinqüència no és més que un delicte dut a terme a través d’un mitjà específic, Internet.

[3]Oscar Manuel Lira Arteaga. *Ciberdelitos: prespectivas para su persecución. (* Ciudad de México: Tirant Lo Blanch, 2018) Pg. 23

[4]Daniel Fernàndez Bermejo y Gorgonio Martinez Atienza . *Ciberseguridad, ciberespacio y ciberdelincuencia*. (Navarra: Aranzadi Thomson Reuters, 2018). Pg. 31

Al 2007 la Comissió Europea publica la Comunicació *Cap a una política general de lluita contra ciberdelinqüència*[5], en la que elabora la seva pròpia definició de ciberdelinqüència. estableix que el terme ciberdelinqüència inclou:

- Les formes tradicionals de delinqüència mitjançant les xarxes de comunicació i sistemes d'informació electrònics com la falsificació o frau
- Els continguts il·legals a través de mitjans de comunicació electrònics com ara les imatges d'abús sexual a menors o incitacions a l'odi racial
- Els delictes específics de les xarxes electròniques, com ara els atacs contra els sistemes informàtics i la pirateria.

Per tant, s'entén d'aquesta comunicació que ciberdelinqüència és tant les activitats delictives realitzades amb ajuda de les xares de comunicacions i sistemes d'informació electrònics com les activitats contra aquestes xarxes i sistemes.

En relació al bé jurídic que protegeix el ciberdelicte, es pot dir que aquest acostuma a ser múltiple o complex. Pot ser, entre altres: la propietat, la intimitat, la informació, la informació sobre la mateixa informació, la seguretat, la fe pública, la violació de la dignitat de la persona o el seu lliure desenvolupament sexual, sempre realitzats a través de la informàtica. A vegades, en canvi, no es tracta de nous béns jurídics dignes de protecció, sinó de noves formes de protegir el contingut dels drets fonamentals, com ara la privacitat, que no és res més que l'ampliació de la intimitat. De fet, cada vegada són més els acadèmics que sostenen que en l'àmbit de la ciberdelinqüència s'ha de crear una nova categoria jurídica penal que inclogui les conductes vinculades amb el dret informàtic, i on es lesionin no només els béns jurídics tradicionals sinó també uns nous béns jurídics protegits propis de l'era digital, com ara la intimitat informàtica, la integritat, confidencialitat i disponibilitat de dades o la confiança en el funcionament dels sistemes informàtics. [6]

Molt sovint els delictes informàtics intenten protegir penalment un concurs de béns jurídics, motiu pel qual s'ha arribat a afirmar que no és un nou tipus de delicte sinó formes delictives noves, ja que més que trobar-nos davant una categoria delictiva, ens trobem davant un nou mecanisme

[5] Comisión Europea. *Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones, de 22 de mayo de 2007, "Hacia una política general de lucha contra la ciberdelincuencia*, (Bruselas: 2007) https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:ES:PDF

[6] José Enrique Anguita Osuna "Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea" *Revista de Estudios en Seguridad Internacional*, Vol. 4, No.1, 2018. Pg. 107-126 http://dx.doi.org/10.18847/1.7.7

tecnològic que ha fet trontollar el sistema penal. Autors com Marco Greke[7] inclouen dins el concepte de delicte informàtic tant el delicte tradicional establert a través d'internet (injuries a través de correu electrònic, venda de droga, extorsió o amenaces vehiculades a través d'internet), com el pròpiament dit delicte contra la informàtica, per atacar dades o sistemes informàtics o les xarxes telemàtiques de comunicació, ja sigui bloquejant sistemes, destruint programes, danyant dispositius d'emmagatzematge, alterant dades (frau), destruint-los (sabotatge) o fent-los servir il·lícitament (pirateria, espionatge).

1.2.2 Classificació dels delictes informàtics

Al tractar-se d'un concepte tant ampli, la ciberdelinqüència requereix d'un estudi per determinar-ne una classificació. Velasco Nuñez[8] fa una classificació triple dels delictes informàtics al considerar que existeix la ciberdelinqüència econòmica, la ciberdelinqüència intrusiva i el ciberespionatge.

En primer lloc, la ciberdelinqüència econòmica són aquells delictes econòmics i patrimonials vinculats a la informàtica. Son atacs a béns jurídics patrimonials externs, duts a terme a través de la informàtica, i realitzats amb la intenció de consumar apoderaments o beneficis econòmicament avaluables sobre el patrimoni de terceres persones. A la *Llei Orgànica 10/1995, de 23 de Novembre, del Codi Penal* trobem aquest tipus de ciberdelinqüència qualificat jurídicament en relació a:

- El robatori inutilitzant sistemes de guàrdia criptogràfica. Article 238.5 CP
- L'estafa informàtica, per enginyeria social o informàtica. Article 248.2 CP
- La defraudació de telecomunicacions informàtiques. Article 255 CP
- L'ús no autoritzat de terminals informàtiques. Article 256 CP
- Els virus o danys informàtics. Article 264.2 CP
- Contra la propietat intel·lectual o industrial informàtica. Articles 273-275 CP
- L' espionatge informàtic de secrets d'empresa. Articles 278-280 CP
- La publicitat enganyosa. Article 282 CP
- Les manipulacions en aparells en perjudici del consumidor. Article 283 CP
- Contra el mercat informàtic. Article 286 CP
- El blanqueig informàtic de capitals. Article 301 CP

[7] Marco Greke, *Understanding Cybercrime: Phoenomena, challanges and legal response.* (Ginebra: Telecomunication Developement Sector on International Telecommunication Union, 2006) http://cybercrime-fr.org/wp-content/uploads/2020/04/Understading-Cybercrime-ITU.pdf

[8] Eloy Velasco Nuñez, *Delitos cometidos a través de internet, cuestiones procesales* (Madrid: La Ley, 2010) Pg. 37

- La falsedat documental en suport electrònic. Article 390 CP.

En segon lloc, la ciberdelinqüència intrusiva son aquells delictes atemptats a través de mitjans informàtics contra la intimitat i privacitat. Son aquell tipus de ciberdelicte que ataca al bé jurídic de la privacitat, com un concepte que inclou la intimitat i totes les modalitats protegides a l'article 18 de la Constitució Espanyola: l'honor, la intimitat familiar, la intimitat personal, la pròpia imatge, el domicili, el secret de comunicacions o l'ús correcte de la informàtica. Al Codi Penal Espanyol trobem aquest tipus de ciberdelinqüència qualificat jurídicament en relació a:

- Les amenaces i coaccions informàtiques. Articles 169 i 172 CP
- La distribució de material pornogràfic i pornografia infantil. Articles 186 a 189 CP
- El descobriment i revelació de secrets. Articles 197 a 200 CP
- Les injuries i calumnies informàtiques. Articles 205 a 216 CP
- La cessió sense consentiment de dades alienes. Articles 417, 418 i 423 CP.

Finalment, el ciberespionatge o ciberterrorisme son aquells atacs a través de mitjans informàtics contra interessos que transcendeixen l'esfera d'allò merament individual, els interessos supraindividuals. Son atacs més greus que afecten indiscriminadament als interessos generals de la població per capgirar el sistema polític o de convivència generalment acceptat. Al Codi Penal Espanyol trobem aquest tipus de ciberdelinqüència qualificat jurídicament en relació a:

- La usurpació de funcions públiques a través de correu electrònic. Article 402 CP
- El descobriment o revelació de secrets relatius a la defensa nacional. Articles 598 i 603 CP.

1.2.3 Especificitats dels delictes informàtics

La delinqüència informàtica obté un tractament característic diferent al tractament de la delinqüència convencional, i s'entén molt més el motiu d'aquesta diferència si establim quines són les seves peculiaritats, que també fan que contingui problemàtiques concretes.

Velasco Nuñez[9] els caracteritza, salvant comptades excepcions, per ser delictes que es cometen a distància, de comissió pràcticament instantània en el temps i sense possible reacció immediata de la víctima. Internet té un abast global, és una xarxa a la que es pot accedir des de qualsevol part del món instantàniament, i això permet que els potencials delinqüents puguin actuar des de qualsevol lloc del món, buscar les víctimes més vulnerables en qualsevol lloc i efectuar atacs des

[9] Eloy Velasco Nuñez, *Delitos cometidos a través de internet, cuestiones procesales* (Madrid: La Ley, 2010) Pg. 41

de qualsevol lloc, evitant la persecució gràcies a la deslocalització que ofereixen aquestes activitats cibernètiques.

Normalment son delictes en massa, que afecten a multitud de víctimes, com ara els virus *worm* que infecten indiscriminadament a una pluralitat d'ordinadors. A més, poden generar un gravamen a major escala degut al seu abast internacional. Si parlem de delictes cibereconòmics, com el robatori de dades o les estafes *phishing*, a part de ser infraccions amb víctimes massives, aquestes acostumen a ser desconegudes pel delinqüent. És a dir, l'atacant ignora dades de la víctima, cosa que a vegades fa que sigui difícil saber quina és la intenció del delinqüent. En quant als autors dels ciberdelictes, podem dir que son experts en la xarxa informàtica, normalment qualificats en programació, informàtica, enginyeria i altres carreres tècniques que aporten el coneixement necessari per dur-los a terme ja que es requereix d'un coneixement específic, no els pot dur a terme qualsevol individu amb coneixements bàsics. Aquesta modalitat delictiva facilita també l'anonimat dels seus autors, ja que no és fàcil rastrejar un individu concret, encara que no estigui utilitzant coneixements tècnics específics. La ciberdelinqüència, per tant, permet relacions anònimes entre perpetradors i víctimes.[10]

També s'ha de tenir en compte que l'estructura descentralitzada i no jerarquitzada de la xarxa no és compatible amb l'existència d'òrgans o institucions que controlin tota la informació que circula, i la seva innovació constant permet que hi hagi noves tècniques i eines que burlin les mesures de seguretat que ja existeixen, facilitant així la comissió dels ciberdelictes i complicant que es pugin prevenir. A més, en relació a la prova, és més complicada la seva obtenció degut el caràcter intangible de les dades i de la informació que contenen, i pel caràcter volàtil que permet que es suprimeixin, es transformin o s'ocultin en qualsevol moment, així com les dificultats que comporta la seva conservació i emmagatzematge.

La característica que més interès té per el que ens ocupa és el clar component internacional de la ciberdelinqüència. Els ciberatacs s'inicien en un punt geogràfic que pot ser mòbil, i degut a les característiques que hem mencionat anteriorment, acostumen a afectar a persones ubicades a una pluralitat de localitzacions geogràfiques. La inexistència de fronteres reals és una de les característiques intrínseques d'Internet, que ofereix molts avantatges però també inconvenients en la persecució de les activitats delictives. L'abast global de la ciberdelinqüència implica que el fenomen sigui, quasi per definició, internacional, cosa que comporta dificultat en la persecució dels delictes, aportant reptes legals a la cooperació internacional per perseguir els delictes d'aquestes característiques.

[10] Josefina Quevedo González. "*Investigación y prueba del ciberdelito*". (Tesi Doctoral, Universitat de Barcelona, 2017) Pg. 52 https://www.tdx.cat/bitstream/handle/10803/665611/JQG_TESIS.pdf?sequence=1&isAllowed=y

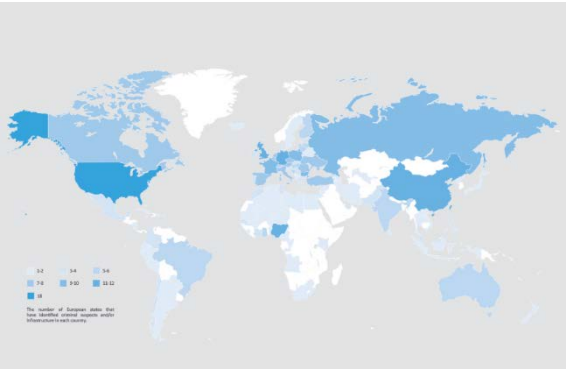
1.3 – Les xifres de la ciberdelinqüència a l'actualitat

Actualment, existeixen uns 2.400 milions d'usuaris connectats a les xarxes, dels quals 540 milions es connecten des d'Europa i uns 29 milions es connecten des d'Espanya. Per entendre la magnitud i repercussió que té la ciberdelinqüència, les víctimes d'aquesta modalitat delictiva perden uns 6 trilions de dòlars com a conseqüència, el cost és enorme. A més, aquesta dada pot anar augmentant anualment. Un estudi de *Cibersecurity Ventures* preveu que aquesta dada augmenti un 15% anualment, i que al 2025 la ciberdelinqüència comporti danys de 10 trilions i mig de dòlars. [11]

La ciberdelinqüència té una gran projecció al futur per dos motius. En primer lloc, les denuncies creixen desmesuradament cada any que passa. En segon lloc, en la majoria dels casos els delinqüents son persones joves, que no arriben als 50 anys d'edat i en molts casos que no arriben ni a la majoria d'edat. Solen ser persones que sempre han conviscut amb les eines tecnològiques i que, per tant, estan acostumats a usar-les. És per tot això que el podem considerar com un crim de caràcter evolutiu, que evoluciona en funció de les últimes tecnologies del moment i és per això també que aquells que el combaten han d'actualitzar-se constantment.

En relació a la classificació explicada anteriorment, la ciberdelinqüència econòmica suposa un 70% dels tipus penals que es denuncien, mentre que la ciberdelinqüència intrusiva suposa un 25%. El ciberespionatge o ciberterrorisme, en canvi, quasi no tenen incidència estadística però això no significa que no tingui impacte ja que per les seves característiques, afecten a la comunitat en conjunt.

L'EUROPOL va dur a terme el 2016 un mapa interactiu en relació a les amenaces geogràfiques i l'activitat relacionada amb la ciberdelinqüència. [12]



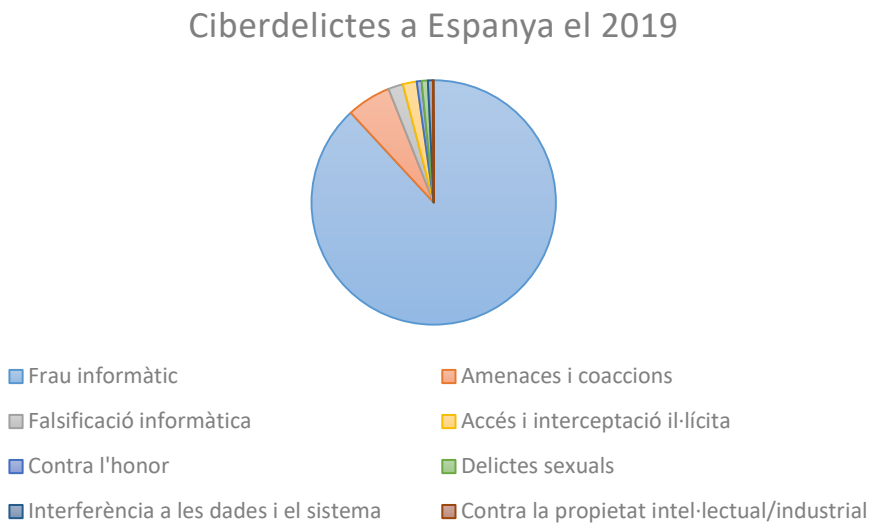
Font: https://www.europol.europa.eu/iocta/2016/distribution.html

[11] Steve Morgan. *2021 report: Cyberwarfare in the C-suite*. (Estats Units: Cybersecurity Ventures, 2021) https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf

[12] "The geographic Distribution of Cybercrime: Cybercrime heatmap" Europol, 2016 https://www.europol.europa.eu/iocta/2016/distribution.html

El mapa mostra el número d'Estats Membres de la UE que han identificat sospitosos o infraestructures criminals als diferents països d'arreu del món. Com podem observar, els Estats Units d'Amèrica, Canadà, Xina, Rússia i Algèria són els països fora de la Unió Europea que més sospitosos o infraestructures criminals tenen que l'han atacat. Dins de la Unió Europea, també podem veure que hi ha un alt nombre de sospitosos procedents d'Estats Membres que ataquen altres Estats Membres. Fent una lectura d'aquest, podem corroborar el caràcter transfronterer de la ciberdelinqüència.

Perquè puguem entendre el gran nombre de ciberdelictes que es duen a terme anualment, segons l'Observatori Espanyol de Delictes Informàtics[13] només a Espanya el 2019 es van produir un total de 218.302 ciberdelictes, dels quals 192.375 són frau informàtic, 12.782 són amenaces i coaccions, 4.275 són falsificació informàtica, 4.004 accés i intercepció il·lícita, 1.422 contra l'honor, 1.774 delictes sexuals, 1.473 interferència en les dades i el sistema i 197 contra la propietat industrial/intel·lectual.



Font: Elaboració pròpia.

[13] "Estadísticas de ciberdelitos en España" Observatorio Español de Delitos Informáticos, 2020. https://oedi.es/estadisticas/

1.4 - La necessitat de cooperació en aquest àmbit i el focus de la nostra anàlisi

La cooperació judicial internacional es pot definir com un mecanisme mitjançant el qual un Estat sol·licita la col·laboració d'un altre Estat per resoldre diferents aspectes d'un procediment judicial. Les normes de cooperació entre Estats, per tant, es creen per la necessitat d'obtenir un resultat determinat al territori d'un altre país, ja sigui la pràctica d'una diligència, l'obtenció d'una declaració o qualsevol altra evidencia que pugui ser d'utilitat per ser incorporada a la investigació.[14] La cooperació judicial internacional, per tant, és una solució als problemes de sobirania i jurisdicció que es podrien produir si es requerís practicar una actuació a territori estranger, ja sigui per part d'autoritats judicials com policials. És així com, mitjançant la coordinació especialitzada d'organismes públics i privats, es duen a terme les diligencies sol·licitades per un determinat Estat sense haver de vulnerar la sobirania de l'altre, i permetent que els resultats obtinguts puguin ser incorporats a un procediment al ser un mecanisme reconegut interestatal i internacionalment. [15]

En el cas de la ciberdelinqüència, els criminals duen a terme molt sovint les seves accions a llocs diferents dels llocs que reben els seus efectes. Tot i així, les lleis nacionals generalment només s'apliquen a un territori específic. És per això que els problemes que hi ha han de resoldre's pel dret internacional, necessitant l'adopció d'instruments legals internacionals. Si no s'articulen els instruments adequats, es pot arribar a produir la impunitat. La dimensió supranacional juga un paper crucial en el tractament de delictes informàtics. Per tant, no hi ha lloc a dubte en que s'han d'executar polítiques conjuntes, generals, que integrin a tots els Estats i sectors de la societat. Weber ens dóna un exemple molt clar de la importància en la cooperació en aquest àmbit. L'any 2000, anteriorment al conveni, un seguit de bancs americans van ser atacats per *hackers* que van accedir a dades confidencials i posteriorment van utilitzar aquesta informació per demanar diners a les víctimes a canvi. El problema greu es va produir quan l'FBI va identificar dos sospitosos a Rússia, i les autoritats russes es van negar a cooperar amb la investigació. En aquell moment, malgrat que els EUA tenien un tractat d'assistència mútua amb Rússia, aquest no especificava la ciberdelinqüència com a un dels crims en que es podien proporcionar assistència, i degut a la falta de col·laboració el delicte va quedar impune.

[14]María Luisa Montenegro, "Cooperación Internacional: Tramitación, obtención de pruebas, e incorporación de pruebas y evidencias" *Revista Jurídica Ministerio Público N°70.* (2017) Pg. 64

[15] Ignacio Novoa Toledo y Leonor Venegas Cruz. *"Herramientas del Convenio de Budapest sobre ciberdelincuencia, y su adecuación a la legislación nacional"*(Tesi Doctoral, Santiago de Chile,2020) Pg. 30

La cooperació entre diferents Estats està directament relacionada amb la solidaritat intercultural, la concurrència recíproca d'idees i solucions, l'ajuda mútua i l'obertura d'altres formes de col·laboració transversal que arribi a noves disciplines. Aquesta generalitat, que és el seu avantatge més gran, també és un inconvenient, ja que aporta dificultat i complexitat a l'hora d'articular procediments participatius que involucrin una gran quantitat d'Estats, cadascun d'ells amb les seves particularitats i interessos, i coordinar tots els elements que estan en joc.[16] És per això que, fins ara, hi ha hagut molt poc èxit a l'hora de crear instruments internacionals en l'àmbit de la ciberdelinqüència, que no van gaire més enllà del Conveni de Budapest del que parlarem més endavant. Malgrat també suposa dificultat coordinar-los, els Estats Membres de la Unió Europea tenen uns objectius, valors i marc legal comuns que han facilitat l'acord en implementar instruments de cooperació relatius a la ciberdelinqüència. El marc legal de la Unió Europea es va desenvolupant progressivament per la protecció d'un mateix objectiu: la seguretat dels ciutadans europeus. Tenint en compte tot el que hem mencionat anteriorment, el nostre anàlisi es centrarà en els instruments de cooperació que existeixen entre els Estats Membres de la Unió Europea.

