Ciberterrorisme. Regulació i estratègies per combatre'l

PID_00272605

Josep Maria Tamarit Sumalla
Nasserine Montornés Mataoui
Ma. del Carme Guirao Cid

Temps mínim de dedicació recomanat: 3 hores

Universitat Oberta de Catalunya

Josep Maria Tamarit Sumalla

Catedràtic de Dret penal a la Universitat Oberta de Catalunya, on és director del Màster en Ciberdelinqüència. La seva activitat de recerca ha estat centrada bàsicament en aspectes relacionats amb la victimologia, la justícia restaurativa i el sistema de sancions penals. Té també diverses publicacions relacionades amb la delinqüència de motivació ideològica i els delictes d'odi. És coordinador del Grup consolidat de recerca sobre el Sistema de justícia penal.

Nasserine Montornés Mataoui

Graduada en criminologia per la UOC i Màster en Sistema de Justícia Penal a la Universitat de Lleida. S'està formant a l'Institut de Seguretat Pública de Catalunya i és tutora del Màster en Ciberdelinqüència de la UOC.

Ma. del Carme Guirao Cid

Graduada en Criminologia per la UOC i Màster en drets humans per la mateixa Universitat. Es becària predoctoral a la Universitat de Lleida, on realitza la seva tesi doctoral sobre adoctrinament i victimització terrorista, tema respecte al qual ha publicat dos articles (2018; 2019).

L'encàrrec i la creació d'aquest recurs d'aprenentatge UOC han estat coordinats pel professor: Josep Maria Tamarit Sumalla (2020)

Primera edició: febrer 2020

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

Índex

Introducció

El ciberterrorisme s'ha convertit en una de les principals preocupacions per a la comunitat internacional. Amb l'ús de les eines cibernètiques els patrons de conducta dels terroristes són cada vegada més difícils de predir, en poder desenvolupar les seves accions en qualsevol dels il·limitats àmbits del ciberespai. A continuació farem referència a la *Deep Web* i a la *Dark Net*, posant especial èmfasi en el sistema TOR (*The Onion Router*) per ser el més utilitzat per part de les organitzacions terroristes, ja que permet als seus usuaris actuar sota l'anonimat.

La inseguretat més gran que genera el ciberterrorisme es deu a la seva elevada capacitat per adaptar-se a nous contextos (inclosos els cibernètics), i pel fet de disposar de sistemes informàtics prou desenvolupats per penetrar en els sistemes de seguretat estatals o institucionals, la qual cosa produeix un dany considerable. Donada la inseguretat que generen les seves accions, el ciberterrorisme té cada vegada més protagonisme en les agendes polítiques dels diferents Estats. No obstant això, de la mateixa manera que ocorria amb la definició de ciberterrorisme, actualment no existeix cap instrument legal que hagi adquirit el consens necessari perquè l'ús malintencionat d'internet per part de les organitzacions terroristes acabi sent castigat a través d'un únic tipus. Per aquest motiu, la regulació jurídica del terrorisme ha tendit a desenvolupar-se des d'un àmbit nacional i pensant en el terrorisme fora de línia. No obstant això, el contingut de les normes penals ha anat modificant-se cada vegada que s'ha produït un nou atemptat, i diverses vegades han estat fortament criticades en considerar que alguns dels seus articles violen determinats drets i llibertats fonamentals, i els relatius a la llibertat d'expressió són els més perjudicats.

En l'àmbit internacional, una llei antiterrorista que va marcar una fita va ser la USA Patriot Act (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*). Després dels atemptats de l'11-S, els Estats Units van adoptar amb aquesta nova normativa una sèrie de mesures destinades a restringir drets i llibertats sota el pretext de la seguretat. A partir d'aquesta llei, queda permès a les autoritats perseguir, capturar, empresonar i interrogar a sospitosos de terrorisme a tot el món, escoltar les comunicacions sense intervenció judicial i negar l'entrada al país a individus sospitosos de pertànyer a una organització terrorista, entre altres. Amb la finalitat de suavitzar aquestes restriccions sobre les llibertats individuals, el 2015 aquesta llei va ser substituïda per la USA Freedom Act, que va afectar, principalment, la gestió i l'emmagatzematge d'informació i dades dels ciutadans nord-americans per part dels serveis d'intel·ligència. Posteriorment, a manera de reflex, han anat sorgint altres lleis en altres països, com la llei antiterrorista francesa que va impulsar François Hollande després de l'onada d'atemptats que van tenir lloc a la capital parisenca el novembre del 2015. Aquesta va concedir amplis poders al

Ministeri de l'Interior, tals com realitzar registres domiciliaris basats en meres sospites i sense necessitat d'una ordre judicial prèvia, arrestos domiciliaris, i l'obligació de presentar-se diàriament a comissaria. Tot això va ser conseqüència de l'estat d'excepció que va durar fins a finals del 2017, quan una nova majoria parlamentària, sota la presidència d'Emmanuel Macron, va aprovar una nova llei que el va cancel·lar. No obstant això, es mantenen alguns dels aspectes més criticats, com la limitació de moviment, la potestat policial de realitzar registres sense ordre judicial (encara que limita la seva execució de les 6 del matí a les 9 de la nit) o la facultat governamental per tancar aquells llocs de culte on se sospiti que s'exposin idees o llancin missatges que alimentin la violència.

Aquestes no van ser les úniques iniciatives polèmiques. En l'àmbit de la Unió Europea, destaca la Directiva de 21 d'abril del 2016 aprovada pel Parlament Europeu amb l'objectiu de crear un registre de noms de passatgers aeris (*Passenger Name Record* o PNR) com una eina més en la lluita antiterrorista, partint del fet que les activitats terroristes (i de delinqüència organitzada) comporten desplaçaments internacionals. Atès que dins de l'espai Schengen no existeix restricció de moviments per als ciutadans dels Estats membres, la directiva va establir poder dur a terme un control i intercanvi entre autoritats policials sobre les dades dels passatgers de les aerolínies. En total, el PNR recopila fins a 19 variables d'informació sobre el passatger, com l'itinerari, el nom i les dades de contacte, els detalls de pagament, l'agència de viatges, l'equipatge i el nombre de seient, entre altres. Totes aquestes iniciatives seran examinades al llarg de les pàgines següents basant-nos en gran mesura en els punts II, III i IV del document de la UNODC, ***L'ús d'internet amb finalitats terroristes***.

Objectius

Els objectius que es pretenen aconseguir en concloure l'estudi del present mòdul sobre regulació i estratègies per combatre el ciberterrorisme són:

1. Conèixer la vinculació de la *Deep Web* i la *Dark Web* amb el ciberterrorisme.

2. Conèixer el sistema TOR i el seu important paper en el ciberterrorisme.

3. Conèixer l'evolució de la legislació antiterrorista en l'àmbit internacional.

4. Descriure el contingut de les principals lleis antiterroristes a Espanya i la seva aplicació al camp del ciberterrorisme.

5. Conèixer les principals estratègies desenvolupades per fer front al ciberterrorisme.

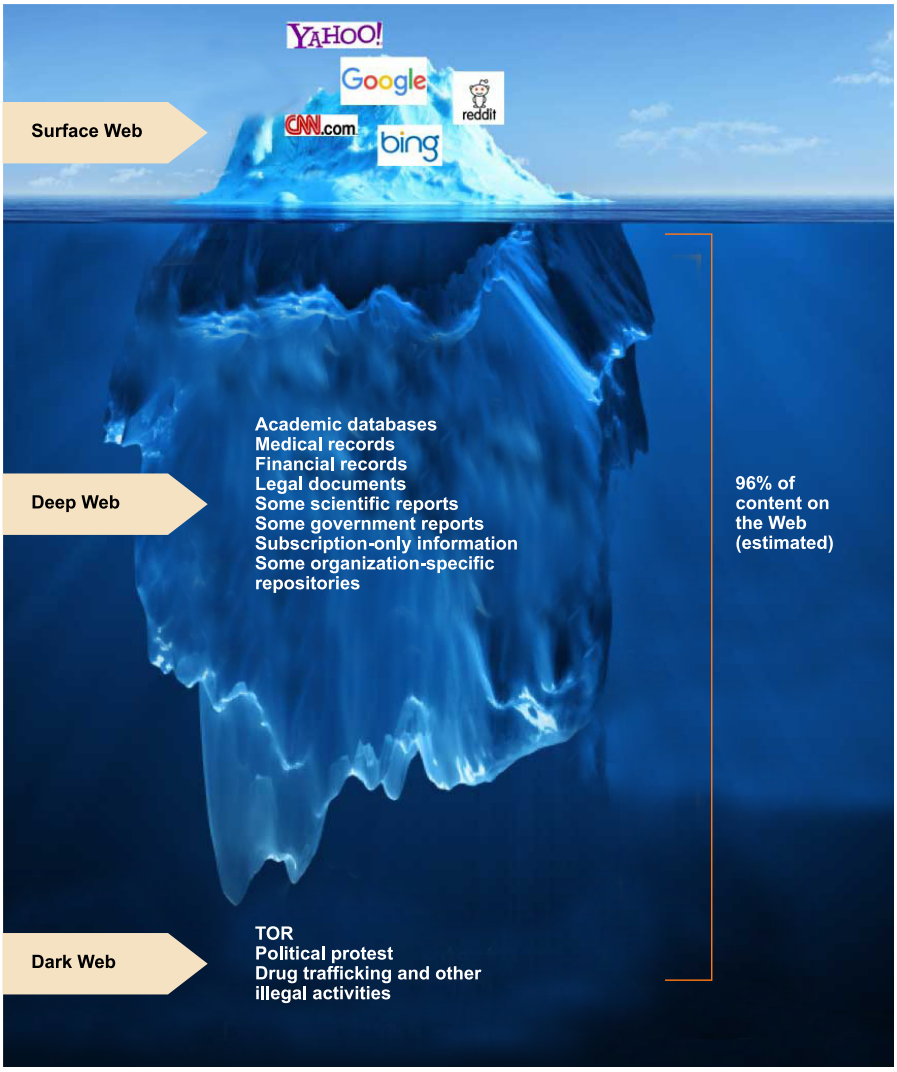
1. Les diverses capes d'internet

Quan naveguem per internet, a través del navegador Google o Yahoo la majoria de vegades, és probable que pensem que tot és aquí i que ho podem consultar amb prou feines en uns segons. Tanmateix, això no és així. El que veiem (o millor dit, al que accedim) és la *clear net* o *surface net*. El ciberespai que consultem en el nostre dia a dia solament representa una mínima part de la realitat que s'hi alberga, ja que molt material queda ocult. Solament aquelles persones amb el coneixement adequat poden submergir-se i explorar el fons de la xarxa. Entre elles hi ha els membres d'organitzacions terroristes. No obstant això, hem d'aclarir que l'espai profund de la xarxa no solament s'utilitza per a finalitats il·lícites com la compra i venda d'armes o drogues o l'intercanvi de material pornogràfic, ja que s'hi poden realitzar moltes altres activitats amb una altra classe de finalitats.

1.1. Definició i delimitació de conceptes

El ciberespai que existeix més enllà de navegadors com Google o Firefox és el que es coneix com a web profund o web fosc (pels seus noms en anglès *Deep Web* i *Dark Web*). A aquesta fracció de ciberespai no hi podem accedir a través de cercadors habituals, atès que es requereixen unes determinades plataformes per arribar-hi. Aquest és el principal motiu pel qual aquests espais resulten molt atractius per als terroristes i per cometre delictes en general. Segons estudiem en el primer mòdul, una de les característiques que definien el ciberespai era l'anonimat, i precisament aquestes eines el garanteixen. El seu ús no deixa rastre susceptible de ser detectat, *a priori*, pels cossos i les forces de seguretat. A continuació entrarem en les profunditats de la xarxa per prendre consciència que hi ha ciberactivitat més enllà de la *clear net*. A més, creiem que el contingut d'aquest apartat pot ser més profitós de cara a l'estudi si presentem les diferents capes o els diferents nivells de la xarxa sota la «metàfora de l'iceberg», atès que el material que nosaltres consultem és una ínfima part de l'extensió real del ciberespai, i el 96 %, aproximadament, del seu contingut queda ocult.