[16] Andrés Díaz Gómez "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest" *REDUR 8*, 169-203 (Desembre 2010) pg. 20 https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071

CAPÍTOL II – MECANISMES DE COOPERACIÓ JUDICIAL PENAL A LA UNIÓ EUROPEA I CIBERDELINQÜÈNCIA

La lluita contra la ciberdelinqüència forma part de l'Espai de Llibertat, Seguretat i Justícia de la Unió Europea, concretament dins l'àmbit de la Europa de la Justícia, on s'articulen instruments i mecanismes per garantir una cooperació judicial penal. Per lluitar contra la ciberdelinqüència han de treballar conjuntament les institucions europees, els Estats Membres i altres entitats com la EUROPOL. [17]

L'article 82.1 del Tractat de Funcionament de la Unió Europea recull el principi de reconeixement mutu, principi en el que està basada la cooperació judicial penal. Aquest principi, que es basa en la confiança entre els Estats Membres i és el fonament bàsic de la cooperació judicial penal de la Unió Europea, suposa un canvi en les relacions de cooperació dels Estats Membres ja que permet que les resolucions emeses per una autoritat judicial d'un Estat Membre siguin reconegudes i executades pels altres Estats Membres, com a norma general.

La Unió Europea té una visió integradora de les Comunitats Europees sobre la cooperació en matèria delictiva als seus Estats Membres. Aquesta visió parteix del desig comú d'arribar a conclusions similars sobre quin ha de ser el tractament adequat de determinats fenòmens, com ara la ciberdelinqüència. Existeixen multituds d'acords específics en matèria de cooperació en Dret Penal, entre ells el Conveni Europeu d'Assistència Judicial en matèria Penal, el Conveni d'aplicació de l'Acord Schengen i la Decisió Marc relativa a l' Ordre de Detenció Europea.

L'article 276 de la Llei Orgànica del Poder Judicial fa referència a que les peticions de cooperació internacional es tramitaran de conformitat amb el previst als tractats internacionals, normativa de la Unió Europea i lleis espanyoles que resultin d'aplicació. Per tant, la base aplicable està constituïda pels convenis en l'àmbit europeu mencionats anteriorment.

Precisament el Conveni relatiu a l'Assistència Judicial en Matèria Penal entre els Estats Membres de la Unió Europea és d'importància en relació a l'objecte del nostre anàlisi, ja que és la culminació dels esforços per maximitzar l'assistència judicial entre els jutjats dels Estats Membres. El Conveni intenta facilitar l'ajuda judicial mútua entre les autoritats competents dels Estats Membres amb l'objectiu que la cooperació penal sigui més eficaç i ràpida. Es preveuen solucions concretes com ara l'intercanvi d'informació, equips d'investigació conjunta, transmissió de documents, intercepció de comunicacions...

[17] José Enrique Anguita Osuna "Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea" *Revista de Estudios en Seguridad Internacional*, Vol. 4, No.1, 2018. Pg. 107-126 http://dx.doi.org/10.18847/1.7.7

El poder punitiu de l'Estat acaba al límit de la frontera, mentre que la ciberdelinqüència troba en la falta de controls transfronterers avantatges per expandir les seves activitats i aconseguir impunitat. D'aquí sorgeix la necessitat d'adoptar mesures compensatòries que estableixin una cooperació policial i judicial més estreta en matèria penal entre els Estats Membres.

Al Tractat d'Amsterdam es desenvolupa l'espai de llibertat, seguretat i justícia, un dels principals objectius de la UE en que es garanteix la lliure circulació de persones, i les mesures adequades pel control de fronteres exteriors i prevenció i lluita contra la delinqüència. És per això que la cooperació penal és un dels seus elements essencials. L'evolució de la cooperació judicial en matèria penal als tractats ha facilitat l'adopció de nous instruments jurídics, basats sobretot en l'aplicació del principi de reconeixement mutu de decisions judicials.

El legislador, amb l'adopció d'aquestes mesures, vol reduir els espais d'impunitat que sorgeixen com a conseqüència de la creació d'espais sense fronteres. Ho fa establint mecanismes de cooperació entre els Estats i assistència judicial que permeten un correcte desenvolupament en aquells procediments en que hi hagi implicació transfronterera i que l'execució de la sanció sigui efectiva. Això es produeix quan el sospitós ha fugit a un altre Estat Membre o quan el fet delictiu afecta a varis Estats Membres.

Es per això que es requereixen, entre altres, mesures relatives a la detenció i entrega de sospitosos i condemnats, intercanvi d'informació i dades, recollida i enviament de proves i execució de resolucions fermes i condemnes. L'Ordre Europea de Detenció i Entrega i l'Ordre Europea d'Investigació són instruments de cooperació judicial que neixen per satisfer aquestes necessitats. Malgrat aquests instruments no es refereixen particularment als delictes informàtics, la majoria de les seves previsions poden ser aplicades a la comissió d'aquests.

A continuació analitzarem aquells elements de la Cooperació Judicial Penal en l'àmbit de la Unió Europea que tenen un paper més important des de la perspectiva de la ciberdelinqüència.

2.1 - Agència de la Unió Europea per a la Cooperació Judicial Penal (Eurojust)

L'Agència de la Unió Europea per la Cooperació Judicial Penal, d'ara en endavant EUROJUST, s'encarrega de realitzar investigacions i actuacions relatives a la delinqüència greu que afecta com a mínim a dos Estats Membres. El seu paper és promoure la coordinació entre autoritats competents de diferents Estats Membres i facilitar la cooperació judicial entre ells. També dóna suport a les autoritats dels Estats Membres per augmentar l'eficàcia de les seves investigacions i actuacions judicials en l'àmbit de la delinqüència transfronterera. L' EUROJUST és competent, de conformitat amb l'article 3 i l'Annex 1 del *Reglament 2018/1727/UE, de 17 de Novembre, sobre l'Agència de la Unió Europea per la Cooperació Judicial Penal*, de la ciberdelinqüència

entre altres formes de delinqüència greu com ara terrorisme, narcotràfic, blanqueig de capitals, corrupció, o racisme i xenofòbia. Díaz Gómez[18] considera que, en la lluita contra la ciberdelinqüència, la importància d'aquesta agència resideix en el recolzament general a les autoritats competents dels Estats Membres per donar la major eficàcia possible a les seves investigacions i actuacions.

L' EUROJUST publica anualment un informe. Al darrer, de 2019[19], es dedica un apartat exclusivament a la ciberdelinqüència en el que s'apunta que la necessitat de cooperació coordinada ha resultat en un augment de remissions de casos de ciberdelictes a la EUROJUST els últims anys. Incideix en el fet que les ubicacions físiques dels autors i les proves electròniques no es poden determinar amb facilitat i acostumen a estar localitzades en diferents països, que la cooperació amb el sector privat també és vital per combatre la ciberdelinqüència i que les autoritats judicials i policials han de poder intercanviar amb agilitat grans quantitats d'informació i proves electròniques. Els instruments de coordinació de l' EUROJUST suposen una gran diferència, ja que poden propiciar un acostament i servir de punt de referència per coordinar proactivament les investigacions, així com trobar solucions per intercanviar dades i proves dins els marcs jurídics aplicables i ajudar a les autoritats a planificar les accions coordinades.

Per exemplificar la funció de l' EUROJUST en la ciberdelinqüència, exposarem la operació *Cepheus*, una ofensiva internacional contra troians[20] d'accés remot que es van fer amb el control dels ordinadors de víctimes de tot Europa i altres parts del món. Al 2018, les autoritats australianes van investigar aquest instrument de segrest informàtic, que va dur a terme a més de 14.500 ordinadors a tot Europa. EUROJUST, en el seu Grup Especial Conjunt d'Acció contra els Delictes Cibernètics (J-CAT) va recolzar les autoritats australianes i va elaborar una investigació intensiva i coordinada amb les autoritats judicials implicades a tota Europa. Les autoritats van treballar com un sol equip compartint dades de la investigació, agrupant recursos tècnics i humans i van aconseguir identificar les respectives possibilitats jurídiques de cada país. Finalment, al Novembre de 2019, es va dur a terme una operació que va confiscar 59 actius informàtics de Bèlgica, Països Baixos, Polònia, Espanya, Suècia i Austràlia i va aconseguir el total desmantellament d'aquest instrument de segrest informàtic.

---

[18] Andrés Díaz Gómez "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest" *REDUR 8*, 169-203 (Desembre 2010) pg. 17 https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071

[19]Eurojust. *Informe anual de Eurojust 2019.* The Hague: Eurojust, 2019. https://www.eurojust.europa.eu/sites/default/files/Publications/AnnualReport/AR2019_ES.pdf p. 42

[20] Un Troià és un programari maliciós (*malware)* que es presenta a l'usuari com un programa aparentment legítim o inofensiu, però que al executar-lo, brinda a l'atacant accés remot a l'equip que està infectat.

A part de prestar assistència operativa, i mitjançant un seguit de reunions i informes, EUROJUST també fomenta el diàleg sobre temàtiques claus relacionades amb la ciberdelinqüència, com la conferència GLACY, en la que més de 100 experts es van centrar en com tractar les investigacions transfrontereres dels abusos sexuals a menors comesos en línia, o la conferència anual SIRIUS, que va ajuntar més de 300 autoritats policials i judicials i representants de grans empreses per abordar problemes i desafiaments que es plantegen en dur a terme investigacions a través d'internet.

A més, al Fòrum Consultiu Anual de la Eurojust, Fiscals Generals dels Estats Membres van focalitzar la seva atenció a com optimitzar l'intercanvi digital d'informació i l'intercanvi de proves electròniques i van abordar qüestions com la pèrdua de localització i de dades en casos penals degut a la naturalesa transfronterera de la ciberdelinqüència.

2.2 - Ordre Europea de Detenció i Entrega

Tenint en compte els elements intrínsecs de la ciberdelinqüència, sobretot l'element supraestatal que la caracteritza, és important que existeixi un instrument de cooperació que imposi mesures relatives a la detenció i entrega de sospitosos i condemnats quan aquests es troben a diferents Estats Membres, i això és el que fa l' Ordre Europea de Detenció i Entrega.

L' Ordre Europea de Detenció i Entrega, també anomenada Euro ordre, està regulada a la *Decisió Marc 2002/584/JAI del Consell, del 13 de Juliol, relativa a l' Ordre de Detenció Europea i als procediments d'entrega entre Estats Membres*. És un procediment judicial que permet a qualsevol país de la UE detenir una persona acusada d'un delicte a un altre país de la UE o ja condemnada per una sentència ferma. Segons l'article primer de la seva decisió marc, és aquella resolució judicial dictada per un altre Estat Membre en vistes de la detenció i l'entrega per un altre Estat Membre d'una persona buscada per l'exercici d'accions penals o per l'execució d'una pena o una mesura de seguretat privatives de llibertat. És un procediment molt més simplificat que una extradició, basat en el reconeixement mutu de les resolucions judicials, i que té la finalitat última de traslladar forçosament una persona d'un Estat Membre a un altre. En definitiva, permet que la lliure circulació a la UE no sigui un problema perquè la justícia actuï i faciliti els tràmits pel seu compliment més enllà de les seves fronteres.

L'article segon de la Decisió Marc estableix que per poder dictar una Ordre Europea de Detenció i Entrega hi ha d'haver un fet penat a la llei de l'Estat emissor amb una pena o mesura privativa de llibertat de mínim dotze mesos o una condemna d'una pena o mesura de seguretat no inferior a quatre mesos de privació de llibertat.

També estableix que donaran lloc a l'entrega els delictes establerts a l'article 2.1 de la Decisió Marc sempre que es castiguin a l'Estat Membre emissor amb una pena o mesura de seguretat privativa de llibertat d'un màxim de mínim tres anys. Entre els delictes que es destaquen a l'Article 2.1 trobem els delictes d'alta tecnologia, en particular el delicte informàtic. La particularitat dels delictes que estan llistats al segon apartat de l'article, i per tant entre ells la ciberdelinqüència, és que no tenen control de la doble tipificació. És a dir, l'entrega no estarà condicionada a que els fets que justifiquen l'emissió de l' Euro Ordre siguin constitutius de delicte al dret de l'Estat Membre d'execució. En canvi, en tots aquells delictes que no estan esmentats al segon apartat de l'article, es podrà supeditar al requisit de doble tipificació l'entrega.

2.2.1 Àmbit d'aplicació material

Les resolucions que provoquen el manament de detenció i que per tant fonamenten que una autoritat judicial emeti una Ordre Europea de Detenció i Entrega són :

- Sentències fermes: que condemnin una pena o mesura de seguretat privativa de llibertat la duració de la qual sigui superior a quatre mesos o que el temps que quedi per complir la mateixa sigui també superior a quatre mesos. En cas de ciberdelinqüència, que condemnin a l'Estat Membre emissor amb una pena o mesura de seguretat privativa de llibertat d'un màxim de mínim tres anys. Alonso Moreda[21] considera que s'haurien de considerar senzillament sentències, ja que aquestes no han de ser fermes sinó definitives. A Espanya, segons l'Article 35 del Codi Penal, mesura de seguretat privativa de llibertat pot ser presó, presó permanent revisable, localització permanent o responsabilitat personal subsidiària per no haver pagat una multa.

- Ordres de detenció interna o internacional: A Espanya les sol emetre el jutge instructor, tot i que en determinats supòsits també pot fer-ho el Ministeri Fiscal en tant a ordres de detenció preventives. Si el jutge o tribunal coneix la localització del subjecte objecte de cerca al moment d'emetre l'ordre, i es tracta d'un Estat de la UE, n'hi ha prou amb emetre una Euro Ordre. En canvi, si no es coneix la localització, s'haurà d'emetre una ordre de detenció interna i internacional, en la que posteriorment es podrà fonamentar l' Ordre Europea si el subjecte resulta estar en un Estat Membre.

- Altres resolucions judicials executives que impliquin privació de llibertat dictada en procediment penal per un delicte que tingui prevista una pena de duració màxima de

[21] Nicolás Alonso Moreda, *Cooperación Judicial en Materia penal en la Unión Europea: La "Euro Orden", Instrumento privilegiado de cooperación.* (Pamplona: Aranzadi, 2016) pg. 430

mínim dotze mesos a l'ordenament jurídic de l'Estat emissor. En cas de ciberdelinqüència, que impliquin a l'Estat membre emissor una pena o mesura de seguretat privativa de llibertat d'un màxim de mínim tres anys. A Espanya, poden ser tant una interlocutòria pel que s'acorda la llibertat provisional o presó provisional. Les dues resolucions tenen per objecte l'adopció d'una mesura cautelar que consisteix en la limitació de la llibertat d'ambulatòria de l'imputat.

2.2.2 Forma i Contingut

La forma que s'ha de seguir és el formulari que es troba a l'annex de la Decisió Marc. És un títol judicial europeu homologat, igual i únic a tots els Estats Membres i que agilitza el procediment al ser senzill i fàcil d'utilitzar. Obligatòriament l' Euro Ordre ha d'incloure la identitat i nacionalitat de la persona buscada, les dades de l'autoritat judicial emissora, la naturalesa i tipificació del delicte, una descripció de les circumstàncies en que es va cometre el delicte, la indicació de la existència de sentència ferma, ordre de detenció o altra resolució judicial executiva, la pena dictada o escala de penes previstes i altres conseqüències del delicte si és possible. La transmissió d'informació i el contingut no és només estrictament amb el formulari perceptiu, sinó que al llarg del procediment hi poden haver més intercanvis d'informació.

2.2.3 Autoritats responsables

L'adopció de les decisions rellevants del procediment de detenció i entrega corren a càrrec de les autoritats judicials exclusivament. L'article 6 de la Decisió Marc dóna marge al dret intern de cada Estat Membre perquè estableixi les autoritats judicials competents per emetre i executar una Euro Ordre, entenent que el Ministeri Fiscal també forma part d'autoritat judicial. A Espanya, i segons l'article 35 de la *Llei 3/2003, de 14 de Març, sobre l' Ordre Europea de Detenció i entrega*, la competència per emetre Euro Ordres és, amb caràcter general, dels jutges i tribunals de jurisdicció penal. Per altra banda, l'autoritat judicial d'execució són els Jutjats Centrals d'Instrucció de l'Audiència Nacional i el Jutge Central de Menors.

A més de les autoritats judicials competents, segons l'article 7, cada Estat Membre pot designar una altra autoritat central per auxiliar-les, que no tenen perquè ser judicials. A Espanya, l'Autoritat Central única és el Ministeri de Justícia. En concret, ho és la Subordinació General de Cooperació Jurídica Internacional del Ministeri de Justícia.

2.2.4 Procediment d'emissió

En cas que l'autoritat judicial d'emissió no conegui la localització de la persona buscada, s'introduirà una descripció al Sistema d'Informació Schengen . Si no hi ha aquesta possibilitat, també es pot acudir als serveis de la INTERPOL. Si la descripció va acompanyada amb el contingut que s'exigeix per l' Euro Ordre descrit anteriorment, serà equivalent a una Ordre Europea de Detenció i Entrega. Tanmateix, també ha de quedar clar que aquesta descripció al SIS és una detenció preventiva, de manera que posteriorment s'haurà d'enviar la documentació habitual i per les vies de transmissió habituals en un termini el màxim de breu possible. S'ha de tenir en compte que la persona reclamada pot ser posada en llibertat si no es realitza aquesta remissió en el termini establert.

En cas que l'autoritat judicial d'emissió conegui la localització de la persona buscada, es podrà comunicar directament a l'autoritat judicial d'execució l' Euro Ordre, segons l'article novè de la Decisió Marc. Si l'autoritat judicial d'emissió no coneix quina és l'autoritat judicial d'execució competent, haurà de fer les indagacions necessàries a través del punts de contacte de la Xarxa Judicial Europea. Si l'autoritat que rep l' Euro Ordre no és competent, no es retornarà aquesta sinó que s'ha de transmetre d'ofici a l'autoritat competent, i informar a l'autoritat emissora. A més, també podrà utilitzar el SIS i INTERPOL, ja que són alternatives que serveixen en qualsevol circumstància. La transmissió de l' Euro Ordre es pot dur a terme per qualsevol mitjà fiable que pugui deixar constància escrita i es pugui autentificar, també en funció dels requisits de cada Estat Membre.

2.2.5 Procediment d'execució

Quan l'autoritat judicial d'execució competent rep l' Euro Ordre, ha de fer un examen preliminar. Primer ha de comprovar que està traduïda a algun dels idiomes oficials de l'Estat d'execució. Si no és el cas, el procediment quedarà suspès fins que s'esmeni l'error. A continuació, l'autoritat judicial ha de comprovar l'autenticitat de l' Euro Ordre i si recull tota la informació necessària requerida. Si es requereix d'informació complementària, sempre es podrà sol·licitar a l'Estat emissor.

Després de l'examen preliminar, si aquest ha estat favorable, s'ordenarà la detenció de la persona. La Decisió Marc es remet al dret intern dels Estats Membres per regular-la. A Espanya, si l' Euro Ordre és rebuda pel Jutjat Central d'Instrucció de l'Audiència Nacional, el jutge ordenarà la detenció mitjançant interlocutòria, mentre que si és rebuda a través del SIS o INTERPOL, la policia pot procedir directament a la detenció, però amb la immediata disposició judicial al Jutjat Central D'Instrucció.

Un cop posat a disposició judicial, l'autoritat judicial haurà d'informar al detingut, a part de dels seus drets, de l'existència de l' Euro Ordre, del seu contingut, i de la possibilitat de consentir la seva entrega a l'autoritat judicial emissora. En cas que la persona reclamada consenti la seva entrega i no hi hagi causes de denegació, l'entrega s'ha d'acordar mitjançant interlocutòria a l'Estat d'emissió. En cas que no la consenti, el Jutge Central d'Instrucció convocarà les parts i el Ministeri Fiscal per celebrar una vista, en el termini màxim de tres dies, i procedirà a escoltar les parts sobre la concurrència de causes de denegació o condicionament d'entrega.