Figura 1. Els diferents nivells d'internet segons la figura d'un iceberg



1.2. *Deep Web*

El terme *Deep Web* (o web profund) va ser utilitzat per primera vegada per Mike K. Bergman quan es va adonar que realitzar una cerca per internet podia ser una mica més complicat del que indicava l'aparença i que incloïa altres espais que no eren visibles o accessibles per a la majoria dels usuaris. Aquestes conclusions derivaven d'un estudi que va realitzar el 2001 en el qual va comprovar que la *clear net* contenia 19 terabytes (TB) d'informació, mentre que la *Deep Web* era de 7.500, la qual cosa evidenciava que en aquesta ubicació la informació existent era, aproximadament, 400 vegades superior (Bergman, 2001).

A la *Deep Web* se li sol atribuir connotacions pejoratives, donada la creença majoritàriament compartida que defensa que s'hi realitzen tot tipus d'activitats il·legals com, per exemple, la compravenda de materials il·lícits, l'intercanvi de material pornogràfic, etc. Tanmateix, això no és així. La *Deep Web* alberga majoritàriament contingut sensible referent als ciutadans, per exemple, dades mèdiques, comptes bancaris, infraccions administratives o penals, etc. De la mateixa manera, nosaltres, quan utilitzem aplicacions com Dropbox o Goo-

gle Drive per desar o compartir documents, fotos o vídeos també estem utilitzant aquesta capa d'internet. Fixem-nos que per poder-hi accedir ens demanen claus de seguretat que ens redirigeixen automàticament a altres servidors. Per tant, definirem la *Deep Web* com:

> Part del web que hi ha sota la *clear net*, el contingut del qual no està indexat per motors de cerca convencionals o més utilitzats, i que està protegit per claus de seguretat, aquest fet en dificulta el rastreig.

1.3. *Dark Web* i *Dark Net*

La *Dark Net* (o web fosc) és l'últim nivell que hem presentat a través del gràfic de l'iceberg i forma part de la *Deep Web*. No obstant això, a diferència d'aquesta, per accedir a la *Dark Web* no es requereix solament un codi de seguretat, sinó uns navegadors determinats, i TOR és el més utilitzat per ciberdelinquents, incloses les organitzacions terroristes. A més d'aquest també n'hi ha d'altres com IP2, ZeroNet o Freenet.

DuckDuckGo

DuckDuckGo (DDG) és un cercador similar a Google, desenvolupat a Pennsilvània per Gabriel Weinberg (Estats Units), però que a diferència dels existents garanteix la privadesa a l'usuari. És a dir, l'activitat que hi puguem dur a terme no queda registrada. Per aquest motiu, any rere any, va guanyant popularitat enfront d'altres motors de cerca com els anteriorment citats. D'altra banda, quan parlem de **The Hidden Wiki** fem referència al directori de llocs web que operen sota el domini «.onion» el contingut del qual pot ser editat de forma anònima per qualsevol persona. Com us haureu adonat, es tracta d'una estructura que opera de forma similar a com ho fa la Wiquipèdia.

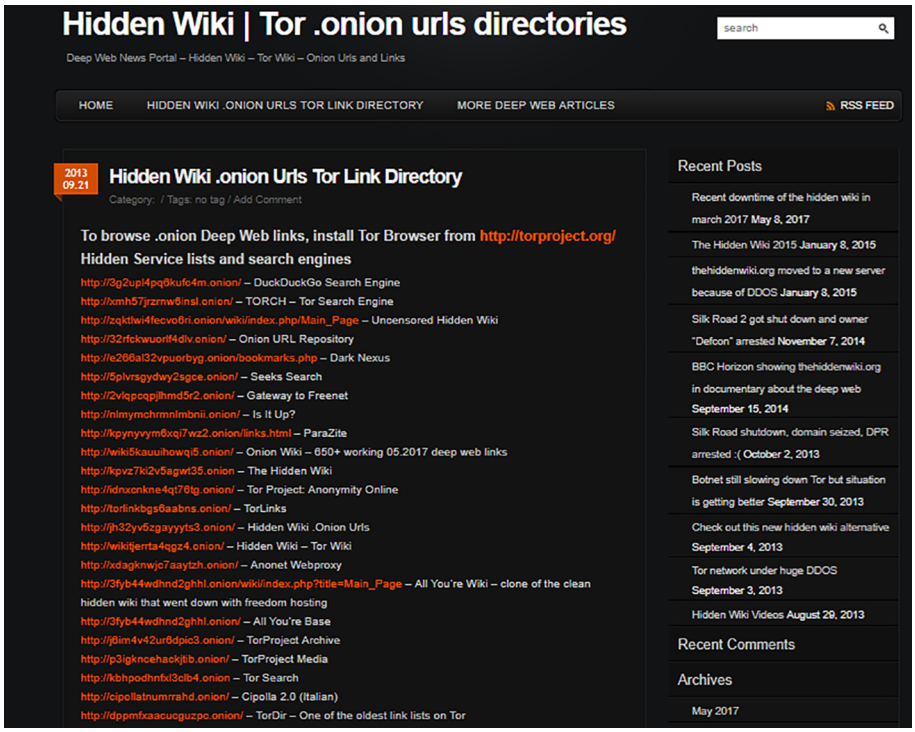
Com hem esmentat a l'inici, TOR és l'abreviatura de *The Onion Router*, un projecte que es va iniciar amb l'objectiu de crear una xarxa de comunicacions paral·lela, i de nivell superior, a l'internet popularment concebut, de manera que mai es poguessin conèixer les dades dels seus usuaris, i es mantingués, així, com una xarxa privada i anònima. Això s'aconsegueix perquè no utilitza una xarxa P2P («*peer to peer*», o punt a punt), com sí que utilitzen els motors de cerca convencionals. Això permet a l'usuari poder accedir, consultar o enviar informació per vies independents de la *clear net*. Tanmateix, això no significa que sigui una eina il·legal.

A la *Dark Web* s'hi pot accedir directament a través de The Hidden Wiki, DuckDuckGo o Tor Browsrer Bundle. No obstant això, no és recomanable fer-ho, donades les conseqüències que pot implicar. El consell que ha de donar-se a tot usuari, fins i tot als qui pretenguin estudiar la ciberdelinqüència, és que es limiti a navegar per entorns de xarxa segurs i coneguts.

Dins de la *Dark Web* trobem les *Dark Net*, xarxes a les quals solament s'hi pot accedir a través d'aquest tipus de servidors i que porten com a domini «.onion» i no l'habitual «.com», la qual cosa impedeix accedir al seu contingut a totes les persones que no tinguin en el seu dispositiu el navegador TOR.

Com a mostra, podeu veure la captura de pantalla següent.

Figura 2. Captura de pantalla de l'escriptori de Hidden Wiki amb dominis «.onion»



L'ús de la *Dark Web* per part de les organitzacions terroristes va en augment a causa de les condicions de seguretat i l'anonimat que els garanteixen aquestes eines, així com als elevats recursos que poden trobar en el seu interior que els són útils per potenciar les seves activitats.

1.4. La criptomoneda

Un altre aspecte relacionat amb el contingut de l'apartat anterior són les criptomonedes.

> Per definició, les criptomonedes són monedes que no reben cap tipus de supervisió per part de cap organisme o banc central (és a dir, descentralitzades) que s'intercanvien a través de xarxes P2P i que estan xifrades.

Aquestes característiques permeten que les transaccions puguin realitzar-se sense intermediaris, i que, en conseqüència, siguin molt difícils de rastrejar, inclosa la informació de l'import, la identitat del pagador i del beneficiari i l'objecte.

Són exemples els bitcoins o el *dash*. Aquest últim és més complex tècnicament parlant i, per tant, constitueix un instrument més difícil de traçar per part dels cossos i les forces de seguretat.

Tot això les ha convertit en un mitjà de pagament segur i atractiu per a les organitzacions terroristes, en poder sortejar els perills que presenta el pagament en metàl·lic. A aquest mitjà se li afegeixen les facilitats que ofereixen les targetes de crèdit i l'aparició de plataformes com PayPal, encara que aquestes suposen un risc més gran si es comparen amb la criptomoneda.

2. Ciberseguretat i normativa sobre (ciber)terrorisme

2.1. Prevenció i ciberseguretat

El ciberterrorisme cada vegada genera més preocupació, però la complexitat del fenomen, els diversos actors implicats i els interessos per part d'Estats dificulten la consecució d'una normativa comuna en l'àmbit internacional que sigui eficaç per fer front al ciberterrorisme i que alhora sigui respectuosa amb els drets i les llibertats dels ciutadans. Donades aquestes circumstàncies, la defensa més efectiva és la ciberseguretat, l'objectiu de la qual és minimitzar el risc aplicant una sèrie de mesures de prevenció.

A continuació descriurem les mesures en matèria de ciberseguretat elaborades per part d'organismes i institucions internacionals amb l'objectiu de fer front a les ciberamenaces i els atacs per part d'organitzacions terroristes. Al tercer apartat del mòdul es farà una breu descripció dels organismes (amb l'enllaç a les pàgines corresponents) més importants que treballen per complir amb el mandat de les normes sobre ciberseguretat.

2.2. Normativa internacional

Com que no existeix un document vinculant de caràcter universal, ens limitarem a citar la resolució més important de l'ONU i a recomanar la lectura del punt 2 («El context internacional») del document ***L'ús d'internet amb finalitats terroristes de la UNODC***.

El document més important en matèria de terrorisme és el contingut de l'**EstratègiaGlobal contra el terrorisme** (A/RE/60/288) que va aprovar el 2006 l'Assemblea General, i el contingut de la qual alberga tot un conjunt d'iniciatives i programes que tenen com a objectius:

Enllaç recomanat

Per conèixer més en profunditat el seu contingut, podeu consultar l'enllaç següent: Estratègia global de les Nacions Unides contra el terrorisme, https://undocs.org/es/a/res/60/288.

1) Fer front a les condicions que propicien la propagació del terrorisme.

2) Prevenir i combatre el terrorisme.

3) Desenvolupar la capacitat dels Estats membres per prevenir i combatre el terrorisme i enfortir el paper del sistema de les Nacions Unides sobre aquest tema.

4) Garantir el respecte universal dels drets humans i de l'estat de dret com a pilar fonamental de la lluita contra el terrorisme.

2.3. Normativa europea

Donada la conscienciació que s'ha desenvolupat a Europa sobre la importància de lluitar contra la ciberdelinqüència i garantir un ciberespai segur, descriurem les normes més importants en matèria de ciberseguretat. S'indiquen, en primer lloc, les normes produïdes al si del Consell d'Europa i, en segon lloc, la normativa de la Unió Europea.

1) Conveni sobre el delicte cibernètic. El 2001 el Consell d'Europa va elaborar aquest document que, tot i que amb continguts mínims, és actualment l'únic instrument que tracta sobre l'activitat delictiva a internet. El seu contingut ha de ser interpretat conjuntament amb altres eines jurídiques que busquen la mateixa fi. Solament així es podrà elaborar una base jurídica fonamentada en la cooperació que busqui detenir l'ús d'internet amb finalitats terroristes.

Enllaç recomanat

Per conèixer més en profunditat el seu contingut, podeu consultar l'enllaç següent: Conveni sobre el delicte cibernètic, https://www.boe.es/diario_boe/txt.php?id=boe-a-2010-14221.

L'objectiu principal que vol aconseguir el conveni és harmonitzar les diferents legislacions nacionals existents sobre delictes cibernètics per millorar els mecanismes de detecció, recerca i persecució, la qual cosa inclou l'obligació dels Estats d'elaborar que persegueixin aquesta fi. El conveni entén per «delicte cibernètic» els delictes relacionats amb l'accés no autoritzat a sistemes, programes o dades informàtiques, i la manipulació il·lícita d'aquests; el frau i la falsificació informàtics, i la temptativa de cometre tals actes o la complicitat en la seva comissió.