Una vegada s'ha detingut la persona, i mentre no procedeix l'entrega, l'autoritat judicial d'emissió pot reclamar dues mesures, que es poden prendre en qualsevol moment del procediment d'execució des de la detenció fins a la decisió d'entrega definitiva: la prestació de declaració del reclamat o demanar el trasllat temporal d'aquest a l'Estat d'emissió. [22]

La primera, la prestació de declaració al reclamat, implica que l'autoritat judicial d'emissió pot traslladar-se a l'Estat d'execució per prestar-li declaració, facilitant així una declaració el més aviat possible del detingut. L'entrega temporal es pot sol·licitar fins i tot abans que l'autoritat d'execució s'hagi pronunciat sobre l'entrega definitiva, per dur a terme diligències penals o la celebració d'una vista oral. Amb la mateixa finalitat, també es pot sol·licitar l'entrega temporal si l'autoritat d'execució, després d'haver acordat l'entrega de la persona reclamada, decideix suspendre-la per estar pendent la celebració d'un judici o compliment d'una pena imposada per un fet diferent al que motiva l' Euro Ordre a l'Estat d'execució. [23]

La segona, el trasllat temporal del reclamat a l'Estat d'emissió, permet la celebració de la vista d'un procediment a l'Estat d'emissió, evitant així que s'hagi de posposar fins la materialització definitiva de l'entrega.

2.2.6 Motius de no execució

Per no executar una Euro Ordre, trobem motius obligatoris i motius facultatius.[24]

L'autoritat judicial d'execució estarà obligada a denegar l'execució en tres casos concrets establerts al tercer article de la Decisió Marc. En primer lloc, quan el delicte estigui cobert per amnistia de l'Estat Membre d'execució. En segon lloc, quan la persona buscada ja ha sigut jutjada pels mateixos fets en un Estat Membre i en cas de condemna aquesta hagi siguda executada o

[22]Nicolás Alonso Moreda, *Cooperación Judicial en Materia penal en la Unión Europea: La "Euro Orden", Instrumento privilegiado de cooperación.* (Pamplona: Aranzadi, 2016) pg. 442-449

[23] Maria Teresa Armenta Deu, *Lecciones de Derecho Procesal* Penal (Madrid: Marcial Pons, 2019) pg. 132

[24]Nicolás Alonso Moreda, *Cooperación Judicial en Materia penal en la Unión Europea: La "Euro Orden", Instrumento privilegiado de cooperación.* (Pamplona: Aranzadi, 2016) pg. 451-544

s'estigui executant. En tercer lloc, quan la persona objecte de l' Euro Ordre no pugui ser considerada penalment responsable dels fets en els que es basa l' Euro Ordre per raó de la edat.

L'autoritat judicial d'execució podrà denegar l'execució facultativament en set casos establerts al quart article de la Decisió Marc.

En primer lloc quan, en aquells delictes que es pot supeditar l'entrega al principi de doble incriminació, no es compleixi el principi. Per tant, aquest motiu no es pot aplicar en ciberdelinqüència. En segon lloc, per litispendència, quan la persona objecte de l' Euro Ordre ja està sotmesa a un procediment penal a l'Estat membre d'execució pel mateix fet. En tercer lloc, per Ne Bis In Idem impropi, quan les autoritats judicials d'execució decideixin no incoar acció penal per la infracció, finalitzar-la o quan la persona buscada tingui resolució definitiva sobre els mateixos fets i obstaculitzi l'exercici de diligencies penals. En quart lloc, per prescripció, tant del delicte o de la pena segons l'Estat Membre d'execució. En cinquè lloc, per Ne Bis In Idem en sentit estricte, quan la persona buscada ha sigut jutjada definitivament pels mateixos fets per un tercer Estat. En sisè lloc, quan l' Euro Ordre s'hagi dictat contra una persona buscada que sigui nacional o resident de l'Estat Membre d'execució o en sigui habitant i es comprometi a executar ell mateix la pena o mesura. En setè lloc, relacionats amb el principi de territorialitat de la llei penal, quan l' Euro Ordre contempli infraccions que el dret de l'Estat d'execució consideri que s'han comés al territori de l'Estat d'execució, o s'hagin comés fora de l'Estat membre d'emissió i el d'execució no permeti la persecució per les mateixes infraccions quan s'hagin comés fora del seu territori.

2.2.7 Entrega i els seus efectes

La decisió sobre l'entrega s'ha d'adoptar deu dies després d'haver-se manifestat consentiment si el detingut dona consentiment a la seva entrega i en seixanta dies des de la detenció si no manifesta consentiment. S'ha de deixar clar que aquests terminis es refereixen a la decisió d'entrega, no a l'entrega material. Les legislacions nacionals, tanmateix, poden concretar els tràmits i la seva duració, ja que la Decisió Marc només dona límits màxims. La llei espanyola manté aquests mateixos terminis.[25]

Una vegada hagi pres la decisió, l'autoritat judicial d'execució notificarà immediatament l'autoritat judicial emissora del sentit de la decisió. En cas que la decisió sigui la denegació de l'entrega, s'haurà de justificar. En canvi, si és conforme a l'entrega, també es donarà aquella informació relativa a la duració de la privació de llibertat que serà deduïda de la pena o mesura de seguretat privativa de llibertat que se li imposi.

[25] Nicolás Alonso Moreda, *Cooperación Judicial en Materia penal en la Unión Europea: La "Euro Orden", Instrumento privilegiado de cooperación.* (Pamplona: Aranzadi, 2016) pg. 575-623

Una vegada s'ha adoptat per l'autoritat judicial d'execució la decisió definitiva sobre l'entrega del reclamat, l'entrega material s'ha de realitzar el més aviat possible i, en tot cas, dins els deu dies següents a l'adopció de la decisió definitiva, que podrà prorrogar-se en cas que no sigui possible l'entrega en deu dies per circumstàncies alienes al control dels Estats Membres afectats.

Segons Alonso Moreda[26], existeixen tres efectes principals de l'entrega.

En primer lloc, el principi d'especialitat, que suposa que la persona entregada per un procediment d'una EuroOrdre no podrà ser processada, condemnada o privada de llibertat sense el consentiment de l'Estat que realitza l'entrega per fets comesos abans de la seva entrega diferents als que l'han motivat. Tanmateix, això és la norma general, i a la Decisió Marc trobem moltes excepcions a aquest principi que fan pensar que es tracta d'un criteri residual. El Tribunal de Justícia ha establert els criteris que permeten determinar si la persona entregada és acusada d'una infracció diferent de la que va motivar la seva entrega. Es basa en la comprovació de si, segons la tipificació jurídica que s'ha fet a l'Estat d'emissió, els elements constitutius son els mateixos pels quals la persona ha sigut entregada i si existeix correspondència suficient entre les dades que figuren a l' Ordre de Detenció Europea i els mencionats a l'acte del procediment posterior. El TJUE admet canvis en les circumstàncies de temps i de lloc sempre que derivin d'elements obtinguts durant el procediment seguits a l'Estat Membre d'emissió en relació als comportaments referits a l' Euro Ordre, i no alterin la naturalesa de la infracció ni impliquin motiu de no execució.

Un altre efecte de l'entrega és l'entrega o extradició ulterior, que la Decisió marc planteja en tres supòsits. En primer lloc, davant els casos en que una persona sobre la que recau una Euro Ordre que es troba a l'Estat d'execució després d'una prèvia extradició des d'un tercer estat, serà necessari el consentiment de l'Estat que l'ha extradit anteriorment per procedir a una nova entrega. En segon lloc, davant els casos en que una persona que és reclamada a través d'una sol·licitud d'extradició i que es troba a l'Estat requerit després d'una prèvia entrega en virtut d'una Euro Ordre, serà necessari el consentiment de l'autoritat competent de l'Estat membre que va procedir a la seva entrega. En tercer lloc, davant els casos en que una persona reclamada mitjançant Euro Ordre i que es trobi en l'Estat d'execució en virtut d'una entrega fruit d'una altre Euro Ordre anterior, com a norma general es requereix el consentiment de l'autoritat judicial d'execució perquè l'autoritat judicial d'emissió pugui procedir a una nova entrega, encara que existeixen excepcions que fan que no sigui necessari.

Finalment, l'entrega d'objectes també és un efecte de l'entrega, que suposa l'entrega d'aquells objectes que puguin servir com a prova o que posseeixi la persona reclamada com a resultat del

[26] Nicolás Alonso Moreda, *Cooperación Judicial en Materia penal en la Unión Europea: La "Euro Orden", Instrumento privilegiado de cooperación.* (Pamplona: Aranzadi, 2016) pg. 613-623

delicte. S'ha de tenir en compte que aquesta obligació d'entrega subsisteix encara que l' Euro Ordre no es pugui executar degut a la mort o evasió de la persona buscada. Està orientada principalment a aquells casos en els que la base de l' Euro Ordre es basi en la finalitat d'exercitar accions penals.

2.3 – Ordre Europea d'Investigació

L' Ordre Europea d'Investigació en matèria penal és de gran importància per la investigació de la ciberdelinqüència ja que estableix un règim únic per obtenir proves en casos de dimensió transfronterera, que com hem anat emfatitzant al llarg de l'anàlisi suposa una de les característiques més rellevants d'aquesta modalitat delictiva.

L' Ordre Europea d'Investigació, amb l'acrònim OEI, està regulada a la *Directiva 2014/41/CE del Parlament Europeu i el Consell, relativa a l'Ordre Europea d'Investigació en matèria penal.* Aquesta Directiva, basada en el principi de reconeixement mutu, neix amb l'objectiu de transformar el sistema tradicional de la obtenció i trasllat dels elements de la prova entre els Estats Membres. Davant la ineficàcia anterior de diferents instruments normatius aplicats al mateix àmbit material, el legislador ha optat per un plantejament basat en un únic instrument processal que pretén atorgar més agilitat, tant a la obtenció de la prova com a la seva transmissió entre diferents Estats Membres.[27] A diferència de l'exhort europeu d'obtenció de proves, a l'OEI es poden no només sol·licitar proves ja existents a l'Estat d'execució, sinó que també es pot sol·licitar qualsevol mesura d'investigació.

L' OEI es pot definir com aquella resolució que emesa per un òrgan judicial té com a finalitat que a l'Estat d'execució es duguin a terme una o diverses mesures d'investigació, podent ser utilitzada tant per la obtenció de proves que ja tenen les autoritats competents a l'Estat d'execució com per obtenir mesures d'assegurament de fonts de prova. Igual que l' Euro Ordre, es tracta d'un autèntic títol executiu europeu. [28] La sol·licitud i pràctica de qualsevol mesura d'investigació es pot dur a terme en qualsevol fase del procediment penal, inclosa la vista.

Podem concloure que a través de l' OEI es pot sol·licitar tant la obtenció de proves que ja existeixen com la realització de mesures d'investigació dirigides a obtenir noves proves i fins i tot que s'acordi una mesura cautelar per assegurar la prova. Aquesta última significa que l'Estat

[27] Mercedes Llorente Sánchez-Arjona. *La Orden Europea de Investigación y su incorporación al derecho español.* (Valencia: Tirant Lo Blanch, 2020) pg. 52

[28] Mercedes Llorente Sánchez-Arjona. *La Orden Europea de Investigación y su incorporación al derecho español.* (Valencia: Tirant Lo Blanch, 2020) pg. 55

d'emissió pot emetre una OEI amb la finalitat d'adoptar qualsevol mesura d'investigació destinada a impedir de forma cautelar la destrucció, transformació, desplaçament, transferència o alienació d'un objecte que pugui ser prova. [29]

2.3.1 Àmbit d'aplicació material

L' OEI té un àmbit d'aplicació material bastant ampli, ja que inclou totes les mesures d'investigació amb l'excepció, tal com estableix l'article tercer de la Directiva, de la creació d'un equip conjunt d'investigació i la obtenció de proves d'aquest equip. El Considerant 8 de la Directiva estableix que l' OEI té un àmbit horitzontal pel que s'han d'aplicar totes les mesures d'investigació dirigides a la obtenció de proves. L'excepció dels equips conjunts d'investigació és perquè aquests es regeixen per la *Decisió Marc 2002/465/JAI del Consell, de 13 de Juny de 2002, sobre equips conjunts d'investigació.* Igualment, també s'exclou

A part del règim general d'obtenció de proves, també es recullen específicament mesures d'investigació concretes que requereixen normes addicionals: el trasllat temporal de detinguts, la compareixença per videotrucada, conferència telefònica o altres mitjans, la informació sobre comptes bancaris i altres tipus de comptes financers, la informació sobre operacions bancaries i altres tipus d'operacions financeres, les mesures d'investigació que impliquin obtenció de proves a temps real, continuadament i durant un determinat període de temps, les investigacions encobertes i la intervenció de les telecomunicacions.

L'aplicació de l' OEI es produeix fonamentalment en el marc de procediments penals, però també es poden produir en l'àmbit de procediments administratius. L' OEI es pot emetre, segons l'article quart de la Directiva, a través dels següents procediments:

- Un procediment penal incoat per una autoritat judicial pels fets constitutius de delicte segons el dret intern de l'Estat d'emissió.

- Un procediment incoat per una autoritat administrativa per fets tipificats al Dret intern de l'Estat d'emissió per ser infraccions de disposicions legals en aquells casos que la decisió pugui donar lloc a un procediment davant una autoritat jurisdiccional en matèria penal.

- Un procediment incoat per una autoritat judicial per fets tipificats al Dret intern de l'Estat d'emissió per ser infraccions de disposicions penals en aquells casos que la decisió pugui donar lloc a un procediment davant una autoritat jurisdiccional en matèria penal.

[29] Lídia Domínguez Ruiz. *La Orden Europea de Investigación. Análisis legal y Aplicaciones Prácticas.* (Valencia: Tirant lo Blanc, 2019) Pg. 59

2.3.2 Forma i contingut

L' OEI s'ha d'emetre utilitzant el formulari establert a l'Annex A de la Directiva, seguint el mateix paràmetre que l' Euro Ordre. Aquest formulari haurà d'incloure obligatòriament les dades de l'autoritat d'emissió, l'objecte i motius de l' OEI, la informació necessària sobre la persona o persones afectades, la descripció de la conducta delictiva que és objecte d'investigació o procediment, les disposicions aplicables del Dret Penal de l'Estat d'emissió i finalment la descripció de la mesura o mesures d'investigació que es sol·liciten i les proves que es volen obtenir.

2.3.3 Autoritats responsables

Partint de la diversitat de sistemes processals que integren la Unió Europea, la Directiva contempla en el seu article segon com a autoritat d'emissió no només al jutge instructor i ministeri fiscal, sinó també qualsevol altra autoritat competent que actuï en qualitat d'autoritat d'investigació en procediments penals i pugui ordenar la obtenció de proves conforme el seu ordenament jurídic. La condició perquè puguin ser autoritat d'emissió aquestes autoritats competents alternatives és que l' OEI sigui validada per un òrgan jurisdiccional, fiscal o magistrat instructor de l'Estat d'emissió.

Per tant, i segons Llorente[30], s'acull a un concepte d'autoritat judicial en sentit ampli, que inclou tant a jutges com membres del Ministeri Fiscal. Igualment, qualsevol altra autoritat competent també pot actuar com autoritat d'emissió. Això podria ser la policia o autoritat administrativa, encara que sempre i en tot cas haurà de ser validada per un òrgan jurisdiccional, fiscal o magistrat instructor.

L'autoritat competent per reconèixer i executar l' OEI és aquella que té competència per reconèixer-la i els procediments aplicables en un cas intern similar, encara que requereixin una autorització judicial de l'Estat d'execució quan es disposi en la legislació interna. Sense perjudici d'això, cada Estat Membre pot designar una autoritat central per assistir les autoritats competents. Per tant, es deixa en mans de cada Estat Membre escollir les autoritats que tindran competència en materia de reconeixement i execució i designació d'autoritats centrals. A Espanya, i segons els apartats 2 i 3 de l'Article 187 de la *Llei 23/2014, de 20 de Novembre, de Reconeixement Mutu de resolucions penals a la Unió Europea*, l'autoritat d'execució és el Ministeri Fiscal sempre que no hi hagi cap mesura limitativa de Drets Fonamentals, que després haurà de ser remesa al jutge o tribunal competent: els Jutges d'Instrucció o de Menors, els Jutges Centrals d'Instrucció o els

[30] Mercedes Llorente Sánchez-Arjona. *La Orden Europea de Investigación y su incorporación al derecho español.* (Valencia: Tirant Lo Blanch, 2020) pg..135

Jutges Centrals d'allò penal o central de menors. Per altra banda, a l'ordenament espanyol la competència d'autoritat central la ostenta el Ministeri de Justicia segons la mateixa llei espanyola, però només assumint la funció d'assistència a autoritats competents, i no la de transmissió i recepció administratives, que du a terme el Ministeri Fiscal.

2.3.4 Procediment d'emissió

Tal i com indica l'article sisè de la Directiva, només es pot emetre una OEI en quan es compleixin dos pressupòsits. En primer lloc, que aquesta sigui necessària i proporcionada a l'objectiu del procediment. En segon lloc, que la mesura d'investigació que es requereixi també s'hagués dictat en les mateixes condicions per un cas intern similar. Aquestes condicions, que s'han d'avaluar per l'autoritat d'emissió, es revisaran per l'autoritat d'execució conforme els paràmetres de la seva legislació interna.

Si l' Ordre és emesa per un jutge, tindrà el format d'interlocutòria, mentre que si és emesa pel Ministeri Fiscal, tindrà format de decret. És important també destacar que es pot sol·licitar l'emissió tant d'ofici com per instància de part. Per tant, pot ser sol·licitada per la defensa per obtenir proves exculpatòries

L' OEI es transmetrà per l'autoritat d'emissió a l'autoritat d'execució per qualsevol mitjà que pugui deixar constància escrita en condicions que permetin a l'Estat d'execució establir-ne l'autenticitat..

Si no es coneix la identitat de l'autoritat d'execució, l'autoritat d'emissió realitzarà les investigacions pertinents per obtenir-ne la informació, entre altres a través dels punts de contacte de la Xarxa Judicial Europea, EUROJUST i el Ministeri de Justícia. En el cas de tractar-se de quelcom relacionat amb ciberdelinqüència, també es podrà ajudar per la Xarxa Judicial Europea contra la Ciberdelinqüència, l'Agència de la Unió Europea de Ciberseguretat, el Centre Europeu de Ciberdelinqüència i el Grup d'acció conjunta contra la ciberdelinqüència.

2.3.5 Procediment de reconeixement i execució

L'autoritat d'execució reconeixerà una OEI i s'assegurarà que aquesta s'executi de la mateixa manera que s'hagués executat si s'hagués ordenat pel mateix Estat d'execució, a no ser que decideixi invocar algun dels motius de denegació o d'ajornament. Igualment, l'autoritat d'emissió pot demanar que autoritats del seu Estat assisteixin a l'execució de l' OEI per recolzar les autoritats de l'Estat d'execució. Aquesta autoritat de l'Estat d'emissió no tindrà cap tipus de competència coercitiva a l'Estat d'execució i estaran sotmesos pel dret del mateix.

La resolució de reconeixement o execució s'adoptarà i la mesura d'investigació es durà a terme amb la mateixa celeritat i prioritat que els casos interns similars. La resolució del reconeixement s'ha de dur a terme en un termini màxim de trenta dies després de la recepció de l' OEI, mentre que la execució en un termini màxim de noranta dies després de l' adopció de la resolució, segons el dotzè article de la Directiva. Tanmateix, en cas que la gravetat del delicte o altres circumstancies ho requereixin, el termini podrà haver de ser més curt.

Una vegada l' OEI s'ha executat, es procedirà al trasllat de les proves obtingudes a l'Estat d'emissió. En el moment del trasllat, s'indicarà si es sol·licita que es retornin les proves a l'Estat d'execució. Si els documents que es traslladen resulten rellevants per altres procediments, l'autoritat d'execució podrà traslladar temporalment les proves amb la condició que es retornin quan deixin de ser necessàries per l'Estat d'emissió, o en qualsevol altre moment en que sigui convenient.

2.3.6 Substitució de mesures d'investigació i motius de denegació i d'ajornament de l'execució

Si l'Estat d'execució considera que hi ha una mesura que obtindrà el mateix resultat a través de mitjans menys invasius pels drets que es puguin veure afectats, substituirà la mesura d'investigació indicada a l' OEI, segons l'article desè de la Directiva. També ho farà en cas que la mesura indicada a l'OEI no existeixi al Dret nacional de l'Estat d'execució o no s'apliqui en un cas intern similar.