2) Decisió Marc 2002/475/JAI, de 13 de juny de 2002, sobre la lluita contra el terrorisme, que harmonitza la definició dels delictes de terrorisme en tots els Estats membres de la Unió Europea. En resposta a la creixent amenaça terrorista, el 2002, el Consell de la Unió Europea va elaborar aquest document, a través del qual va introduir una definició específica i comuna del concepte de delicte de terrorisme, entenent-lo com «[...] delictes greus que es converteixen en delictes de terrorisme per raó de la intencionalitat del delinqüent. El concepte de delicte de terrorisme és, per tant, una combinació de dos elements: un element objectiu, ja que es refereix a una relació de conductes delictives greus, tal com es defineixen conforme a la legislació nacional, i un element subjectiu, ja que aquests actes es consideraran delictes de terrorisme quan es cometin amb una intenció determinada [...]» –article 3–; aquesta decisió va establir un conjunt de normes amb l'objectiu de garantir que els delictes terroristes es perseguissin de manera eficaç i va establir mesures concretes dirigides a víctimes de delictes de terrorisme. No obstant això, cal dir que aquesta decisió marc s'ha substituït per la Directiva (UE) 2017/541 del Parlament Europeu i del Consell, de 15 de març de 2017, relativa a la lluita contra el terrorisme, la qual veurem en aquest mateix apartat.

3) Decisió Marc 2005/222/JAI, relativa als atacs contra els sistemes d'informació. La Decisió del 2005 s'havia elaborat com a resposta a l'amenaça de la delinqüència organitzada i la inquietud davant la possibilitat d'atacs ter-

roristes contra els sistemes d'informació que formen part d'infraestructures vitals dels Estats membres de la Unió, deixant a cada Estat que legisli sobre aquest tema. Encara que de la mateixa manera que l'anterior decisió marc, aquesta va ser substituïda a través de la Directiva 2013/40/UE del Parlament Europeu i del Consell, de 12 d'agost del 2013, relativa als atacs contra els sistemes d'informació.

4) Decisió Marc de 24 d'octubre del 2008, relativa a la lluita contra la delinqüència organitzada (2008/841/JHA). Tres anys després de l'anterior, la Decisió Marc 2008/841 sorgeix com a substitució a l'Acció Comuna 98/733/JAI, de 21 de desembre del 1998, relativa a la tipificació penal de la participació en una organització delictiva en els Estats membres de la Unió Europea. Té per objecte donar resposta al compromís que es va establir en l'àmbit de la lluita contra el terrorisme, que, donada la naturalesa del fenomen, requereix reforçar els programes de lluita contra la delinqüència organitzada.

Enllaç recomanat

Per conèixer més en profunditat el seu contingut, podeu consultar l'enllaç següent: Decisió Marc de 24 d'octubre del 2008, http://data.europa.eu/eli/dec_framw/ 2008/841/oj.

L'article més important és el número **2**, en plasmar la voluntat del document. Concretament manifesta que:

> «Tots els Estats membres adoptaran les mesures necessàries per tipificar com a delicte a un o tots dos dels tipus de conducta següents relacionats amb una organització delictiva: (a) la conducta de tota persona que, de manera intencionada i sabent la finalitat i activitat general de l'organització delictiva o de la seva intenció de cometre els delictes en qüestió, participi activament en les activitats il·lícites de l'organització, inclosa la facilitació d'informació o de mitjans materials, reclutant a nous participants, així com en tota forma de finançament de les seves activitats sabent que la seva participació contribuirà a l'assoliment de la finalitat delictiva d'aquesta organització; (b) la conducta de tota persona que consisteixi en un acord amb una o més persones per procedir a una activitat que, de ser duta a terme, suposi la comissió del delicte [...]. Per tant, el que ens ve a dir és que tots els Estats membres adoptin les mesures necessàries per tipificar com a delicte les conductes pròpies d'organitzacions delictives».

5) Decisió Marc de 28 de novembre (2008/919/JAI), relativa a la lluita contra el terrorisme. Neix després de l'aparició de cèl·lules terroristes no estructurades, no jeràrquiques, semiautònomes i lligades entre elles en xarxa que recorrien a les noves tecnologies per comunicar-se, captar nous membres i mobilitzar-se. No obstant això, heu de saber que el 2017 aquesta va ser substituïda per la Directiva 2017/541, que veurem més endavant.

De la mateixa manera que hem vist en l'anterior decisió marc, aquest nou document exposa en **l'article 3** que els Estats membres han d'adoptar totes aquelles mesures que estimin necessàries per garantir la seguretat dels seus ciutadans, la qual cosa implica tipificar com a delicte de terrorisme totes aquelles conductes que:

- Atemptin contra la vida o la integritat física d'una persona;
- El segrest o la presa d'ostatges;
- L'apoderament il·lícit d'aeronaus i de bucs o d'altres mitjans de transport col·lectiu o de mercaderies;
- La fabricació, la tinença, l'adquisició, el transport, el subministrament o la utilització d'explosius o armes de foc, armes químiques, biològiques, radi-

ològiques o nuclears inclusivament, així com la recerca i el desenvolupament d'armes químiques, biològiques, radiològiques o nuclears; i/o
- L'alliberament de substàncies perilloses, o la provocació d'incendis, inundacions o explosions l'efecte de les quals sigui posar en perill vides humanes.

Si bé totes aquestes conductes són més susceptibles de ser realitzades al món real, en la modalitat en línia cobra especial importància el contingut dels apartats d) i h) del mateix article segons els quals també ha de considerar-se delicte de terrorisme:

- (apartat d) les destruccions massives d'instal·lacions estatals o públiques, sistemes de transport, infraestructures, sistemes informàtics inclosos, plataformes fixes emplaçades en la plataforma continental, llocs públics o propietats privades, que puguin posar en perill vides humanes o produir un gran perjudici econòmic; i
- (apartat h) la pertorbació o interrupció del subministrament d'aigua, electricitat o un altre recurs natural bàsic l'efecte del qual sigui posar en perill vides humanes. Accions que, d'acord amb el mòdul 1, són susceptibles de ser definides de ciberterrorisme si són realitzades a través de mitjans informàtics.