En canvi, podrà denegar l'execució, en els paràmetres de l'article onzè:

- Si existeix una immunitat o privilegi al Dret de l'Estat d'execució que faci impossible executar l' OEI

- Si la seva execució podés lesionar interessos de seguretat nacional

- Si no s'hagués autoritzat per un cas intern similar a l'Estat d'execució en procediments administratius o incoats per autoritats judicials sense ser procediments penals encara

- Si l'execució fos contraria al Ne Bis In Idem

- Si l' OEI es refereix a un delicte comés no a l'Estat d'emissió sinó a l'Estat d'execució i no es considera delictiu conforme la llei interna

- Si l'execució podria ser incompatible amb les obligacions de l'Estat Membre d'execució

- Si la conducta no és constitutiva de delicte segons l'Estat d'execució i no forma part d'una llista llarga de delictes establerts a l'Annex D de la Directiva si a l'Estat d'emissió és punible amb una pena de màxim un mínim de tres anys. Els delictes informàtics formen part d'aquesta llista, de manera que aquest no pot ser un motiu de denegació d'execució en cas de ciberdelinqüència.

- Si la mesura sol·licitada només està disponible per una determinada categoria de delictes.

També hi ha la possibilitat de l'ajornament del reconeixement o l'execució, si l'execució podés perjudicar una investigació penal o actuacions judicials en curs o els objectes, documents o dades que s'han d'obtenir estan sent utilitzades en altres procediments. S'ha de tenir en compte que, en aquest cas, tan aviat com deixin d'existir aquests motius, l'autoritat d'execució haurà d'adoptar immediatament les mesures d'execució.

2.3.7 Normes addicionals per determinats tipus de mesures

Com ja hem assenyalat, l' OEI crea un règim únic i general per la obtenció de proves, però la Directiva també recull específicament mesures d'investigació concretes que requereixen normes addicionals. A aquests preceptes es recullen requisits propis per l'adopció i pràctica de cada una de les mesures mencionades, i s'afegeixen més motius de denegació.

En primer lloc trobem el trasllat temporal de detinguts per dur a terme una mesura d'investigació. Aquest trasllat es pot dur a terme tant a l'Estat d'emissió com a l'Estat d'execució. Si es du a terme a l'Estat d'emissió des de l'Estat d'execució, s'afegeixen com a motius de denegació que el detingut no doni el seu consentiment i que el trasllat pugui causar la prolongació de la detenció del detingut. Els dos Estats acordaran les disposicions pràctiques relatives al trasllat temporal, com ara les condicions de la detenció i les dates en que s'haurà de retornar. La persona que es trasllada no pot ser detinguda a l'Estat d'emissió per actes anteriors a la seva sortida de l'Estat d'execució, a no ser que es quedi al territori quinze dies més dels necessaris o l'hagi abandonat i retornat. Per descomptat, el temps de detenció a l'Estat d'emissió es deduirà del període de privació de llibertat. Si el trasllat temporal es du a terme a l'Estat d'execució des de l'Estat d'emissió, l'únic motiu de denegació nou serà que el detingut no doni el seu consentiment, mentre que la resta procedirà de la mateixa manera que el trasllat a l'Estat d'emissió.

En segon lloc trobem la compareixença per mitjans tècnics, que pot ser per videotrucada o conferència telefònica. En cas de videotrucada, es podrà dur a terme si la persona que es troba a l'Estat d'execució ha de ser escoltat com a testimoni o pèrit per l'Estat d'emissió. Els motius de denegació complementaris són que l'investigat o acusat no doni el seu consentiment i que l'execució de la mesura sigui contraria als principis fonamentals del Dret de l'Estat d'execució.

Igualment, les autoritats dels dos Estats es posaran d'acord per establir les disposicions pràctiques. Tanmateix, hi ha unes normes que s'hauran de seguir: durant la declaració hi ha d'haver un representant de l'Estat d'execució, la compareixença es durà a terme davant directament davant l'autoritat de l'Estat d'emissió, en cas que es necessiti intèrpret l'Estat d'execució l'ha de proporcionar i s'informarà als investigats o acusats dels drets processals que tenen. Un cop finalitzada la declaració, l'autoritat d'execució haurà de prendre acta. En cas de conferència telefònica, es podrà dur a terme en el mateix sentit, i malgrat no té els motius de denegació especials de la videotrucada, la resta de condicions són les mateixes.

En tercer lloc trobem la informació bancària i financera, que pot ser sobre comptes bancaris i altres tipus de comptes financers o sobre operacions bancaries i altres tipus d'operacions financeres. En relació a comptes bancaris i financers, es podrà emetre una OEI per determinar si una persona física o jurídica objecte d'un procediment penal és titular o posseeix el control d'un compte a un banc localitzat al territori de l'Estat d'execució, i obtenir-ne les dades. A la mateixa OEI s'ha d'indicar perquè es considera que la informació sol·licitada és fonamental pel procediment penal, i s'ha d'incloure tota la informació que pugui facilitar l'execució. En relació a operacions bancaries i financeres, es podrà emetre EOI per obtenir dades de comptes bancaris específics i operacions bancaries que s'hagin efectuat dins un termini concret pels comptes indicats. Igualment s'haurà d'explicar a l' OEI les raons per les que la informació sol·licitada és pertinent pel procediment penal.

En quart lloc trobem aquelles mesures d'investigació que impliquen la obtenció de proves a temps real, de manera continuada i durant un determinat període de temps. En aquestes mesures, que són de gran importància en la ciberdelinqüència i per tant s'utilitzen en aquest àmbit regularment, es pot denegar l'execució també si no s'autoritzés en casos interns similars. Els dos Estats acordaran les disposicions pràctiques, l'autoritat d'emissió indicarà les raons per les que és necessària la informació sol·licitada i l'Estat d'execució serà el competent per actuar, dirigir i controlar les operacions relacionades amb l'execució de la mesura. Dos exemples d'aquest tipus de mesures poden ser el seguiment de les operacions bancaries o una entrega vigilada al territori de l'Estat d'execució.

En cinquè lloc trobem les investigacions encobertes, que suposa que es poden emetre OEI per sol·licitar a l'Estat d'execució que col·labori amb l'Estat d'emissió per realitzar investigacions d'activitats delictives per part d'agents infiltrats o amb identitat falsa. L'autoritat d'emissió indicarà les raons per les que considera que la investigació ha de ser encoberta. Els motius addicionals per denegar el reconeixement i execució seran que la realització d'investigacions encobertes no fos autoritzada en casos interns similars i que no hi hagi hagut acord en les disposicions pràctiques. Les investigacions es duran a terme conforme el Dret de l'Estat en el que

es realitzin, i l'Estat d'execució tindrà la competència d'actuació, direcció i control de les operacions.

En sisè lloc trobem la intervenció de les telecomunicacions, que pot ser amb assistència tècnica o sense assistència tècnica d'un altre Estat membre. Per la seves característiques electròniques, aquestes son les mesures d'execució que tenen més rellevància en ciberdelinqüència. En cas que sigui una intervenció de telecomunicacions amb assistència tècnica d'un altre Estat Membre, l' OEI es podrà emetre per intervenir les telecomunicacions de l'Estat l'assistència del qual es requereixi. L' OEI inclourà la informació necessària per identificar la persona objecte d'intervenció, la duració de la intervenció i les dades tècniques suficients per garantir l'execució de la sol·licitud. Els motius addicionals per la denegació de l'execució són que aquesta no estigues autoritzada en casos interns similars. L' OEI es podrà executar de dues formes: O bé amb la transmissió immediata de les telecomunicacions a l'Estat d'emissió, o bé amb la intervenció, registre i posterior transmissió del resultat de la intervenció a l'Estat d'emissió. El segon cas tracta les intervencions sense assistència tècnica d'un altre Estat. Això suposa que, quan per dur a terme una mesura d'investigació l'autoritat d'execució autoritza la intervenció de comunicacions, aquesta haurà de notificar a l'autoritat d'emissió d'aquesta intervenció si s'utilitza la direcció de comunicacions de la persona que figura a l' OEI.

CAPÍTOL III – ESTRATÈGIES, INSTRUMENTS NORMATIUS I ESTRUCTURES DE LA UNIÓ EUROPEA PER SEGUIR COMPLINT AMB LA LLUITA CONTRA LA CIBERDELINQÜÈNCIA

Els fonaments del marc legal de la Unió Europea s'han anat desenvolupant al llarg dels anys per protegir la seguretat dels seus ciutadans. Per ajudar els Estats Membres a lluitar contra la delinqüència i terrorisme, la UE ha creat un conjunt d'instruments. Actualment, i com hem anat mencionant anteriorment, la lluita contra la ciberdelinqüència és un dels reptes més rellevants tant a escala internacional com europea i nacional, i és per això que és important reforçar-ne els instruments, identificant maneres de sobreposar-se als obstacles de les investigacions en ciberdelinqüència. [31]

Des de principis de segle la Unió Europea ha mostrat reiteradament el seu compromís per fer front a la ciberdelinqüència. La feina feta pels Estats Membres i la Unió Europea en seva lluita es veu reflectida a través d'una multitud d'accions i iniciatives adoptades: instruments normatius, comunicacions, agències, projectes... En aquest apartat analitzarem les accions i iniciatives més rellevants que s'han dut a terme, dividint-les en tres blocs: Les comunicacions i informes, els instruments normatius i les agències, organismes i agrupacions creats.

3.1 – L'estratègia de la Unió Europea

La Unió Europea ha sigut conscient des dels inicis dels perills que comporten les noves tecnologies, com queda ja demostrat al Llibre Blanc de la Comissió del 1993 sobre *Creixement, competitivitat, ocupació. Reptes i pistes per entrar al segle XXI*[32], que dóna resposta a l'agitació social que suposaven les noves tecnologies i reconeix que s'ha de crear un espai comú d'informació que sigui arbitrat per un marc jurídic que fomenti el seu desenvolupament i permeti la investigació i cooperació entre els Estats Membres.

Seguint els passos del Llibre Blanc, a principis del segle XXI ja comencen a haver-hi manifestacions de les institucions que tenen en compte la preocupació per la ciberdelinqüència.

[31] Liana Iulia Paul " European Cooperation in Fighting Cybercrime" *Fiat Iustitia* No. 1/2016 p 154- 159 (2016) https://econpapers.repec.org/article/dcujournl/v_3a10_3ay_3a2016_3ai_3a1_3ap_3a154-159.htm

[32] Comisión de las Comunidades Europeas. *Libro Blanco, "Competitividad, Empleo Retos y Pistas para entrar en el siglo XXI. (*Luxemburgo: 1993). http://evalua.catedu.es/documentos/aragon/NormativaVarios/LB1993CrecimientoCompetitividadYEmpleoI.pdf

La Comunicació adoptada el 2001 per la Comissió Europea en relació a una *Creació de la Societat d'Informació més segura mitjançant la millora de les seguretats de les infraestructures d'informació i la lluita contra els delictes informàtics*[33], analitza camins per millorar la prevenció de delictes informàtics i la lluita contra qualsevol activitat delictiva relacionada amb noves tecnologies.

Al 2007, la Comissió Europea publica la Comunicació *Cap a una política general de lluita contra ciberdelinqüència"*[34] amb els objectius de millorar i facilitar la coordinació i cooperació entre les autoritats dels Estats Membres, desenvolupar un marc polític coherent per la UE en matèria de lluita contra la ciberdelinqüència i sensibilitzar sobre els perills que comporta. Estableix un camí a seguir en aquest àmbit, comprometent la Comissió a profunditzar sobre la política de la lluita contra la ciberdelinqüència. Així mateix, dos anys més tard publica una altra Comunicació titulada *Protegir Europa dels Ciberatacs i interrupcions a gran escala: augmentar la preparació, seguretat i resistència.*[35] es centra en la prevenció, preparació i coneixement, i en ella es defineix un pla de mesures immediates per potenciar la seguretat i resistència de les infraestructures crítiques d'informació.

La Comunicació de la Comissió del 2013 nomenada *Estratègia de Ciberseguretat de la Unió Europea: Un ciberespai obert, protegit i segur*[36] es planteja la necessitat de crear un entorn digital més segur, amb les garanties d'un funcionament adequat de les noves tecnologies d'informació i comunicació. Planteja el desenvolupament d'una estratègia que garanteixi el respecte dels principis de ciberseguretat a nivell nacional, europeu i internacional: la protecció dels drets

[33] Comisión Europea. *Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones: Creación de una sociedad de la información más segura mediante la mejora de la Seguridad de las infraestructuras de información y la lucha contra los delitos informáticos*, (Bruselas: 2001) https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52000DC0890

[34] Comisión Europea. *Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones, de 22 de mayo de 2007, "Hacia una política general de lucha contra la ciberdelincuencia*, (Bruselas: 2007) https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:ES:PDF

[35] Comisión Europea. *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 30 de marzo de 2009, sobre protección de infraestructuras críticas de información: "Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, Seguridad y resistencia"*. (Bruselas, 2009) https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52009DC0149&from=EN

[36] Comisión Europea. *Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones - Estrategia de Ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro, (*Bruselas, 2013) https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A52013JC0001

fonamentals, la llibertat d'expressió, les dades personals i la intimitat, l'accés a tothom i garantir la seguretat. La comunicació estableix que la lluita contra la ciberdelinqüència ha de consistir sobretot en cooperació. Donada la complexitat del problema i les moltes parts que intervenen, la solució no pot consistir en una supervisió europea centralitzada, ja que son les administracions nacionals les que es troben en millors condicions per organitzar les activitats de prevenció i resposta a incidents i atacs, així com establir contactes amb els sectors privats i ciutadans[37]. Tanmateix, però, queda clar que aquesta resposta a escala nacional hauria de comptar amb la intervenció de la Unió Europea i que, per tant, la ciberdelinqüència i ciberseguretat s'han d'abordar de manera global.

El sisè informe *De la situació relativa a una Unió de la Seguretat Genuïna i efectiva* [38] elaborat per la Comissió el 2017 recomana contemplar la ciberdelinqüència com una de les cinc amenaces prioritàries, conjuntament amb el tràfic i distribució de droga, el tràfic il·lícit de migrats, els robatoris i assalts organitzats i el tracte de sers humans. Altrament, el novè informe *De la situació relativa a una Unió de la Seguretat Genuïna i efectiva*[39] destaca l'important tasca del Centre Europeu de Ciberdelinqüència, del que parlarem més endavant, que recolza les autoritats nacionals en la lluita contra la ciberdelinqüència mitjançant l'assessorament. També ressalta la importància de la cooperació entre les autoritats públiques i l'industria en la lluita contra la ciberdelinqüència i la radicalització d'internet. Destaca la reunió informal de Ministres de Justícia i assumptes de la UE celebrada a Tallin el mateix any, centrada en la lluita contra la ciberdelinqüència, corrupció i reformes judicials essencials, on es va reiterar el compromís conjunt d'adoptar noves mesures per fer-hi front i reforçar la ciberseguretat.

Per altra banda, i també al 2017, la comunicació de la Comissió relativa a *Resiliència, dissuasió i defensa: enfortir la ciberseguretat a la Unió Europea*[40] insta a millorar la cooperació transfronterera relativa a la preparació i prevenció de ciberdelinqüència, recorda que s'hauria de crear un pla director que donés un enfoc coordinat de la cooperació davant la crisi entre els

[37] A Espanya, per exemple, trobem l'Observatori Espanyol de Delictes Informàtics (OEDI).

[38] Comisión Europea. *Informe de la Comisión al Parlamento Europeo, al Consejo Europeo y al Consejo. Sexto informe de situación relativo a una Unión de la Seguridad genuina y efectiva*, (Bruselas, 2017) https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017DC0213

[39] Comisión Europea. *Informe de la Comisión al Parlamento Europeo, al Consejo Europeo y al Consejo. Noveno informe de situación relativo a una Unión de la seguridad genuina y efectiva*, (Bruselas, 2017) https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017DC0407

[40] Comisión Europea. *Comunicación conjunta al Parlamento Europeo y al Consejo. Resiliencia, disuasión y defensa: fortalecer la Ciberseguridad de la UE*, (Bruselas, 2017) https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A52017JC0450

diferents elements de l'ecosistema cibernètic, i ressalta la importància de la ciberseguretat per la nostra prosperitat i seguretat. En definitiva, es pretén reforçar la resiliència de la Unió als ciberatacs, pel que s'ha d'adoptar un enfoc col·lectiu i ampli, implementant mesures de diferent tipus, com ara reforçar ENISA, crear un mercat únic de ciberseguretat, poder obtenir respostes ràpides d'emergència...

A la recomanació de la Comissió *Sobre la resposta coordinada als incidents i crisis de ciberseguretat a gran escala*[41] del mateix any també se'ns recorda la rellevància que té la ciberdelinqüència i la prioritat actual que té la seva cooperació. Assegura que una resposta eficaç davant incidents i crisis en ciberseguretat a nivell de la UE requereix una cooperació ràpida i eficaç entre totes les parts interessades pertinents i es basa en la preparació i capacitats dels Estats Membres, així com en una acció comuna coordinada.

Al 2017, la Comissió de les Llibertats Civils, Justícia i Assumptes d'Interior del Parlament Europeu emet un Informe *Sobre la lluita contra la Ciberdelinqüència*[42], en la que s'analitzen diversos aspectes en relació a la ciberdelinqüència: la prevenció, l'augment de la responsabilitat dels prestadors de serveis, les proves electròniques, la creació de capacitats a nivell europeu, la cooperació millorada amb tercers països i el reforç de la cooperació policial i judicial. L' informe mostra especial preocupació pels ciberdelictes que queden impunes i demana als Estats Membres cooperació amb les autoritats judicials i EUROJUST, per poder anivellar les condicions d'una utilització legal dels instruments d'investigació en línia. Subratlla la necessitat d'elaborar normes processals comunes que permetin establir els factors territorials que determinin el dret aplicable i definir les mesures d'investigació que es puguin utilitzar independentment de les fronteres geogràfiques.

Al 2018, el Consell du a terme dues accions rellevants. En primer lloc, adopta unes Conclusions sobre *Activitats informàtiques malintencionades*[43]en les que recalca la importància d'un ciberespai mundial, obert, lliure, estable i segur, en el que s'apliquin plenament els Drets Humans,

---

[41] Comisión Europea. *Recomendación de la Comisión de 13.9.2017 sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala*, (Bruselas, 2017) https://ec.europa.eu/transparency/regdoc/rep/3/2017/ES/C-2017-6100-F1-ES-MAIN-PART-1.PDF

[42]Parlamento Europeo, Comisión de Libertades Civiles, Justicia y Asuntos de Interior. *Informe sobre la lucha contra la ciberdelincuencia*. (Bruselas, 2017) https://www.europarl.europa.eu/doceo/document/A-8-2017-0272_ES.html

[43] Consell de la Unió Europea. "Actividades Informáticas malintencionadas: el Consejo Adopta unas Conclusiones" Comunicat de premsa, 16 d'Abril de 2018. https://www.consilium.europa.eu/es/press/press-releases/2018/04/16/malicious-cyber-activities-council-adopts-conclusions/pdf

les Llibertats Fonamentals i l'Estat de Dret. Manifesta la seva preocupació per l'ús d'activitats informàtiques malintencionades, i reitera que la Unió Europea seguirà desenvolupant la seva capacitat per afrontar la ciberdelinqüència. En segon lloc, a la reunió de 18 d'octubre[44] demana mesures per enfortir la ciberseguretat, particularment a aquelles capaces de respondre ciberatacs i dissuadir que es cometin.

Al 2019, el Consell adopta unes Conclusions en relació a la *Importància de la tecnologia 5G per l'economia europea i la necessitat de mitigar els riscos per la seguretat relacionats amb el 5G*[45] en les que destaca el paper important que tindrà el 5G al futur i posa èmfasi en el plantejament de seguretat que ha de tenir, i que ha de ser global.

Al 2020, el consell adopta unes Conclusions relatives a la *Ciberseguretat dels dispositius connectats*[46] en la que reconeix el major ús de productes de consum i dispositius industrials connectats a internet i els riscos que això comporta per la ciberseguretat, privacitat i seguretat d'informació. Aquestes conclusions defineixen prioritats per abordar la qüestió i fomentar la competitivitat mundial per garantir en màxim nivell de seguretat i protecció.

Al 2021, el Consell també adopta unes Conclusions sobre *L'estratègia de Ciberseguretat a la Unió Europea*[47], que exposa el marc d'actuació de la UE destinat a protegir els seus ciutadans i empreses de ciberamenaces , promoure sistemes d'informació segurs i protegir un ciberespai global, obert, lliure i segur. Destaca la importància de reforçar la cooperació amb organitzacions internacionals i tercers països socis per avançar a una interpretació compartida del panorama de la ciberdelinqüència.

---

[44]Consell de la Unió Europea. "Ciberdefensa: El Consejo actualiza el marco político. Comunicat de premsa, 19 de Novembre de 2018. https://www.consilium.europa.eu/es/press/press-releases/2018/11/19/cyber-defence-council-updates-policy-framework/pdf

[45]Consell de la Unió Europea. "Importancia de la tecnología 5G y riesgos para la Seguridad: El Consejo adopta unas conclusiones. Comunicat de premsa, 3 de Desembre de 2019. thttps://www.consilium.europa.eu/es/press/press-releases/2019/12/03/significance-and-security-risks-of-5g-technology-council-adopts-conclusions/

[46]Consell de la Unió Europea. "Ciberseguridad de los dispositives conectados: el Consejo adopta unas conclusiones. Comunicat de premsa, 2 de Desembre de 2020. https://www.consilium.europa.eu/es/press/press-releases/2020/12/02/cybersecurity-of-connected-devices-council-adopts-conclusions/pdf

[47] Consell de la Unió Europea. *Proyecto de Conclusiones del Consejo sobre la Estrategia de Ciberseguridad de la UE para la Década Digital.* Brusel·les, 2021. https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/es/pdf

3.2 – Instruments normatius

El *Conveni sobre Ciberdelinqüència de 2001*, també conegut com el Conveni de Budapest, adoptat al Consell d'Europa suposa una fita important en la creació d'instruments, malgrat no estigui estrictament elaborat en el marc de la Unió Europea, ja que es tracta del principal instrument internacional en matèria de cooperació internacional en la lluita contra la ciberdelinqüència, i la Unió Europea sempre ha animat als Estats i tercers països a ratificar-lo. Aquest Conveni, donada la seva importància, l'analitzarem més endavant.

Al llarg dels anys la Unió Europea ha anat adoptant instruments normatius que afecten directament a delictes integrats a la ciberdelinqüència, com ara la pornografia infantil o el frau en sistemes de pagament diferents a l'efectiu. També s'han adoptat instruments vinculats directament amb la ciberdelinqüència, com ara els relacionats amb Sistemes d'Informació, Ciberseguretat, ENISA o mesures restrictives. Així mateix, també s'han adoptat instruments normatius en altres àmbits que tenen una estreta relació amb la ciberdelinqüència, com protecció de dades o terrorisme.

En relació a la pornografia infantil, per exemple, el 2002 es va aprovar la *Decisió 2000/375/JAI del Consell de 29 de Maig de 2000 relativa a la lluita contra la pornografia infantil a internet,* que estableix la prevenció i lluita contra la producció, tractament, possessió i difusió de la pornografia infantil. Aquesta Decisió Marc és reforçada el 2004 per l'aprovació de la *Decisió Marc 2004/68/JAI del Consell, de 22 de Desembre de 2003, relativa a la lluita contra la explotació sexual dels nens i la pornografia infantil,* que es deroga el 2011 per la *Directiva 2011/93/UE del Parlament Europeu i del Consell, de 13 de Desembre de 2011, relativa a la lluita contra els abusos sexuals i la explotació sexual dels menors i la pornografia infantil i per la que es substitueix la Decisió Marc 2004/68/JAI del Consell.* Aquesta directiva, que lluita contra els abusos sexuals i explotació sexuals de menors, inclosa la pornografia infantil, estableix mesures que adrecen millor els nous desenvolupaments al context digital, establint les infraccions relacionades amb la pornografia infantil i més específicament els enganys de menors amb fins sexuals per mitjans tecnològics, com ara el *grooming*, el ciberassetjament pedòfil. La Directiva també estableix mesures pels llocs web d'Internet que contenguin o difonguin pornografia infantil.

En relació al frau i falsificació de mètodes de pagament diferents a l'efectiu, al 2001 s'adopta la *Decisió Marc 2001/413/JAI del Consell, de 28 de Maig de 2001, sobre la lluita contra el frau i la falsificació de mètodes de pagaments diferent a l'efectiu*, que és derogada el 2019 per la *Directiva 2019/713/UE del Parlament Europeu i el Consell, de 17 d'Abril de 2019, sobre la lluita contra el frau i la falsificació de mitjans de pagament diferents a l'efectiu i per la que se*

substitueix la Decisió Marc 2001/413/JAI del Consell. La directiva estableix normes mínimes relatives a la definició de les infraccions penals i sancions aplicables en l'àmbit del frau i falsificació de mitjans de pagament diferents a l'efectiu, i ens és d'especial interès ja que inclou els mitjans digitals d'intercanvi i les monedes virtuals, així com sistemes d'informació i dades informàtiques.

En relació als Sistemes d'Informació, el 2005 s'adopta la *Decisió marc 2005/222/JAI del Consell, de 24 de Febrer de 2005, relativa als atacs contra els sistemes d'informació* que té per objecte lluitar contra la delinqüència informàtica i promoure la seguretat de la informació reforçant la cooperació entre les autoritats judicials i altres autoritats competents. Aquesta Decisió es substitueix el 2013 per la *Directiva 2013/40/UE del Parlament Europeu i del Consell, de 12 d'Agost de 2013, relativa als atacs contra els sistemes d'informació i per la que es substitueix la Decisió Marc 2005/222/JAI del Consell* que té l'objectiu d'afrontar els ciberatacs a gran escala a través de requerir que els Estats Membres reforcin les lleis nacionals en relació a ciberdelinqüència i introdueixin sancions més elevades. Per tant, intenta harmonitzar les normes relatives a delictes i penes de sistemes d'informació, així com millorar la cooperació entre autoritats competents: Estats Membres, EUROJUST, EUROPOL i ENISA.

En relació a Ciberseguretat, el 2016 es va aprovar la *Directiva 2016/1148/UE del Parlament Europeu i del Consell, de 6 de Juliol de 2016, relativa a les mesures destinades a garantir un elevat nivell comú de seguretat de les xarxes i sistemes d'informació de la Unió* amb l'objectiu d'aconseguir un elevat nivell comú de seguretat a les xarxes i sistemes d'informació dins la Unió Europea per millorar el funcionament del mercat interior. La Directiva estableix obligacions als Estats Membres d'adoptar una estratègia nacional concreta, crea un grup de Cooperació per recolzar i facilitar la cooperació estratègica i intercanvi d'informació i crea la Xarxa CSIRT, de la que també parlarem més endavant, que és una xarxa d'equips de resposta a incidents de seguretat informàtica.

En relació a la creació de l'Agència Europea de Seguretat de la Xarxa i la informació, al 2004 s'aprova el *Reglament 460/2004/CE del Parlament Europeu i del Consell, de 10 de Març de 2004, pel que es crea l'Agència Europea de Seguretat de la Xarxa i la informació,* amb l'acrònim d'ENISA, de la que aprofundirem més endavant. Al 2013, va ser derogat pel *Reglament 526/2013/UE del Parlament Europeu i del Consell, de 21 Maig de 2013, relatiu a l'Agència de Seguretat de les Xarxes de la Informació de la Unió Europea (ENISA) i pel que es deroga el Reglamento 460/2004/CE,* que al seu lloc va ser derogat al 2019 pel *Reglament 2019/881/UE del Parlament Europeu i del Consell, de 17 d'Abril de 2019, relatiu a ENISA (Agència de la Unió Europea per la Ciberseguretat) i a la certificació de la ciberseguretat de les tecnologies de la Informació i la Comunicació i pel que es deroga el Reglament 526/2013/UE.* Aquest reglament

té dos àmbits materials diferents, els dos interrelacionats i destinats a assolir un nivell elevat de ciberseguretat i garantir el correcte funcionament de la UE. En primer lloc, el reglament reforça l'Agència de la Unió Europea per la Ciberseguretat. Com aprofundirem posteriorment, li concedeix un mandat permanent, més recursos i més tasques. En segon lloc, estableix un marc de certificació de ciberseguretat per tota la UE tant per productes, serveis com processos digitals. Això garanteix el correcte funcionament del mercat interior. Les empreses que facin negoci a algun Estat Membre es beneficiaran d'haver de certificar els seus productes, processos i serveis digitals només un cop, i que aquests certificats estiguin reconeguts a tota la UE. ENISA té un paper important en aquest marc, ja que és l'encarregat de preparar i mantenir el marc, i ha de preparar el terreny tècnic per esquemes de certificació específics i informar-ne al públic.

En relació a mesures restrictives, el Consell adopta el 2019 una *Decisió 7299/2019 del Consell, de 16 de Maig de 2019, sobre mesures restrictives per lluitar contra els ciberatacs que amenacin a la Unió o als seus Estats Membres,* en la que s'estableix un marc que permet a la UE imposar mesures restrictives específiques per dissuadir i contrarestar els ciberatacs que representen una amenaça exterior per la UE o els seus Estats Membres, en particular els perpetrats contra tercers Estats o organitzacions internacionals. Per tal que es puguin sancionar, han de ser atacs que tinguin repercussions importants i que s'originin o es cometin des de l'exterior de la UE, utilitzin infraestructura exterior a la UE, siguin comesos per persones o entitats establertes fora la UE o siguin comesos amb l'ajuda de persones o entitats fora de la UE. De fet, el Consell utilitza aquest instrument per primera vegada el 2020, quan imposa mesures restrictives contra sis persones i tres entitats[48], responsables d'atacs informàtics. Entre les sancions imposades figuren la prohibició de viatjar i la immobilització dels béns.

En relació a protecció de dades, ja al 1995 entra en vigor la *Directiva 95/46/CE del Parlament Europeu i del Consell, de 24 d'Octubre de 1995, relativa a la protecció de les persones físiques pel que respecta el tractament de dades personals i la lliure circulació d'aquestes dades,* derogada el 2016 pel *Reglament 2016/679/UE del Parlament Europeu i del Consell, de 27 d'Abril de 2016, relatiu a la protecció de les persones físiques pel que respecta el tractament de dades personals i la lliure circulació d'aquestes dades i pel que es deroga la Directiva 95/46/CE,* que també s'anomena Reglament General de Protecció de Dades. Aquest reglament té l'objectiu d'establir normes relatives a la protecció de les persones físiques pel que respecta el tractament de dades personals i normes relatives a la lliure circulació d'aquestes dades. Al 2002 s'aprova la *Directiva 2002/58/CE del Parlament Europeu i del Consell, de 12 de Juliol de 2002, relativa al*

[48] Consell de la Unió Europea. "La UE impone por primera vez sanciones en resupesta a los ciberataques" Comunicat de premsa, 30 de Juny, 2020. https://www.consilium.europa.eu/es/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/

tractament de les dades personals i a la protecció de la intimitat al sector de les comunicacions electròniques, també anomenada la Directiva sobre privacitat i les comunicacions electròniques, que contribueix a la protecció de les dades personals i al dret de la intimitat. Al 2006 s'aprova la *Directiva 2006/24/CE del Parlament Europeu i del Consell, de 15 de Març de 2006, sobre conservació de dades generades o tractades en relació a la prestació de serveis de comunicacions electròniques d'accés públic o de xarxes públiques de comunicacions i per la que es modifica la Directiva 2002/58/CE,* però aquesta acaba sent anul·lada pel Tribunal de Justícia de la Unió Europea. En el marc de la Directiva aprovada el 2002 també s'aprova el 2013 el *Reglament 2013/611/UE de la Comissió, de 14 de Juny de 2013, relatiu a mesures aplicables a la notificació de casos de violació de dades personals*. Finalment, és rellevant mencionar del 2008 la *Decisió Marc 2008/977/JAI del Consell, de 27 de Novembre de 2008, relativa a la protecció de dades personals tractades en el marc de la cooperació policial i judicial en matèria penal,* derogada el 2016 per la *Directiva 2016/680/UE del Parlament Europeu i del Consell, de 27 d'Abril de 2016, relativa a la protecció de les persones físiques pel que respecta el tractament de dades personals per part de les autoritats competents per fins de prevenció, investigació, detecció o enjudiciament d'infraccions penals o d'execució de sancions penals, i a la lliure circulació d'aquestes dades i per la que es deroga la Decisió Marc 2008/977/JAI del Consell.*

En relació al terrorisme, el 2002 es va aprovar la *Decisió Marc 2002/475/JAI del Consell, de 13 de Juny de 2002, sobre la Lluita contra el terrorisme.* Al 2017 es va aprovar la *Directiva 2017/541/UE del Parlament Europeu i del Consell, de 15 de Març de 2017, relativa a la lluita contra el terrorisme per la que es substitueix la Decisió Marc 2002/475/JAI del Consell i es modifica la Decisió 2005/675/JAI del Consell,* que va derogar la Decisió Marc anterior i també va modificar la *Decisió 2005/671/JAI del Consell, de 20 de Setembre de 2005, relativa a l'intercanvi d'informació i cooperació en relació a delictes de terrorisme.* Aquesta directiva inclou mesures contra els continguts en línia que constitueixin provocació pública.

3.3 - Agències, organismes i agrupacions

3.3.1 L'Agència de la Unió Europea de Ciberseguretat (ENISA)

L'Agència Europea de Seguretat a les Xarxes i de la Informació, també coneguda com l'Agència de la Unió Europea per la Ciberseguretat, i amb l'acrònim ENISA, neix amb l'adopció del 2004 del *Reglament 460/2004 del Parlament Europeu i del Consell en virtut del qual es crea l'Agència Europea de Seguretat de les Xarxes i la Informació,* malgrat actualment el marc jurídic és el

Reglament de 2019 *Relatiu a ENISA i la certificació de la ciberseguretat de les tecnologies de la Informació i la Comunicació.*

Té l'objectiu d'aconseguir un elevat nivell comunitari de ciberseguretat en tota la UE i és el punt de referència d'assessorament en qüestions relacionades amb la ciberseguretat per les institucions, òrgans i organismes de la unió, així com pels Estats Membres. És per això que algunes de les seves tasques consisteixen en prestar assistència i assessorament en l'elaboració i revisió de la política i el Dret de la Unió Europea en l'àmbit de ciberseguretat o assistir als Estats Membres perquè apliquin de manera coherent les polítiques i dret de la UE.

A més, ENISA té un paper molt important en la cooperació entre els Estats Membres, ja que un dels seus objectius és fomentar-la, en particular l'intercanvi d'informació, i la coordinació a nivell de la UE entre els Estats, els òrgans, les institucions i altres parts interessades ja siguin públiques com privades.

De fet, a l'article 7 del Reglament estableix que l'Agència recolzarà la cooperació operativa entre els Estats Membres, les institucions, els òrgans i els organismes de la UE i entre les parts interessades, a través de sinergies com ara el CERT-UE[49], i mitjançant intercanvi de coneixements, assessorament i directrius i establiment de disposicions pràctiques. A més, ENISA també s'ocupa de la secretaria de la Xarxa CSIRT, de la que parlarem més endavant.

A l'article 12 del mateix reglament es parla de la cooperació a nivell internacional, on s'estableix que ENISA contribuirà als esforços de la UE per cooperar amb tercers països i organitzacions internacionals en relació als problemes que es refereixin a la ciberseguretat, pels següents mitjans:

- Participar com a observador en la organització d'exercicis internacionals i analitzar els seus resultats.
- Facilitar l'intercanvi de millors pràctiques a petició de la Comissió.
- Facilitar assessorament especialitzat a la Comissió quan sigui necessari.

A l'article 42 s'estableix també que ENISA podrà cooperar amb les autoritats competents de tercers països o organitzacions internacionals si és necessari per complir amb els seus objectius. És per això que podrà establir acords de treball amb aquests tercers països i organitzacions internacionals amb prèvia aprovació de la Comissió, encara que aquests no podran imposar obligacions jurídiques ni a la UE ni als seus Estats Membres.

[49] Computer Emergency Response Team (CERT-UE) és un equip permanent format per experts en seguretat informàtica de les diferents institucions de la UE, que coopera amb equips dels diversos Estats Membres així com amb empreses especialitzades en ciberseguretat. Va estar establert a l'Agenda Digital pel Europa adoptada el Maig del 2010.

3.3.2 El Centre Europeu de Ciberdelinqüència (EC3)

La Comissió Europea va proposar la creació i desenvolupament d'aquest centre a la comunicació *La repressió del delicte a l'era digital: creació d'un centre europeu de ciberdelinqüència* [50]. L'EUROPOL va crear el Centre Europeu de Ciberdelinqüència al 2013 per enfortir la resposta de la ciberdelinqüència a la UE, i d'aquesta manera ajudar a protegir els ciutadans europeus, les empreses i els governs d'aquesta modalitat delictiva. Des que es va fundar, ha contribuït a la lluita de la ciberdelinqüència en múltiples ocasions: ha participat en operacions de perfil alt, ha actuat com a suport en desplegaments que han provocat detencions i ha analitzat fitxers maliciosos. [51] EC3 és l'eix central d'informació i intel·ligència criminal, dóna suport a les operacions i investigacions d'Estats Membres oferint anàlisis operatius i coordinació, proporciona productes d'anàlisis estratègic que permeten la presa de decisions informada a nivell tàctic i estratègic, proporciona capacitats de suport tècnic forense digital i tècnic altament especialitzat i representa la comunitat policial de la UE en àrees d'interès comú, entre altres.

Per entendre com treballa explicarem el funcionament de la seva Junta. Té un enfoc triple:

- Estratègia: Es divideix en dos equips. El primer, relatiu a la prevenció i gestió de grups d'interès, estableix aliances, assegura el desenvolupament de formació estandarditzada i coordina mesures de prevenció i sensibilització. El segon, relatiu a l'estratègia i desenvolupament, s'encarrega de l'anàlisi estratègic, la formulació de polítiques i mesures legislatives i gobernança d'Internet.

- Anàlisis forense: També es divideix en dos equips, l'anàlisi forense digital i l'anàlisi forense de documents. Els dos es centren en el recolzament operatiu i investigació i desenvolupament.

- Operacions: S'enfoquen a la explotació sexual infantil en línia, el frau de pagament i els delictes dependents d'altes tecnologies. Igualment també participa en una àrea criminal addicional, els mercats criminals en línia a la *DarkWeb.*

Cada any, el Centre Europeu de Ciberseguretat publica un informe estratègic que fa referència a les principals novetats i amenaces emergents, així com el desenvolupament en matèria de

[50] Comisión Europea. *Comunicación de la Comisión al Consejo y al Parlamento Europeo: La represión del delito en la era digital: creación de un centro europeo de ciberdelincuencia. (*Bruselas*, 2012)* *https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52012DC0140*

[51]Europol. European Cybercrime Centre – EC3. Combating crime in a digital age. (The Hague: Europol, 2021) https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

ciberdelinqüència, anomenat *The Internet Organised Crime Threat Assessment* (IOCTA). Aquest informe anual demostra la dimensió i varietat dels ciberdelictes, i com l' EC3 és una part clau en la resposta de l'EUROPOL i la UE per la lluita contra aquests.

L'IOCTA de 2020[52], per exemple, s'estructura amb els quatre capítols principals en relació a les quatre àrees principals d'operacions. En relació als delictes dependents d'altes tecnologies, l'informe remarca que el *Ransomware* (programes maliciosos) segueix sent l'amenaça més important ja que els criminals amenacen la publicació de dades si les víctimes no paguen. En relació al l'explotació sexual infantil en línia, es diu que aquesta segueix augmentant, i encara més amb la pandèmia COVID-19. Les aplicacions de xats encriptats fan que sigui encara més difícil la persecució judicial i la investigació d'aquestes activitats. En relació al frau en pagament, aquest està augmentant i s'està convertint més sofisticat. El frau d'inversió online s'està convertint en un dels cibercrims més importants, generant pèrdues de milions i afectant a milers de víctimes. En relació a l'abús criminal de la *Dark Web*, no hi ha hagut cap mercat dominant que hagi pujat des del 2019.

3.3.3 Grup d'Acció Conjunta Contra la Ciberdelinqüència (J-CAT)

El Grup d'Acció Conjunta Contra el Ciberdelicte[53], amb l'acrònim J-CAT, es va posar en marxa el Setembre de 2014 i treballa juntament amb EC3 en els casos de ciberdelinqüència internacional més importants que afecten els Estats Membres de la UE i els seus ciutadans. Té l'objectiu d'impulsar accions coordinades contra amanaces i objectius claus de la ciberdelinqüència facilitant la identificació conjunta, preparació, inici i execució d'investigacions i operacions transfrontereres.

Està integrat per un equip operatiu permanent de funcionaris dels diferents Estats Membres de la UE i socis de cooperació que no pertanyen a la UE, que tenen seu a la EUROPOL i es complementen amb EC3. Els funcionaris provenen de 9 Estats Membres (Entre els que hi ha Espanya, representada per la Policia Nacional i la Guardia Civil), de 7 països socis que no pertanyen a la UE i del EC3.