D'altra banda, destaquem el contingut de l'article **5** («Provocació pública a la comissió d'un delicte de terrorisme»), ja que defensa que les mesures necessàries per garantir que es tipifiqui com a delicte també han d'incorporar «[...] el fet de difondre o fer públics per qualsevol altre mitjà, ja sigui en línia o no [...]»; l'article **21** («Mesures contra els continguts en línia que constitueixin provocació pública»), on s'exposa que «Els Estats membres adoptaran les mesures necessàries per garantir la ràpida eliminació dels continguts en línia albergats al seu territori [...]» o « [...] els Estats membres podran adoptar mesures per bloquejar l'accés a aquest contingut per part dels usuaris d'internet dins del seu territori».

Donada la importància d'aquest document, és necessari saber com la Unió Europea defineix «infraestructura crítica». Segons el Programa d'Infraestructures Crítiques, aquestes són:

> «aquelles instal·lacions, xarxes, aquells serveis i equips físics i de tecnologia de la informació la interrupció o destrucció dels quals tindria un impacte més gran en la salut, la seguretat o el benestar econòmic dels ciutadans o en l'eficaç funcionament dels Governs dels Estats membres».

Al seu torn, aquestes les podem classificar atenent a dos criteris: segons propietat (pública o privada); i segons criteris sectorials (centrals i xarxes d'energia; tecnologies de les comunicacions i la informació; finances; salut; alimentació; aigua; transport; producció, emmagatzematge i transport de mercaderies perilloses). No obstant això, la UE és conscient que en plena globalització la delimitació territorial és confusa i difícil, i que és millor parlar d'interdependència, un aspecte que les fa ser vulnerables a possibles ciberatacs terroristes. Per aquest motiu, si es vol protegir aquest tipus d'infraestructures, es requereix un treball cooperatiu i sincronitzat, raó per la qual es va crear la Xarxa d'Alertes en Infraestructures Crítiques (CIWIN o Critical Infraestructures Warning Information Network).

6) Directiva 2013/40/UE del Parlament Europeu i del Consell, de 12 d'agost del 2013 relativa als atacs contra els sistemes d'informació i per la qual se substitueix la Decisió Marc 2005/222/JAI del Consell. La Directiva esmentada té com a objectiu el d'aproximar les normes de dret penal dels Estats membres en matèria d'atacs contra els sistemes d'informació, mitjançant l'establiment de normes mínimes relatives a la definició de les infraccions penals i les sancions aplicables, i millorar, així, la cooperació entre les autoritats competents, inclosa la policia i els altres serveis especialitzats encarregats de l'aplicació de la llei als Estats membres, així com els organismes especialitzats de la Unió, com Eurojust, Europol i el seu Centre Europeu contra la Ciberdelinqüència i l'Agència Europea de Seguretat de les Xarxes i de la Informació (ENISA).

Els sistemes d'informació són un element essencial per a la interacció política, social i econòmica a la Unió, i l'augment d'aquests porta a la directiva a posar èmfasi en la seva definició per després considerar aspectes com les infraestructures crítiques, els atacs de gran escala i els ciberatacs. És important, per tant, en aquesta matèria disposar de definicions comunes, a fi de garantir l'aplicació coherent de la Directiva en els Estats membres.

Les diferències i divergències significatives que existeixen entre les legislacions i els processos penals dels Estats membres en aquest àmbit poden dificultar la lluita contra la delinqüència organitzada i el terrorisme, i complicar la cooperació policial i judicial efectiva en aquest àmbit. La naturalesa transnacional i transfronterera dels moderns sistemes d'informació significa que els atacs solen revestir un caràcter transfronterer, la qual cosa planteja la necessitat urgent de prosseguir l'aproximació del dret penal en aquest àmbit.

Per tant, l'objectiu principal de la Directiva és el de garantir que els atacs contra els sistemes d'informació siguin castigats en tots els Estats membres amb penes efectives, proporcionades i dissuasòries, i millorar i fomentar la cooperació judicial entre les autoritats judicials i altres autoritats competents, atès que no

Lectures recomanades

Per a una anàlisi més profunda, podeu consultar:

J. L. González Cussac (2006). «El Derecho Penal frente al Terrorismo». En: J. L. Gómez Colomer; J. L. González Cussac. *Terrorismo y proceso penal acusatorio*. València: Tirant lo Blanch.

I. Agudo Fernández; M. Jaén; A. Perrini (2016). «Los delitos de terrorismo en el Código Penal». En: *Terrorismo en el siglo XXI: La respuesta penal en el escenario mundial*. Madrid: Dykinson.

R. García Albero; G. Quintero (dir.) (2016). *Comentarios a la parte especial del Derecho Penal* (7.ª ed.). Cizur Menor: Aranzadi.

Enllaç recomanat

Per a conèixer més en profunditat el seu contingut pot consultar-se 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 qual se substitueix la Decisió marc 2005/222/JAI del Consell. Enllaç:

http://data.europa.eu/eli/dir/2013/40/oj.

poden ser aconseguits de manera suficient pels Estats membres, i que, per tant, a causa de les seves dimensions o dels seus efectes, poden aconseguir-se millor a escala de la Unió.

7) Directiva (UE) 2016/1148 del Parlament Europeu i del Consell, de 6 de juliol del 2016, relativa a les mesures destinades a garantir un elevat nivell comú de seguretat de les xarxes i dels sistemes d'informació a la Unió. Les xarxes i els sistemes d'informació exerceixen un paper crucial a la societat. La seva fiabilitat i seguretat són essencials per a les activitats econòmiques i socials, i en particular per al funcionament del mercat interior de la UE. Així mateix, la magnitud, la freqüència i els efectes dels incidents de seguretat s'estan incrementant i representen una greu amenaça per al funcionament de les xarxes i dels sistemes d'informació. Aquests sistemes poden convertir-se, a més, en objectiu d'accions nocives deliberades destinades a perjudicar o interrompre el seu funcionament. Aquest tipus d'incidents pot interrompre les activitats econòmiques, generar considerables pèrdues financeres, menyscabar la confiança de l'usuari i causar grans danys a l'economia de la Unió.