Entre els molts èxits assolits pel J-CAT, i a tall d'exemple, podem trobar la detenció el 2019 d'un individu de 36 anys del Regne Unit que va arribar a robar fins 10 Milions d'Euros en

[52]Europol. *Internet Organised Crime Threat Assessment 2020.* (The Hague: Europol, 2020) https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

[53]Europol. Joint Cybercrime Action Taskforce (J-CAT). (The Hague: Europol, 2021) https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce

criptomònada a més de 85 víctimes arreu del món, o les detencions a Espanya, Itàlia i França d'organitzacions que creaven grups de Whatsapp per intercanviar i crear material d'abús sexual infantil. Només el 2020 van reforçar 79 operacions de perfil alt.[54]

3.3.4 La Xarxa Judicial Europea contra la Ciberdelinqüència (EJCN)

La Xarxa Judicial Europea contra la Ciberdelinqüència és una xarxa de fiscals i jutges instructors especialitzats en cibercrims i investigacions criminals al ciberespai. Es va establir el 2016 amb la *Conclusió de la Xarxa Judicial Europea contra la Ciberdelinqüència*[55]. Té l'objectiu de facilitar l'intercanvi de coneixements tècnics i millors pràctiques, promovent la cooperació entre les autoritats judicials competents i fomentant el diàleg per garantir l'Estat de Dret al ciberespai.

Es reuneixen dos vegades a l'any a la seu de l'EUROJUST, i tenen com a observadors el Consell, la comissió, EUROJUST, el CE3 i la Xarxa Judicial Europea.

Durant les reunions de la Xarxa Judicial Europea sobre Ciberdelinqüència de 2019, els experts van debatre solucions pràctiques per abordar els desafiaments com ara el tancaments de dominis maliciosos, l'accés transfronterer directe a les proves electròniques i l'intercanvi espontani de proves en investigacions de ciberdelictes transfronterers. [56]

3.3.5 La Xarxa CSIRT

La Xarxa CSIRT[57] és un instrument de cooperació en ciberdelinqüència que dóna resposta als atacs cibernètics dels Estats Membres i treballa conjuntament per protegir els ciutadans i empreses de la Unió. Es crea el 2016 a través de la *Directiva 2016/1148/UE del Parlament Europeu i del Consell, de 6 de Juliol de 2016, relativa a les mesures destinades a garantir un elevat nivell comú de seguretat de les xarxes i sistemes d'informació de la Unió,* la Comissió hi participa com a observador i ENISA n'és el secretari i també li dona suport. La Xarxa CSIRT ofereix un fòrum en el que els membres poden cooperar, intercanviar informació i fomentar la confiança. Fent això,

[54]Europol, J-CAT. *J-CAT Factsheet 2020.* (The Hague: Europol, 2021) https://www.europol.europa.eu/publications-documents/j-cat-factsheet-2020

[55] Consell de la Unió Europea. *Conclusions of the Council of the European Union the European Judicial Cybercrime Network.* Brusel·les, 2016. https://data.consilium.europa.eu/doc/document/ST-10025-2016-INIT/en/pdf

[56] Eurojust. *Informe anual de Eurojust 2019.*

[57] CSIRTs Network. About CSIRTs Network. https://csirtsnetwork.eu/

els membres milloren la gestió dels incidents transfronterers i fins i tot poden debatre de forma coordinada davant incidents concrets.

La Xarxa CSIRT està formada pels representants dels CSIRTs dels Estats Membres. Els CSIRTs (Computer Security Incident Response Team) són equips que resolen els incidents que succeeixen a empreses, ciutadans, governs i institucions. A la Unió Europea actualment n'hi ha més de 500. A Espanya, per exemple, trobem el CCN-CERT, la capacitat de resposta a incidents de seguretat de la informació del Centre Criptològic nacional, i el INCIBE-CERT, el centre de resposta a incidents de seguretat de referència pels ciutadans i entitats de dret privat a Espanya, operat per l'Institut Nacional de Ciberseguretat i depenent del Ministeri d'Assumptes Econòmics i Transformació Digital.

3.3.6 Centre Europeu de Competència Industrial, Tecnològica i d'Investigació en Ciberseguretat

L'11 de Desembre de 2020 les institucions de la UE arriben a un acord polític, que encara està subjecte a l'aprovació pel Parlament Europeu i el Consell de la Unió[58], per crear un Centre Europeu de Competència Industrial, Tecnològica i d'Investigació de Ciberseguretat. Aquest Centre, quan es faci realitat, contribuirà a garantir la seguretat del mercat únic digital i augmentarà l'autonomia de la UE en matèria de ciberseguretat. Ajudarà la UE a posar en comú els seus coneixements especialitzats en investigació, tecnologia i desenvolupament en matèria de ciberseguretat, i a promoure la implantació de les solucions d'última generació. Estarà ubicat a Bucarest (Romania), i complementarà les tasques d'ENISA.

[58]Consejo de la Unión Europea. Nuevo Centro de Competencia en Ciberseguridad y nueva red: acuerdo informal con el Parlamento Europeo. Comunicat de premsa, 11 de Desembre de 2020. https://www.consilium.europa.eu/es/press/press-releases/2020/12/11/new-cybersecurity-competence-centre-and-network-informal-agreement-with-the-european-parliament/

CAPÍTOL IV – LA MÀXIMA EXPRESSIÓ DE COOPERACIÓ EN MATÈRIA DE CIBERDELINQÜÈNCIA: EL CONVENI SOBRE CIBERDELINQÜÈNCIA

En aquest apartat farem un anàlisi del Conveni sobre Ciberdelinqüència, que suposa la màxima cooperació en matèria de ciberdelinqüència existent en el pla internacional, al ser el seu únic instrument, i també afecta la cooperació entre els Estats Membres de la Unió Europea, al ser tots ells Estats Firmants del conveni.

4.1 - La història del conveni

El *Conveni sobre Ciberdelinqüència del Consell d'Europa de 8 de Novembre de 2001* es va desenvolupar com a resposta a la preocupació creixent en relació a l'adequació de la legislació sobre la ciberdelinqüència. Aquest conveni proposa harmonitzar les lleis relatives a la ciberdelinqüència i assegurar l'existència d'instruments processals per poder perseguir-la amb èxit a través de la cooperació entre els Estats signants.

Al 1989, el Consell d'Europa va publicar un seguit de recomanacions degut a la necessitat de noves lleis substantives que criminalitzessin conductes disruptives comeses a través de xarxes informàtiques. [59] Al 1995 es va publicar un segon estudi referent a la inadequació de les lleis processals penals relacionades amb la ciberdelinqüència. [60] A partir d'aquests informes, el Consell d'Europa va establir un Comitè d'experts en crim al ciberespai per fer un esborrany d'un conveni que facilités cooperació internacional en la investigació i persecució de la ciberdelinqüència. El resultat va ser el Conveni sobre Ciberdelinqüència del Consell d'Europa, que estudiarem a continuació.[61] Els Estats Membres del Consell d'Europa, Canadà, Japó, Sudàfrica i els Estats Units d'Amèrica van participar a la negociació del conveni, que va durar quatre anys, i van ser els primers en ratificar-lo i signar-lo el 2001. A més, i segons el seu article 37, qualsevol altre Estat també pot ser-ne part ratificant-lo. A l'actualitat, 65 Estats han ratificat el conveni.

[59] Consell d'Europa. *Recommendation No. R(89) 9 of the Committee of Ministers to Member States on Computer-related crime*. Brusel·les, 1989. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f1094

[60] Consell d'Europa. *Recommendation No. R(95) 13 of the Committee of Ministers to Member States concerning probems of criminal procedure law connected with information technology*. Brusel·les, 1995. https://rm.coe.int/16804f6e76

[61] Amalie M. Weber, The Council of Europe's Convention on Cybercrime, *Berkeley Technology Law Journal* 18, no. 1, 2003. http://www.jstor.org/stable/24120528 Pg. 425-446

Espanya va firmar el conveni el 23 de novembre de 2001 i el va ratificar el 2010, nou anys més tard, publicat al Butlletí Oficial de l'Estat (BOE) número 226 de 17 de Setembre de 2010.Les reformes necessàries després de la seva ratificació no es van produir fins l'entrada en vigor de la Llei Orgànica 5/2010, de 22 de Juny, que modifica la Llei Orgànica 10/1995, de 23 de Novembre, del Codi Penal.

4.2 - Objectius

El Conveni sobre la Ciberdelinqüència de 8 de Novembre de 2001, altrament anomenat Conveni de Budapest, va entrar en vigor l'1 de juliol de 2004. La seva rellevància és clau ja que, malgrat la seva antiguitat, és l'únic tractat multilateral vinculant dirigit a combatre la ciberdelinqüència.

Com ja hem dit anteriorment, el conveni proposa harmonitzar les lleis relatives a aquesta disciplina i també està orientat a facilitar la cooperació en la persecució d'aquesta modalitat delictiva, proporcionant als Estats part del mateix un marc per aquesta cooperació internacional. Segons el Consell, els problemes anteriors al Conveni estaven relacionats amb la falta de regulació criminal, de poders processals i de disposicions de cooperació i assistència mútua entre Estats. El conveni, per tant, pretén que les part adoptin legislació apropiada a la ciberdelinqüència, assegurar que els funcionaris encarregats de l'aplicació de la llei tinguin les eines processals necessàries per investigar i perseguir eficaçment els delictes informàtics i proporcionar cooperació internacional a les parts del conveni.

El seu principal objectiu, establert al preàmbul del mateix, és aconseguir aplicar una política criminal comuna per protegir la societat de la ciberdelinqüència, mitjançant l'adopció de la legislació adequada i la cooperació internacional. El preàmbul també indica que el Conveni resulta necessari per prevenir la ciberdelinqüència a través de la seva tipificació i l'assumpció dels poders suficients per lluitar de forma efectiva contra aquests delictes, facilitant la seva detecció, investigació i sanció, i sobretot establint disposicions que permetin una cooperació internacional en aquest àmbit que sigui ràpida i fiable. En definitiva, fer més eficients i eficaces les investigacions i procediments penals relatius als delictes relacionats amb sistemes i dades informàtiques, així com facilitar l'obtenció de proves electròniques dels delictes.

La seva manera de fer front a la ciberdelinqüència es resumeix en tres pilars, també plausibles pels tres capítols bàsics del conveni: Harmonització de lleis nacionals, millora de tècniques d'investigació i augment de cooperació entre Estats. També inclou aspectes legals com la jurisdicció, i estableix mesures de coordinació com ara l'assistència mútua per establir un contacte permanent entre les autoritats competents dels diferents Estats.

El conveni té com a finalitat bàsica completar els tractats i acords aplicables entre les parts. Continuant el nostre anàlisi en relació als Estats Membres de la Unió Europea, hem de tenir en compte que tots han ratificat el conveni. Per tant, aquest serà un complement al Conveni relatiu a l'Assistència Judicial en matèria penal entre els Estats Membres de la Unió Europea, la Decisió Marc relativa a l' Ordre de Detenció Europea i tots els altres instruments a nivell europeu de cooperació penal en general.

4.3 - Contingut i breu anàlisi

El conveni està organitzat en quatre capítols.

Al primer capítol s'estableix la terminologia, les definicions de llenguatge tècnic en relació a la ciberdelinqüència que s'utilitzen al llarg del conveni: sistema informàtic, dades informàtiques, proveïdor de serveis i dades sobre el tràfic.

Al segon capítol s'estableixen les mesures que han d'adoptar a nivell nacional els Estats signants del conveni, dividint-se aquestes en tres apartats.

- Estableix un cànon comú de ciberdelictes, un dret penal substantiu. Determina, per tant, un conjunt d'actuacions que estan considerades part de ciberdelinqüència, i les divideix en quatre categories. [62] Malgrat això no suposi una harmonització de les lleis nacionals de forma absoluta, suposa un avenç important ja que implica que tots els Estats signants partiran de la mateixa tipificació del delicte. El conveni té molta flexibilitat, ja que manté oberta pels Estats la punició, permetent l'aplicació flexible dels tipus penals. Això, segons Diaz Gómez[63], permet treballar per una lluita comuna, castigant conductes similars però respectant a la vegada els ordenaments jurídics propis dels Estats.

- Exigeix un conjunt comú de poders processals, que suposa una millora en les tècniques d'investigació. El conveni obliga els Estats part a tenir un conjunt d'eines processals a nivell nacional perquè les autoritats puguin dur a terme investigacions específiques en

[62] El conveni divideix els delictes informàtics en quatre categories: (i)Delictes en contra la confidencialitat, integritat i disponibilitat de dades i sistemes informàtics, que inclou accés il·lícit, intercepció il·lícita, interferència en les dades i en el sistema i abús dels dispositius; (ii) Delictes informàtics, que inclou falsificació informàtica i frau informàtic; (iii) Delictes relacionats amb el contingut, que inclou delictes relacionats amb pornografia infantil; i (iv) Delictes relacionats amb infraccions de propietat intel·lectual i dels drets afins.

[63]Andrés Díaz Gómez "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest" *REDUR 8*, 169-203 (Desembre 2010) pg. 25 https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071

l'àmbit de la ciberdelinqüència. Entre aquests poders processals trobem la conservació ràpida de les dades informàtiques emmagatzemades, la conservació i revelació parcial de dades sobre el tràfic, les ordres de presentació, el registre i confiscació de dades informàtiques emmagatzemades, obtenció a temps real de dades informàtiques i intercepció de dades sobre el contingut.

- Estableix un conjunt de normes per les que les parts poden fer valer la seva jurisdicció. Aquest conjunt de normes permeten que un Estat pugui reclamar jurisdicció d'un ciberdelicte que ha tingut conseqüències al seu territori, encara que l'autor hagi comés el delicte des d'un lloc diferent. A més, el conveni també atorga jurisdicció de l'Estat dels ciutadans que cometen delictes fora les fronteres de l'estat, sempre que el delicte també sigui castigat per la llei penal de la jurisdicció on s'hagués comés el delicte, o si el delicte s'hagués comés fora de la jurisdicció territorial de qualsevol estat. Part de la doctrina afirma que seran molt freqüents els supòsits en que diversos tribunals disputin el coneixement d'una causa, degut al manteniment de la concurrència de diversos criteris d'atribució competència sense establir criteris de prelació ni altres sistemes de prioritats.

Al tercer capítol s'estableix un marc de cooperació internacional, especialment d'interès per la recerca que ens ocupa i on, per tant, hi farem èmfasi al següent apartat. El conveni proporciona principis generals de cooperació internacional, extradició i assistència mútua, així com disposicions especials en relació a assistència mútua en matèria de mesures provisionals i a poders d'investigació.

Al quart capítol s'estableixen disposicions finals, relatives a la firma, entrada en vigor, adhesió, aplicació territorial i efectes del conveni entre altres.

4.4 – Les previsions de Cooperació Internacional al Conveni

El tercer capítol versa exclusivament sobre la cooperació internacional. Al preàmbul del Conveni ja es dona importància i necessitat als vincles de cooperació internacional, sobretot als seus paràgrafs 7 i 8, on es reconeix la necessitat de cooperació entre els Estats i el sector privat a la lluita contra la ciberdelinqüència, així com la necessitat de protegir els interessos legítims en la utilització i desenvolupament de tecnologies d'informació. També estima que la lluita efectiva contra la ciberdelinqüència requereix una cooperació internacional reforçada, ràpida i eficaç en matèria penal. Aquest capítol es divideix en dos seccions, relatives la primera a principis generals i la segona a disposicions especials.

4.4.1 Principis generals

El conveni proporciona, inicialment, tres principis generals de cooperació internacional.

- La cooperació internacional es proporcionarà entre els Estats "en la major mesura possible".[64]

- La obligació de cooperar no només s'estén als delictes establerts al conveni, sinó que també a les proves electròniques vinculades a delictes. Això suposa que els termes d'aquest capítol son tant aplicables quan es cometi un delicte utilitzant un sistema informàtic, un ciberdelicte, com quan es cometi un delicte comú, com ara un assassinat, que no s'ha comés mitjançat l'ús de sistemes informàtics però involucra igualment proves electròniques. Tanmateix, s'ha de tenir en compte que els articles relatius a extradició i assistència mútua per la obtenció en temps reals de dades relatives al tràfic i per la intercepció de dades relatives al contingut permeten que les parts prevegin diferents modalitats per l'aplicació d'aquestes mesures. [65]

- Les disposicions relatives a la cooperació internacional no substitueixen les disposicions preexistents en acords internacionals en matèria d'assistència mútua, extradició, ni tampoc els acords recíprocs entre les parts o les disposicions pertinents al dret intern de cada Estat en matèria de cooperació internacional.

El conveni també proporciona principis generals en relació a extradició i assistència mútua.

En relació a l'extradició, el conveni estableix la obligació d'atorgar-la als Estats part en aquells delictes definits al segon capítol quan aquests siguin castigats per la legislació de les dues parts implicades amb una pena de privació de llibertat d'una duració màxima d'almenys un any. Tanmateix, això ha d'estar conforme al que està disposat als instruments ja existents entre les parts.[66] Ja que el nostre anàlisi es centra en els Estats Membres de la Unió Europea, ens hem de remetre a l' Ordre Europea de Detenció i Entrega, que analitzarem més endavant.

[64] Aquest principi exigeix que les parts es brindin una àmplia cooperació recíproca, i que redueixin al mínim els impediments a la circulació fluida i ràpida de la informació i les proves a nivell internacional.

[65]Consell d'Europa. *Informe Explicatiu del Conveni sobre la Ciberdelinqüència*. https://rm.coe.int/16802fa403 Pg. 69

[66] Amalie M. Weber, The Council of Europe's Convention on Cybercrime, *Berkeley Technology Law Journal* 18, no. 1, 2003. http://www.jstor.org/stable/24120528 Pg. 433

En relació a l'assistència mútua, el conveni estableix, i aplicant els principis generals mencionats anteriorment, que les parts es concediran assistència mútua "en la major mesura possible" tant per investigacions o procediments relatius ciberdelictes com per obtenir proves electròniques d'un delicte d'una altra categoria, i que aquesta assistència estarà subjecta a les condicions previstes pel dret intern o tractats d'assistència mútua aplicables. A més, les parts estan obligades a tenir una base jurídica per dur a terme les formes específiques de cooperació que s'anuncien a la resta del capítol i que especificarem més endavant. També s'estableix un procediment ràpid en cas d'urgència, en el que les parts podran transmetre sol·licituds d'assistència o comunicacions relacionades amb les mateixes per mitjans ràpids de comunicació com el fax o el correu electrònic, amb confirmació oficial posterior si es requereix, i l'altra part haurà d'acceptar la sol·licitud i donar resposta amb els mateixos mitjans. Aquest procediment s'estableix perquè les dades informàtiques son molt volàtils, són molt senzilles d'eliminar i en alguns casos només s'emmagatzemen per curts períodes de temps, i això fa impossible seguir la pista d'un delicte fins al seu autor o destruir les proves essencials per la seva culpabilitat.[67] També s'incorpora una definició de la doble tipificació penal[68], per els casos en que s'hagi d'utilitzar el concepte en assistència mútua, i la considera la conducta constitutiva de delicte ho sigui en virtut del dret intern dels dos Estats Membres, amb independència que estiguin inclòs dins la mateixa categoria o tinguin la mateixa terminologia. Aquesta definició es dona per evitar que les parts adoptin una prova massa rígida a l'aplicar la doble tipificació penal, i a que s'apliqui de manera flexible per facilitar la concessió de l'ajuda. [69] Finalment, també s'estableix un procediment d'informació espontània en aquells casos en que una part tingui informació que consideri que pot ajudar a la part receptora a iniciar o dur a terme investigacions o procediments, sense petició prèvia.

4.4.2 Disposicions especials

A continuació dels principis generals, el conveni proporciona disposicions especials en relació a l'assistència mútua en matèria de mesures provisionals i en relació als poders d'investigació. Igualment, ens parla de la Xarxa 24/7. La finalitat d'aquesta secció és establir uns mecanismes

[67] Consell d'Europa. *Informe Explicatiu del Conveni sobre la Ciberdelinqüència*. https://rm.coe.int/16802fa403 Pg.73

[68]En relació a Ciberdelinqüència i en el marc d'aquest Conveni, quan parlem del principi de doble tipificació penal hem de tenir en compte que els delictes establerts al segon capítol del conveni compliran automàticament el principi entre les parts del mateix. Per tant, només s'haurà d'analitzar en aquells delictes no definits al conveni.

[69] Consell d'Europa. *Informe Explicatiu del Conveni sobre la Ciberdelinqüència*. https://rm.coe.int/16802fa403 Pg.75

específics per adoptar mesures eficaces i concertades a nivell internacional, tant a nivell de ciberdelictes com de proves electròniques. [70]Les investigacions internacionals concertades de delictes informàtics i les proves electròniques són possibles gràcies a les provisions d'assistència mútua al conveni. Aquestes provisions d'assistència mútua son tant en relació a les mesures provisionals com en relació als poders d'investigació.

En relació a les mesures provisionals podem trobar dos mecanismes.

- La conservació ràpida de dades informàtiques emmagatzemades suposa establir un mecanisme en que una part pot fer una sol·licitud de conservació ràpida de dades emmagatzemades al territori de la part requerida a través d'un sistema informàtic, amb l'objectiu que les dades no siguin alterades o eliminades durant el període de temps necessari per preparar, transmetre i executar una sol·licitud d'assistència mútua per obtenir les dades. Es tracta, per tant, d'una mesura limitada i provisional, que en principi s'hauria d'aplicar molt més ràpidament que una sol·licitud tradicional d'assistència mútua. Aquesta mesura, a més, és menys intrusiva que l'assistència mútua convencional, ja que la part requerida ha d'assegurar que les dades es preservaran, però no hauran de ser entregades fins que es compleixin els criteris per permetre la seva revelació conforme els règims habituals d'assistència mútua. [71] És important destacar que, com a regla general, per la conservació de dades no es requereix la doble tipificació penal explicada anteriorment, ja que proporcionar els aclariments necessaris per establir l'existència d'aquesta doble tipificació penal pot suposar un temps que pot posar en perill l'obtenció de les dades, en una situació amb el temps tant escàs. Tanmateix, si una part exigeix la doble tipificació penal com a condició per respondre una sol·licitud d'aquestes característiques i té motius per creure que en el moment de la divulgació no es complirà amb aquest principi, pot exigir-lo com a condició prèvia. [72] A part de per l'exigència de doble tipificació penal, un Estat només podrà rebutjar una sol·licitud de conservació de dades si això perjudiqués la seva sobirania, seguretat, ordre públic o altres interessos fonamentals, o quan es consideri un delicte polític.

[70] Consell d'Europa. *Informe Explicatiu del Conveni sobre la Ciberdelinqüència*. https://rm.coe.int/16802fa403 Pg.82

[71] Consell d'Europa. *Informe Explicatiu del Conveni sobre la Ciberdelinqüència*. https://rm.coe.int/16802fa403 Pg.83

[72] Com hem dit anteriorment, només es podrà exigir com a condició prèvia la doble tipificació penal en aquells delictes no establerts al capítol segon del conveni, ja que els establerts compleixen la doble tipificació penal automàticament.

- La revelació ràpida de dades conservades sobre el tràfic suposa, a petició de l'Estat on s'ha comés el delicte, que la part requerida ha de conservar les dades relatives al tràfic. És a dir, a les dades en relació a una transmissió que ha viatjat a través dels seus ordinadors, amb la participació d'un proveïdor de serveis d'aquest estat, amb el fi de rastrejar la transmissió fins el seu origen i identificar l'autor del delicte, o localitzar proves essencials. Igualment, només es podrà denegar aquesta revelació de dades si la sol·licitud fa referència a un delicte polític o l'execució podria atemptar a la sobirania, seguretat, ordre públic o altres interessos essencials.

En relació als poders d'investigació, trobem tres altres mecanismes d'assistència mútua, que son els mecanismes habituals.

- L'assistència mútua en relació a l'accés a dades informàtiques emmagatzemades suposa que un Estat podrà sol·licitar a un altre que registri, confisqui o obtingui i reveli dades emmagatzemades a través d'un sistema informàtic situat al territori de la part requerida. La resposta haurà de ser el més aviat possible quan hi hagi motius per creure que les dades estan especialment exposades al risc de pèrdua o modificació. Tanmateix, no es requerirà l'autorització de l'estat, i per tant es podrà actuar unilateralment, quan les dades es troben a disposició del públic, independentment de la seva ubicació geogràfica, i si s'obté el consentiment lícit i voluntari de la persona legalment autoritzada per revelar les dades.

- L'assistència mútua per obtenció a temps real de dades sobre el tràfic és un mecanisme que permet que les parts es prestin assistència mútua per obtenir a temps real dades sobre el tràfic associat a comunicacions que passen a través d'un sistema informàtic a un altre estat. És fonamental que els investigadors dels Estats puguin obtenir les dades relatives al tràfic en temps real d'altres Estats, ja que són essencials per rastrejar una comunicació fins al seu origen, i poden haver sigut eliminats automàticament per un proveïdor de serveis en la cadena de transmissió abans de poder ser conservats. [73] Les parts prestaran l'assistència obligatòriament respecte aquells delictes pels que es podrien aconseguir també les dades a temps real en el seu propi estat.

- L'assistència mútua en relació a la intercepció de dades sobre el contingut suposa que les parts es prestaran assistència per obtenir i gravar en temps real dades sobre el contingut de comunicacions específiques transmeses per mitjà d'un sistema informàtic. Al ser un

[73] Consell d'Europa. *Informe Explicatiu del Conveni sobre la Ciberdelinqüència*. https://rm.coe.int/16802fa403 Pg. 87

mecanisme molt intrusiu, té una obligació restringida per lleis i tractats aplicables per les parts.

En quant a la xarxa 24/7, es tracta d'un mecanisme establert pel tractat que suposa que tots els Estats part tindran designat un punt de contacte disponible les vint-i-quatre hores del dia, set dies a la setmana, per garantir la prestació d'ajuda immediata. El motiu d'aquest mecanisme, i com s'hi ha anat posant èmfasi, és la resposta ràpida que s'exigeix per combatre la ciberdelinqüència. És per això, precisament, que la cooperació policial existent i les modalitats d'assistència mútua requereixen canals complementaris per abordar de manera més eficaç i ràpida els desafiaments de la era informàtica. [74]L'assistència inclourà assessorament tècnic, conservació de dades, obtenció de proves, subministrament d'informació jurídica i localització de sospitosos.

[74] Consell d'Europa. *Informe Explicatiu del Conveni sobre la Ciberdelinqüència*. https://rm.coe.int/16802fa403 Pg.89

CAPÍTOL V – CRÍTIQUES I PROPOSTES A LA COOPERACIÓ CIBERDELICTUAL

En aquest apartat farem una crítica al sistema de cooperació ciberdelictual que existeix actualment a la Unió Europea i també al *Conveni sobre ciberdelinqüència*. Igualment, analitzarem propostes per millorar el model de cooperació actual.

Susan W. Brenner[75] proposa l'adopció d'un nou sistema com a alternativa a la cooperació internacional en ciberdelinqüència. Afirma que existeixen tres models d'estructurar una resposta adequada, els dos últims especulatius.

En primer lloc, el model ja existent adoptat pel Consell d'Europa amb el *Conveni sobre Ciberdelinqüència*, en el que la responsabilitat davant la ciberdelinqüència és analitzada en detall entre els Estats, que investiguen, processen i sancionen les delinqüents informàtics. Brenner considera que aquest model té el problema en la seva aproximació, ja que té base territorial i la ciberdelinqüència no.

En segon lloc, un model hipotètic que suposés la centralització del compliment de la llei en una agència individual responsable de controlar la ciberdelinqüència a tot el món. Aquest seria el model més extrem, però generaria una agència global responsable d'investigar la ciberdelinqüència, processar els delinqüents i sancionar-los. Aquesta aproximació està dissenyada per Brenner a partir de la premissa que el ciberespai és una nova jurisdicció, una àrea diferent en l'activitat humana que requereix la seva pròpia institució, i suposaria acceptar quelcom desconegut per dret, però que segons l'autora és inevitable.

En tercer lloc, un altre model hipotètic en que el processament i la sanció dels delinqüents segueixi sent competència dels Estats, però els procediments d'investigació criminal i detenció dels delinqüents sigui delegat a una agència central. A diferència d'INTERPOL, aquesta agència no coordinaria només les investigacions entre autoritats locals de diferents països, sinó que seria la responsable de la conducció d'investigacions i de l'enviament d'evidències. Aquest model seria més beneficiós pels Estats, ja que no haurien d'entregar tota la responsabilitat en relació a la ciberdelinqüència, seria una solució entremig dels dos primers models. Els Estats encara assumirien la responsabilitat de definir que és ciberdelinqüència, però milloraria la resposta general a la ciberdelinqüència. Una agència global centralitzada podria observar les seves tendències, i en comptes de investigacions disperses arreu del món, cada una treballant amb la seva estructura institucional, l'agència podria identificar les conductes prèviament.

[75]Susan Brenner. "La Convención sobre Cibercrimen del Consejo de Europa". *Revista chilena de Derecho y Tecnología; Universidad de Chile, Volumen I, Nro. I*, 2012. https://rchdt.uchile.cl/index.php/RCHDT/article/view/24030 Pg. 230

Analitzant els models de Brenner des de la perspectiva del nostre treball, podem dir que la lluita contra la ciberdelinqüència a la Unió Europea té un sistema que encaixa amb el primer model, però també té semblances amb el tercer model. Els Estats són els que analitzen, investiguen, processen i sancionen els delictes cibernètics. Tanmateix, hi ha actors de la Unió com ENISA, EC3, J-CAT, EJCN o la Xarxa CSIRT que coordinen les investigacions entre les autoritats locals dels diferents Estats Membres, però també son en part responsables de conduccions de les mateixes: impulsen accions coordinades, proporcionen anàlisis de fitxers...

Malgrat això, no podem dir que la Unió Europea tingui una agència que sigui plenament responsable de les investigacions i enviament de proves, ja que totes les que hem mencionat actuen com a suport per coordinar els Estats Membres i donar-los assistència si ho requereixen. Encara que el sistema que hi ha actualment a la Unió Europea no sigui una reproducció exacte del tercer model de Brenner, s'hi acosta molt més que el model internacional de cooperació en ciberdelinqüència actual. Si es creessin instruments similars als que existeixen a la Unió a nivell internacional, suposaria un avenç molt rellevant, ja que és un molt bon exemple de cap on s'ha d'encaminar la cooperació en aquest àmbit.

Per altra banda, Díaz Gómez[76] estableix un conjunt de requisits que ha de tenir l'adequada cooperació internacional en matèria ciberdelictual. En primer lloc, la cooperació ha de tenir pensament universal, abastar tants Estats com sigui possible ja que si no, l'aplicació pot quedar frustrada. També hi ha d'haver límits formals de cooperació, és a dir, un harmonització de les normes substantives i processals però que respecti les normes i tradicions pròpies dels Estats i Tractats Internacionals. Igualment hi ha d'haver límits materials de cooperació, és a dir, s'han de complir els principis Non Bis In Ídem, de culpabilitat, d'humanitat en les penes, de legalitat... Un altre requisit essencial és que han de participar tots els sectors de la societat: governs i administracions però també organitzacions internacionals, associacions, experts, empreses...A més, la regulació ha de ser coherent i homogènia, sense contradiccions i amb lògica normativa.

Si comparem aquests requisits amb la realitat de la cooperació a la Unió Europea ens trobem amb que els compleix gairebé tots. La legislació de la Unió Europea és capdavantera en les noves formes de cooperació entre Estats, tant en matèria de ciberdelinqüència com de cooperació internacional en general. Té una visió integradora de la cooperació en matèria de ciberdelinqüència en els seus Estats Membres, que parteix del desig comú d'arribar a conclusions similars sobre quin ha de ser el tractament adequat de determinats fenòmens, i que sens dubte té el pensament universal del que Díaz Gómez fa referència. A més, no només és una cooperació

[76] Andrés Díaz Gómez "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest" *REDUR 8*, 169-203 (Desembre 2010) pg. 24 https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071

entre Estats i institucions, sinó que també hi participen activament altres actors com experts en la matèria, centres privats o empreses que treballen al sector.

El *Conveni sobre ciberdelinqüència*, conegut com Conveni de Budapest, també ha aixecat crítiques i valoracions.

Segons Weber[77], l'eficàcia del conveni es veu minvada per la subordinació de la mateixa a altres acords pre-existents d'assistència mútua i per l'ambigüitat del compromís que prenen les parts. A més, també qüestiona el valor del conveni perquè considera que, tenint en compte que la ciberdelinqüència és un tipus delictiu ràpidament canviant, el feixuc procediment que es requereix per esmenar el conveni podria suposar un risc per una fixació prematura de la llei.

Diaz Gómez[78], per altra banda, considera que la aparició del Conveni ha permès iniciar el camí decisiu cap a la harmonització dels tipus penals relatius a la ciberdelinqüència i l'apropiada instrumentalització de les normes processals i de la col·laboració policial per la seva lluita, especialment en relació a l'intercanvi de dades i informació. Tanmateix, es mostra molt crític respecte el mateix, ja que considera que conté desencerts en l'articulat i potencials complicacions en matèria de drets.

Finalment, Brenner[79] considera que perquè el Conveni aconseguís el seu objectiu, hauria de ser ratificat i implementat per tots els països del món, però això no treu que sigui un instrument útil per facilitar la cooperació entre els països que l'han implementat. El conveni tracta la ciberdelinqüència com un delicte convencional, que ha de ser resolt unilateralment. Malgrat no es pot negar que es tracta d'un tipus de delinqüència, es pot caracteritzar amb més precisió: té les característiques bàsiques pròpies de la delinqüència tradicional[80], però no té la base territorial. Tanmateix, el conveni dona a aquesta circumstància una resposta tradicional, sol·licitant als països brindar-se assistència els uns als altres a través d'investigacions i procediments als respectius països, resposta que implica continuar amb el sistema de compliment local i descentralitzat.

---

[77] Amalie M. Weber, The Council of Europe's Convention on Cybercrime, *Berkeley Technology Law Journal* 18, no. 1, 2003. http://www.jstor.org/stable/24120528 Pg. 425-446

[78]Andrés Díaz Gómez "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest" *REDUR 8,* 169-203 (Desembre 2010) pg. 34 https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071

[79] Susan Brenner. "La Convención sobre Cibercrimen del Consejo de Europa". *Revista chilena de Derecho y Tecnología; Universidad de Chile, Volumen I, Nro. I,* 2012. https://rchdt.uchile.cl/index.php/RCHDT/article/view/24030 Pg. 232

[80] Això és: un actor, una víctima i la comissió del dany socialment intolerable.

CONCLUSIONS

Primera. La ciberdelinqüència és una modalitat delictiva que requereix un tractament especial al tenir característiques diferents a la delinqüència convencional ja que, entre altres, té un abast global que implica que sigui un fenomen internacional. La inexistència de fronteres reals a Internet i el fet que les víctimes de la ciberdelinqüència estiguin molt freqüentment localitzades a punts geogràfics diferents que els autors dels delictes fan complicada la seva persecució i la obtenció de proves.

Segona. El seu caràcter supranacional requereix de la cooperació internacional per donar solució als problemes que es produeixen quan es requereix practicar una actuació a territori estranger. Només quan s'estableixen mecanismes de cooperació i assistència judicial entre els Estats és quan es pot desenvolupar plenament un procediments en que hi hagi implicació transfronterera. És per això que l'adopció d'instruments de cooperació és estrictament necessària per lluitar radicalment contra la ciberdelinqüència. Concretament els Estats Membres de la Unió Europea tenen uns objectius, valors i marc legal comuns que faciliten l'acord en implementar instruments de cooperació en aquest àmbit.

Tercera. La Unió Europea es serveix d'instruments genèrics en relació a la Cooperació Judicial Penal que agafen especial rellevància en la lluita contra la ciberdelinqüència. Un exemple és EUROJUST, competent de ciberdelinqüència com a forma de delinqüència greu, que propicia un acostament entre els Estats Membres. És el punt de referència per coordinar investigacions, trobar solucions per poder fer intercanvis dins els marcs jurídics aplicables i donar més eficàcia a les seves investigacions i actuacions.

Quarta. Un altre instrument del que fa ús la Unió Europea per lluitar contra la ciberdelinqüència és l' Euro Ordre, en aquells casos en que acusats o condemnats es troben a un altre Estat Membre, per procedir a la seva detenció i entrega. En ciberdelinqüència és comú l´ús d'aquest instrument degut al seu caràcter transfronterer, i precisament és un dels delictes que no requereixen control de doble tipificació perquè es pugui executar l'Euro Ordre, sinó que únicament requereix que es castigui a l'Estat emissor amb una pena d'un màxim de mínim tres anys.

Cinquena. El règim únic per obtenir proves en casos de dimensió transfronterera que proporciona l'Ordre Europea d'Investigació també és d'utilitat en la modalitat delictiva d'anàlisi per l'elevada necessitat de proves transfrontereres. També en aquest instrument la ciberdelinqüència obté un tracte especial al ser un dels delictes pels que no es pot denegar l'execució pel simple fet de no ser una conducta constitutiva de delicte a l'Estat d'execució. A més, mesures concretes com aquelles que impliquen la obtenció de proves a temps real o la intervenció de telecomunicacions es regulen en aquest instrument i son molt utilitzades en la persecució de la ciberdelinqüència.

Sisena. La ciberdelinqüència va en augment, i amb aquesta crescuda també hi ha una conseqüent evolució estratègica de la UE. Des de principis de segle s'ha manifestat en relació a la ciberdelinqüència mostrant la seva preocupació al respecte i buscant noves maneres de millorar-ne la seva lluita. A través de múltiples Comunicacions de la Comissió Europea s'ha mostrat al llarg dels anys favorable a millorar i facilitar la cooperació entre Estats Membres en aquest àmbit i sensibilitzar sobre els perills que comporta, establint plans estratègics per una millora de la seva persecució i plantejant també estratègies relacionades amb ciberseguretat com a prevenció, requerint la resposta coordinada dels incidents a gran escala. El Consell també ha anat adoptant Conclusions recalcant la necessitat d'enfortir la ciberseguretat a la Unió.

Setena. La Unió Europea ha sabut estar a l'altura i no només ha manifestat les seves inquietuds sinó que també les ha materialitzat a través d'una pluralitat d'instruments normatius que ha anat desenvolupant al llarg dels anys per protegir els seus ciutadans i lluitar contra la ciberdelinqüència. En relació a Dret Material, la Unió Europea ha legislat en pornografia infantil, frau i falsificació de mètodes de pagament diferents a l'efectiu, terrorisme i protecció de dades entre altres, però també ha creat a partir d'instruments normatius, per exemple, agències com ENISA o mesures restrictives per lluitar contra ciberatacs i atacs contra els sistemes d'informació i mesures destinades a garantir un elevat nivell comú de ciberseguretat.

Vuitena. La Unió Europea també ha reaccionat davant aquesta nova amenaça amb la creació de diferents agències, organismes i agrupacions que, duent a terme una diversitat d'accions, tenen l'objectiu principal de lluitar contra la ciberdelinqüència. Primerament, ENISA assessora en qüestions relacionades amb la ciberdelinqüència a les institucions, òrgans i organismes de la Unió, així com als Estats Membres, fomenta la cooperació entre els Estats Membres i coordina els Estats, òrgans, institucions i parts interessades, ja siguin públiques o privades. En segon lloc, EC3 participa en operacions i actua com a suport en desplegaments, com a part de EUROPOL. Dona suport a operacions i investigacions d'Estats Membres oferint anàlisis operatius i coordinació. En tercer lloc, J-CAT impulsa accions coordinades amb EC3 contra amenaces facilitant la identificació conjunta, preparació, inici i execució d'investigacions i operacions transfrontereres. En quart lloc, la Xarxa Judicial Europea contra la Ciberdelinqüència, formada per fiscals i jutges instructors especialitzats en cibercrims, facilita l'intercanvi de coneixements tècnics i promou la cooperació entre autoritats judicials. Finalment, la Xarxa CSIRT dona resposta als atacs cibernètics dels Estats Mambes i treballa per protegir els ciutadans i empreses de la Unió. Addicionalment, hi ha previsions de crear un Centre Europeu de Competència Industrial, Tecnològica i d'Investigació en Ciberseguretat que garanteixi la seguretat al mercat únic digital i ajudi la UE a posar en comú els seus coneixements especialitzats en investigació, tecnologia i desenvolupament en matèria de ciberseguretat, però encara no s'ha fet realitat.