Per això, la Directiva estableix mesures amb l'objecte d'aconseguir un elevat nivell comú de seguretat de les xarxes i dels sistemes d'informació dins de la Unió, a fi de millorar el funcionament del mercat interior. Per a aquesta finalitat, la Directiva:

- Estableix obligacions per a tots els Estats membres d'adoptar una estratègia nacional de seguretat de les xarxes i dels sistemes d'informació;
- Crea un grup de cooperació per donar suport i facilitar la cooperació estratègica i l'intercanvi d'informació entre els Estats membres i desenvolupar la confiança i seguretat entre ells;
- Crea una xarxa d'equips de resposta a incidents de seguretat informàtica (en endavant, «xarxa de CSIRT», per les seves sigles en anglès Computer Security Incident Response Teams) amb la finalitat de contribuir al desenvolupament de la confiança i seguretat entre els Estats membres i promoure una cooperació operativa ràpida i eficaç;
- Estableix requisits en matèria de seguretat i notificació per als operadors de serveis essencials i per als proveïdors de serveis digitals;
- Estableix obligacions perquè els Estats membres designin autoritats nacionals competents, punts de contacte únics i CSIRT amb funcions relacionades amb la seguretat de les xarxes i els sistemes d'informació.

8) Directiva (UE) 2017/541 del Parlament Europeu i del Consell, de 15 de març del 2017, relativa a la lluita contra el terrorisme i per la qual se substitueix la Decisió Marc 2002/475/JAI del Consell i es modifica la Decisió 2005/671/JAI del Consell. La Directiva estableix normes mínimes relatives a la definició de les infraccions penals i les sancions en l'àmbit dels delictes de

terrorisme, els delictes relacionats amb un grup terrorista i els delictes relacionats amb activitats terroristes, així com mesures de protecció, suport i assistència a les víctimes del terrorisme.

Una de les qüestions rellevants de la Directiva és la referida a les mesures contra els continguts en línia que constitueixin provocació pública (art. 21). Per això estableix el següent:

> «Els Estats membres adoptaran les mesures necessàries per garantir la ràpida eliminació dels continguts en línia albergats al seu territori constitutius de provocació pública a la comissió d'un delicte de terrorisme [...]».

I en el mateix article és remet al 5, on es precisa que:

> «Els Estats membres adoptaran les mesures necessàries per garantir que es tipifiqui com a delicte, quan es cometi intencionadament, el fet de difondre o fer públics per qualsevol altre mitjà, ja sigui en línia o no, missatges destinats a incitar a la comissió d'un dels delictes enumerats a l'article 3 de la Directiva».

2.4. Legislació espanyola

Donades les normes que es deriven dels documents que acabem d'estudiar, cada Estat membre ha de realitzar accions dirigides a la ciberseguretat i ciberdefensa. Això inclou l'elaboració de lleis, protocols, programes i activitats que incloguin la sensibilització i formació entre professionals.

Abans d'entrar a aprofundir en la modificació del Codi Penal en matèria de terrorisme, considerem important destacar els documents següents:

1) Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i dels sistemes d'informació. El Decret pretén reforçar les accions de ciberseguretat en concebre que no n'hi ha prou amb les eines actuals per garantir un òptim nivell de seguretat en xarxes i sistemes d'informació. Unes accions que són summament necessàries si tenim en compte que aquestes infraestructures tenen un paper crucial en la societat i en l'activitat econòmica i política que s'hi realitzen.

2) El Reial decret llei 12/2018 va transposar el contingut de la Directiva 2016/1148. En aquest document es defineix el «servei digital» com «el servei de la societat de la informació prestat habitualment a títol onerós, a distància, per via electrònica i a petició de l'interessat». No obstant això, la llei solament afecta aquelles empreses amb més de 50 empleats i amb un volum de negoci anual superior als 10.000.000 d'euros, en considerar que són les que majoritàriament proveeixen de serveis digitals. Per tant, aquest tipus d'empreses o institucions han de garantir:

- La seguretat dels sistemes i de les instal·lacions;
- La correcta gestió d'incidents, així com la continuïtat de les activitats. D'això se n'encarreguen tres institucions: el Centre Criptològic Naci-

onal-Computer Emergency Response Team –CCN-CERT–, l'Institut Nacional de Ciberseguretat-Computer Emergency Response Team (INCIBE-CERT) i el Ministeri de Defensa;

- La supervisió, les auditories i proves necessàries; i
- El compliment de les normes internacionals.

Declaració ministerial d'administració electrònica de Tallin

El 2017 Espanya va subscriure aquest document, complint amb els objectius marcats en el Pla d'Acció sobre Administració Electrònica de la Unió Europea que ha de desenvolupar-se íntegrament el 2022. Aquesta declaració té com a objectiu garantir que qualsevol empresa i ciutadà europeu pugui interactuar digitalment amb l'Administració pública, basant-se en els principis de fiabilitat i seguretat; d'obertura i transparència i interoperabilitat per defecte.

2.4.1. Delictes de terrorisme

El Codi Penal defineix els delictes de terrorisme a l'article 573. Segons la redacció, es considerarà delicte de terrorisme la comissió de qualsevol delicte greu contra la vida o la integritat física, la llibertat, la integritat moral, la llibertat i indemnitat sexuals, el patrimoni, els recursos naturals o el medi ambient, la salut pública, de risc catastròfic, incendi, de falsedat documental, contra la Corona, d'atemptat i tinença, tràfic i dipòsit d'armes, municions o explosius, previstos en el present Codi, i l'apoderament d'aeronaus, bucs o altres mitjans de transport col·lectiu o de mercaderies, quan es duguessin a terme amb qualsevol de les finalitats següents:

1) Subvertir l'ordre constitucional, o suprimir o desestabilitzar greument el funcionament de les institucions polítiques o de les estructures econòmiques o socials de l'Estat, o obligar als poders públics a realitzar un acte o a abstenir-se de fer-lo.

2) Alterar greument la pau pública.

3) Desestabilitzar greument el funcionament d'una organització internacional.

4) Provocar un estat de terror en la població o en una part d'aquesta.

No obstant això, cal dir que la regulació dels delictes de terrorisme ha sofert diverses modificacions des de l'aprovació del Codi Penal del 1995, de les quals mereixen ser destacades les introduïdes per la **Llei orgànica 2/2015, de reforma del CP** en matèria de terrorisme, que modifica el capítol VII del títol XXII i comprèn els articles 571 a 580, i la **LO1/2019, de 20 de febrer**, per la qual es modifica la Llei orgànica 10/1995, de 23 de novembre, del Codi Penal, per traslladar Directives de la Unió Europea en els àmbits financer i de terrorisme i abordar qüestions d'índole internacional.