Novena. El Conveni sobre Ciberdelinqüència és la màxima expressió de cooperació en matèria de ciberdelinqüència existent en el pla internacional i també afecta la cooperació entre els Estats Membres de la Unió Europea al ser-ne tots signants. Estableix terminologia, mesures que els Estats signants han d'adoptar a nivell nacional i un marc de cooperació internacional. Específicament en aquest últim punt, determina uns principis generals, com l'assistència mútua o la obligació de cooperar també en proves electròniques vinculades a delictes, i unes disposicions especials relacionades, per exemple, amb mesures provisionals i poders d'investigació. És molt important tenir en compte, tanmateix, que aquest conveni no substitueix els acords recíprocs entre les parts. Per exemple, les disposicions relacionades amb extradició no seran utilitzades dins la Unió Europea ja que es regeix per la *Decisió Marc 2002/584/JAI del Consell, del 13 de Juliol, relativa a l' Ordre de Detenció Europea i als procediments d'entrega entre Estats Membres*. Tanmateix, en aquells àmbits en que no hi ha acords entre els Estats Membres, s'utilitzarà el Conveni. Igualment, els Estats Membres de la UE l'utilitzaran per relacionar-se amb tercers Estats, tenint en compte també possibles acords que puguin existir entre ells.

REFERÈNCIES BIBLIOGRÀFIQUES

LLIBRES I ARTICLES

- Alonso Moreda, Nicolás. *Cooperación Judicial en Materia penal en la Unión Europea: La "Euro Orden", Instrumento privilegiado de cooperación.* Pamplona: Aranzadi, 2016.

- Aguilera Morales, Marien, Alejandro Hernández López, Teresa Armenta Deu, Sandra Jiménez Arroyo, Raquel Borges Blázquez, Mar Jimeno Bulnes, Gianluca Borgia, María Elena Laro González, María José Cabezudo Bajo, Rubén López Picó, Serena Cacciatore, Francisco Matías Lázaro, Sonia Calaza López, Juan Alejandro Montoro Sánchez, Roser Casanova Martí, Jordi Nieva-Fenoll, Elisabet Cerrato Guri, Pilar Peiteado Mariscal, Montserrat de Hoyos Sancho, Enrique César Pérez, Luño Robledo, Lidia Domínguez Ruiz, Ana Sánchez Rubio, Lucana Estévez Mendoza, Mercedes Serrano Masip, Anna Fiodorova, Elisa Simó Soler, Pedro Miguel Freitas, M.ª Dolores Ramírez Benavente, Nicolás Rodríguez García, Francisco Salvador Gil García, María Isabel Romero Pradas, Luis Gomez Amigo, John A. E. Vervaele, María Isabel González Cano i Rocío Zafra Espinosa de los Monteros .*Orden Europea de Investigación y prueba transfronteriza en la Unión europea.* Dirigit por María Isabel González Cano. Valencia: Tirant lo Blanch, 2019.

- Anguita Osuna, José Enrique "Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea" *Revista de Estudios en Seguridad Internacional*, Vol. 4, No.1, 2018. Pg. 107-126 http://dx.doi.org/10.18847/1.7.7

- Armenta Deu, Maria Teresa. *Lecciones de Derecho Procesal* Penal. Madrid: Marcial Pons, 2019.

- Brenner, Susan. "La Convención sobre Cibercrimen del Consejo de Europa". *Revista chilena de Derecho y Tecnología; Universidad de Chile, Volumen I, Nro. I,* 2012. https://rchdt.uchile.cl/index.php/RCHDT/article/view/24030

- Díaz Gómez, Andrés "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest" *REDUR 8*, 169-203 (Desembre 2010) https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071

- Domínguez Ruiz, Lídia. *La Orden Europea de Investigación. Análisis legal y Aplicaciones Prácticas.* Valencia: Tirant lo Blanch, 2019.

- Fernàndez Bermejo, Daniel y Martinez Atienza, Gorgonio. *Ciberseguridad, ciberespacio y ciberdelincuencia.* Navarra: Aranzadi Thomson Reuters, 2018.

- Iulia Paul, Liana " European Cooperation in Fighting Cybercrime" *Fiat Iustitia* No. 1/2016 p 154- 159 (2016) https://econpapers.repec.org/article/dcujournl/v_3a10_3ay_3a2016_3ai_3a1_3ap_3a154-159.htm

- Lira Arteaga, Oscar Manuel. *Ciberdelitos: prespectivas para su persecución.* Ciudad de México: Tirant Lo Blanch, 2018.

- Llorente Sánchez-Arjona, Mercedes. *La Orden Europea de Investigación y su incorporación al derecho español.* Valencia: Tirant Lo Blanch, 2020.

- Montenegro, María Luisa. "Cooperación Internacional: Tramitación, obtención de pruebas, e incorporación de pruebas y evidencias" *Revista Jurídica Ministerio Público N°70.* (2017)

- Novoa Toledo, Ignacio i Venegas Cruz, Leonor *"Herramientas del Convenio de Budapest sobre ciberdelincuencia, y su adecuación a la legislación nacional*" Tesi Doctoral, Santiago de Chile, 2020.

- Quevedo González, Josefina. *"Investigación y prueba del ciberdelito"*. Tesi Doctoral, Universitat de Barcelona, 2017. https://www.tdx.cat/bitstream/handle/10803/665611/JQG_TESIS.pdf?sequence=1&isAllowed=y

- Velasco Nuñez, Eloy. *Delitos cometidos a través de internet, cuestiones procesales* . Madrid: La Ley, 2010.

- Weber, Amalie M. The Council of Europe's Convention on Cybercrime, *Berkeley Technology Law Journal* 18, no. 1, 2003. http://www.jstor.org/stable/24120528

INFORMES

- Comisión Europea. *Informe de la Comisión al Parlamento Europeo, al ConsejoEuropeo y al Consejo. Sexto informe de situación relativo a una Unión de la Seguridad genuina y efectiva*. Bruselas, 2017. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017DC0213

- Comisión Europea. *Informe de la Comisión al Parlamento Europeo, al Consejo Europeo y al Consejo. Noveno informe de situación relativo a una Unión de la seguridad genuina y efectiva*. Bruselas, 2017. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017DC0407

- Consell d'Europa. *Informe Explicatiu del Conveni sobre la Ciberdelinqüència*. https://rm.coe.int/16802fa403

- Eurojust. *Informe anual de Eurojust 2019*. The Hague: Eurojust, 2019. https://www.eurojust.europa.eu/sites/default/files/Publications/AnnualReport/AR2019_ES.pdf p. 42

- Europol, J-CAT. *J-CAT Factsheet 2020.* The Hague: Europol, 2021. https://www.europol.europa.eu/publications-documents/j-cat-factsheet-2020

- Europol. *Internet Organised Crime Threat Assessment 2020.* The Hague: Europol, 2020. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

- Europol. *The geographic Distribution of Cybercrime: Cybercrime heatmap*. 2016 https://www.europol.europa.eu/iocta/2016/distribution.html

- Greke, Marco. *Understanding Cybercrime: Phoenomena, challanges and legal response.* Ginebra: Telecomunication Developement Sector on International Telecommunication Union, 2006. http://cybercrime-fr.org/wp-content/uploads/2020/04/Understading-Cybercrime-ITU.pdf

- Parlamento Europeo, Comisión de Libertades Civiles, Justicia y Asuntos de Interior. *Informe sobre la lucha contra la ciberdelincuencia*. Bruselas, 2017. https://www.europarl.europa.eu/doceo/document/A-8-2017-0272_ES.html

- Steve Morgan. *2021 report: Cyberwarfare in the C-suite*. Estats Units: Cybersecurity Ventures, 2021. https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf

- Unión Internacional de Telecomunicaciones, Divisón de Aplicaciones TIC y Ciberseguridad. *El Ciberdelito: Guía para Países en Desarollo.* 2009. https://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf

COMUNICATS DE PREMSA DEL CONSELL DE LA UNIÓ EUROPEA

- Consell de la Unió Europea. *Actividades Informáticas malintencionades: el Consejo adopta unas Conslusiones.* Comunicat de premsa, 16 d'Abril de 2018. https://www.consilium.europa.eu/es/press/press-releases/2018/04/16/malicious-cyber-activities-council-adopts-conclusions/pdf

- Consell de la Unió Europea. *Ciberdefensa: El Consejo actualiza el marco político.* Comunicat de premsa, 19 de Novembre de 2018. https://www.consilium.europa.eu/es/press/press-releases/2018/11/19/cyber-defence-council-updates-policy-framework/pdf

- Consell de la Unió Europea. *Ciberseguridad de los dispositives conectados: el Consejo adopta unas conclusiones.* Comunicat de premsa, 2 de Desembre de 2020. https://www.consilium.europa.eu/es/press/press-releases/2020/12/02/cybersecurity-of-connected-devices-council-adopts-conclusions/pdf

- Consell de la Unió Europea. *Importancia de la tecnología 5G y riesgos para la Seguridad: El Consejo adopta unas conclusiones.* Comunicat de premsa, 3 de Desembre de 2019. thttps://www.consilium.europa.eu/es/press/press-releases/2019/12/03/significance-and-security-risks-of-5g-technology-council-adopts-conclusions/

- Consell de la Unió Europea. *La UE impone por primera vez sanciones en resupesta a los ciberataques.* Comunicat de premsa, 30 de Juny, 2020 https://www.consilium.europa.eu/es/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/

- Consell de la Unión Europea. *Nuevo Centro de Competencia en Ciberseguridad y nueva red: acuerdo informal con el Parlamento Europeo.* Comunicat de premsa, 11 de Desembre de 2020. https://www.consilium.europa.eu/es/press/press-releases/2020/12/11/new-cybersecurity-competence-centre-and-network-informal-agreement-with-the-european-parliament/

COMUNICACIONS DE LA COMISSIÓ EUROPEA

- Comissió de las Comunitats Europees. *Libro Blanco, "Competitividad, Empleo Retos y Pistas para entrar en el siglo XXI.* Suplemento 6/93. Luxemburg, 1993. http://evalua.catedu.es/documentos/aragon/NormativaVarios/LB1993CrecimientoCompetitividadYEmpleoI.pdf

- Comissió Europea. *Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones - Estrategia de Ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro.* Brussel·les, 2013. https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A52013JC0001

- Comissió Europea. *Comunicación de la Comisión al Consejo y al Parlamento Europeo: La represión del delito en la era digital: creación de un centro europeo de ciberdelincuencia.* Brussel·les, *2012. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52012DC0140*

- Comissió Europea. *Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones: Creación de una sociedad de la información más segura mediante la mejora de la Seguridad de las infraestructuras de información y la lucha contra los delitos informáticos*, Brussel·les, 2001. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52000DC0890

- Comissió Europea. *Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones, de 22 de mayo de 2007, "Hacia una política general de lucha contra la ciberdelincuencia".* Brussel·les: 2007. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:ES:PDF

- Comissió Europea. *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 30 de marzo de 2009, sobre protección de infraestructuras críticas de información: "Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, Seguridad y resistencia"*. Brussel·les, 2009. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52009DC0149&from=EN

- Comissió Europea. *Comunicación conjunta al Parlamento Europeo y al Consejo. Resiliencia, disuasión y defensa: fortalecer la Ciberseguridad de la UE*. Brussel·les, 2017. https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A52017JC0450

CONCLUSIONS DEL CONSELL DE LA UNIÓ EUROPEA

- Consell de la Unió Europea. *Conclusions of the Council of the European Union the European Judicial Cybercrime Network.* Brusel·les, 2016. https://data.consilium.europa.eu/doc/document/ST-10025-2016-INIT/en/pdf

- Consell de la Unió Europea. *Proyecto de Conclusiones del Consejo sobre la Estrategia de Ciberseguridad de la UE para la Década Digital.* Brusel·les, 2021. https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/es/pdf

PÀGINES WEB

- Centro Estadístico de Observación y Monitoreo de Ciberdelitos en Guatemala. *Historia del Cibercrimen.* 2019. Disponible a: https://ogdi.org/historia-del-cibercrimen

- CN-CERT Centro Criptológico Nacional. *Misión y Objetivos*. Disponible a: https://www.ccn-cert.cni.es/sobre-nosotros/mision-y-objetivos.html

- CSIRTs Network. *About CSIRTs Network*. Disponible a: https://csirtsnetwork.eu/

- Europol. *European Cybercrime Centre – EC3. Combating crime in a digital age*. 2021. Disponible a: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

- Europol. *Joint Cybercrime Action Taskforce (J-CAT).* 2021. Disponible a: https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce

- Florida Tech. *A Brief History of Cyber* Crime. 2020. Disponible a: https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/

- Observatorio Español de Delitos Informáticos. *Estadísticas de ciberdelitos en España*. 2020. Disponible a: https://oedi.es/estadisticas/

LEGISLACIÓ CONSULTADA

Normativa internacional:

- Conveni sobre Ciberdelinqüència, Budapest, 23 de Novembre de 2001 (BOE, núm. 226, 17-09-2010, pg. 78847 - 78896) https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf

Normativa comunitària:

- Reglament 2013/611/UE de la Comissió, de 14 de Juny de 2013, relatiu a mesures aplicables a la notificació de casos de violació de dades personals (DOUE L, núm. 173, 26-06-2013) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32013R0611&from=ES

- Reglament 2016/679/UE del Parlament Europeu i del Consell, de 27 d'Abril de 2016, relatiu a la protecció de les persones físiques pel que respecta el tractament de dades personals i la lliure circulació d'aquestes dades i pel que es deroga la Directiva 95/46/CE (DOUE L, núm. 119, 04-05-2016) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=es

- Reglament 2019/881/UE del Parlament Europeu i del Consell, de 17 d'Abril de 2019, relatiu a ENISA (Agència de la Unió Europea per la Ciberseguretat) i a la certificació de la ciberseguretat de les tecnologies de la Informació i la Comunicació i pel que es deroga el Reglament 526/2013/UE (DOUE L, núm. 151/15, 07-06-2019) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0881&from=es

- Reglament 460/2004/CE del Parlament Europeu i del Consell, de 10 de Març de 2004, pel que es crea l'Agència Europea de Seguretat de la Xarxa i la informació (DOUE L, núm. 77/1, 13-03-2004) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32004R0460&from=ESReglament 526/2013/UE

- Parlament Europeu i del Consell, de 21 Maig de 2013, relatiu a l'Agència de Seguretat de les Xarxes de la Informació de la Unió Europea (ENISA) i pel que es deroga el Reglamento 460/2004/CE (DOUE L, núm. 165/41,18-06-2013) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32013R0526&from=es

- Directiva 2002/58/CE del Parlament Europeu i del Consell, de 12 de Juliol de 2002, relativa al tractament de les dades personals i a la protecció de la intimitat al sector de les comunicacions electròniques (DOUE L, núm. 201, 31-07-2002) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32002L0058&from=ES

- Directiva 2006/24/CE del Parlament Europeu i del Consell, de 15 de Març de 2006, sobre conservació de dades generades o tractades en relació a la prestació de serveis de comunicacions electròniques d'accés públic o de xarxes públiques de comunicacions i per la que es modifica la Directiva 2002/58/CE (DOUE L, núm 105/54, 13-04-2006) https://www.boe.es/doue/2006/105/L00054-00063.pdf

- Directiva 2011/93/UE del Parlament Europeu i del Consell, de 13 de Desembre de 2011, relativa a la lluita contra els abusos sexuals i la explotació sexual dels menors i la pornografia infantil i per la que es substitueix la Decisió Marc 2004/68/JAI del Consell (DOUE L, núm. 335/1, 17-12-2011) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32011L0093&from=ES

- Directiva 2013/40/UE del Parlament Europeu i del Consell, de 12 d'Agost de 2013, relativa als atacs contra els sistemes d'informació i per la que es substitueix la Decisió Marc 2005/222/JAI del Consell (DOUE L, núm. 218/8, 14-08-2013) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32013L0040&from=ES

- Directiva 2014/41/CE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a l' Ordre Europea d'Investigació en matèria penal (DOUE L, núm. 130, 01-05-2014) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32014L0041&from=ES

- Directiva 2016/1148/UE del Parlament Europeu i del Consell, de 6 de Juliol de 2016, relativa a les mesures destinades a garantir un elevat nivell comú de seguretat de les xarxes i sistemes d'informació de la Unió (DOUE L, núm. 194, 19-07-2016) https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016L1148

- Directiva 2016/1148/UE del Parlament Europeu i del Consell, de 6 de Juliol de 2016, relativa a les mesures destinades a garantir un elevat nivell comú de seguretat de les xarxes i sistemes d'informació de la Unió (DOUE L, 194/1, 19-07-2016) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148&from=ES

- Directiva 2016/680/UE del Parlament Europeu i del Consell, de 27 d'Abril de 2016, relativa a la protecció de les persones físiques pel que respecta el tractament de dades personals per part de les autoritats competents per fins de prevenció, investigació, detecció o enjudiciament d'infraccions penals o d'execució de sancions penals, i a la lliure circulació d'aquestes dades i per la que es deroga la Decisió Marc 2008/977/JAI del Consell (DOUE L, núm. 119, 04-05-2016) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L0680&from=es

- Directiva 2017/541/UE del Parlament Europeu i del Consell, de 15 de Març de 2017, relativa a la lluita contra el terrorisme per la que es substitueix la Decisió Marc 2002/475/JAI del Consell i es modifica la Decisió 2005/675/JAI del Consell (DOUE L, núm. 88, 31-03-2017) https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32017L0541

- Directiva 2019/713/UE del Parlament Europeu i el Consell, de 17 d'Abril de 2019, sobre la lluita contra el frau i la falsificació de mitjans de pagament diferents a l'efectiu i per la que se substitueix la Decisió Marc 2001/413/JAI del Consell (DOUE L, núm. 123/18, 10-05-2019) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019L0713&from=en

- Directiva 95/46/CE del Parlament Europeu i del Consell, de 24 d'Octubre de 1995, relativa a la protecció de les persones físiques pel que respecta el tractament de dades personals i la lliure circulació d'aquestes dades (DOCE L. núm. 281, 23-11-1995) https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046

- Decisió 2000/375/JAI del Consell, de 29 de Maig de 2000, relativa a lluita contra la pornografia infantil a internet (DOCE L, núm. 138/1, 09-06-2000) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32000D0375&from=EN

- Decisió 2005/671/JAI del Consell, de 20 de Setembre de 2005, relativa a l'intercanvi d'informació i cooperació en relació a delictes de terrorisme (DOUE L, núm. 253/22, 29-09-2005) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32005D0671&from=GA

- Decisió 7299/2019 del Consell, de 16 de Maig de 2019, sobre mesures restrictives per lluitar contra els ciberatacs que amenacin a la Unió o als seus Estats Membres https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/es/pdf

- Decisió Marc 2001/413/JAI del Consell, de 28 de Maig de 2001, sobre la lluita contra el frau i la falsificació de mètodes de pagaments diferent a l'efectiu (DOCE L, núm. 149/1, 02-06-2001) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32001F0413&from=ES

- Decisió Marc 2002/475/JAI del Consell, de 13 de Juny de 2002, sobre la Lluita contra el terrorisme (DOUE L, núm. 164, 22-06-2002) https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002F0475:20081209:ES:PDF

- Decisió Marc 2002/584/JAI del Consell, del 13 de Juliol, relativa a l' Ordre de Detenció Europea i als procediments d'entrega entre Estats Membres (DOCE L, núm. 190/1, 18-07-2002) https://eur-lex.europa.eu/resource.html?uri=cellar:3b151647-772d-48b0-ad8c-0e4c78804c2e.0005.02/DOC_1&format=PDF

- Decisió Marc 2004/68/JAI del Consell, de 22 de Desembre de 2003, relativa a la lluita contra la explotació sexual dels nens i la pornografia infantil (DOUE L, núm. 13/44, 20-01-2004) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32004F0068&from=FR

- Decisió marc 2005/222/JAI del Consell, de 24 de Febrer de 2005, relativa als atacs contra els sistemes d'informació (DOUE L, núm. 69/67, 16-03-2005) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32005F0222&from=ES

- Decisió Marc 2008/977/JAI del Consell, de 27 de Novembre de 2008, relativa a la protecció de dades personals tractades en el marc de la cooperació policial i judicial en matèria penal (DOUE L, núm. 350, 20-12-2008) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32008F0977&from=ES

- Comissió Europea. *Recomendación de la Comisión de 13.9.2017 sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala.* Brussel·les, 2017. https://ec.europa.eu/transparency/regdoc/rep/3/2017/ES/C-2017-6100-F1-ES-MAIN-PART-1.PDF

- Consell d'Europa. *Recommendation No. R (95) 13 of the Committee of Ministers to Member States concerning probems of criminal procedure law connected with information technology*. Brusel·les, 1995. https://rm.coe.int/16804f6e76

- Consell d'Europa. *Recommendation No. R(89) 9 of the Committee of Ministers to Member States on Computer-related crime*. Brusel·les, 1989. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f1094

Normativa nacional:

- Llei orgànica, 10/1995, de 23 de Novembre, del Codi Penal. (BOE, núm. 281, 24-11-1995, pg. 33987-34058)