Les reformes han afectat, entre altres tipologies, el delicte d'adoctrinament, descrit a l'**article 575**, la modificació del qual es va produir com a resposta a la Decisió Marc 2002/475/JAI del Consell de la Unió Europea, de 13 de juny del 2002, sobre la lluita contra el terrorisme, modificada per la Decisió Marc 2008/919/JAI, de 28 de novembre del 2008. D'aquesta manera passa a ser penalment castigat aquell o aquelles que:

> «[...] amb la finalitat de capacitar-se per dur a terme qualsevol dels delictes tipificats en aquest capítol, rebi adoctrinament o ensinistrament militar o de combat –article 575.1– [...]. S'entendrà que comet aquest delicte qui, amb tal finalitat, accedeixi de manera habitual a un o diversos serveis de comunicació accessibles al públic en línia o continguts accessibles a través d'internet [...]. Així mateix s'entendrà que comet aquest delicte qui, amb la mateixa finalitat, adquireixi o tingui en poder seu documents que estiguin dirigits o, que pel seu contingut, resultin idonis per incitar a la incorporació a una organització o un grup terrorista o a col·laborar amb qualsevol d'aquests o en les seves finalitats –article 575.2– [...]. La mateixa pena s'imposarà a qui, per a aquesta mateixa fi, o per col·laborar amb una organització o un grup terrorista, o per cometre qualsevol dels delictes compresos en aquest capítol, es traslladi o s'estableixi en un territori estranger controlat per un grup o una organització terrorista –article 575.3–».

Aquest últim apartat ha estat modificat el 2019 a través de la LO 1/2019, de 20 de febrer, per transposar la Directiva UE de 15 de març del 2017 relativa a la lluita contra el terrorisme. Amb la nova redacció s'elimina l'exigència que el desplaçament es produeixi cap a una zona controlada per l'organització terrorista:

> «La mateixa pena s'imposarà a qui, per a aquesta mateixa fi, o per col·laborar amb una organització o grup terrorista, o per cometre qualsevol dels delictes compresos en aquest Capítol, es traslladi o s'estableixi en un territori estranger».

També s'introdueix, mitjançant la LO 1/2019, un nou article 580 bis, en virtut del qual la responsabilitat penal de les persones jurídiques s'estén a tots els delictes de terrorisme tipificats en el capítol. La Directiva del 2017 donava peu a això, tot i que, en ser tan ampli el catàleg de delictes de terrorisme previst en el CP espanyol, el nombre de supòsits pels quals les empreses podrien incórrer en responsabilitat penal corporativa és tan elevat que podem afirmar que, també en aquest cas, el legislador ha incorregut en desmesura (García Albero, 2019).

A més de la definició, d'altres novetats que va introduir la LO 2/2015 va ser la figura de l'adoctrinament (art. 575.1) i l'autoadoctrinament (art. 575.2), definint-lo com a:

> «capacitar-se per cometre algun dels delictes tipificats (en matèria de terrorisme)» [...] «s'entendrà que comet aquest delicte qui, amb tal finalitat, accedeixi de manera habitual a un o diversos serveis de comunicació accessibles al públic en línia o continguts accessibles a través d'internet o d'un servei de comunicacions electròniques els continguts de les quals estiguin dirigits o resultin idonis per incitar a la incorporació a una organització o grup terrorista, o a col·laborar amb qualsevol d'aquests o en les seves finalitats. [...] Així mateix, s'entendrà que comet aquest delicte qui, amb la mateixa finalitat, adquireixi o tingui en poder seu documents que estiguin dirigits o que, pel seu contingut, resultin idonis per incitar a la incorporació a una organització o grup terrorista o a col·laborar amb qualsevol d'aquests o en les seves finalitats».

2.4.2. Delictes informàtics amb finalitats terroristes

Finalment, ha de tenir-se en compte el previst en l'article 573.2 del CP, segons el qual es consideren delictes de terrorisme els previstos en els articles 197 bis i 197 ter (accés a sistemes d'informació i intercepció de dades informàtiques) i 264 i 264 bis (danys informàtics), quan es realitzin amb alguna de les finalitats de caràcter terrorista a les quals al·ludeix el Codi, concretament les esmentades en el punt anterior (art. 573.1). Això té com a conseqüència l'aplicació de la pena superior en grau a la prevista legalment per als respectius delictes (en virtut de l'art. 573 bis-3), la qual cosa planteja complexes qüestions de *non bis in idem*, donada la qualificació que al seu torn preveu el Codi en els indicats delictes comuns.

Enllaç recomanat

Per conèixer el contingut de les normes penals, és imprescindible consultar directament el CP. Concretament, la Llei orgànica 2/2015, de 30 de març, per la qual es modifica la Llei orgànica 10/1995, de 23 de novembre, del Codi Penal, en matèria de delictes de terrorisme. https://www.boe.es/buscar/doc.php?id=boe-a-2015-3440.

Per tant, podem concloure que a Espanya el (ciber)terrorisme s'està combatent, legalment, mitjançant l'avenç de la barrera punitiva, i s'amplien de manera desmesurada els casos en els quals pot aplicar-se el concepte de «terrorisme». Un avenç de la intervenció penal que, tal com han criticat diversos autors, se situa fins a la mera ideació subjectiva (Guirao, 2009).

3. Estratègies desenvolupades contra el ciberterrorisme

Les característiques de la xarxa dificulten el rastreig d'activitats ciberterroristes. Per aquest motiu, no es disposa d'eines eficaces per detenir-les i prevenir-les. A continuació descriurem aquelles estratègies que s'estan utilitzant amb aquestes finalitats, així com les institucions que estan posant els seus esforços a contenir aquesta activitat.

3.1. Estratègies per a la lluita contra el terrorisme

La lluita antiterrorista constitueix una prioritat per a diversos organismes, institucions i Estats. Arran d'això s'han anat adoptant diferents iniciatives amb l'objectiu d'intentar prevenir, protegir, perseguir i respondre a futurs atemptats que aquestes organitzacions podran cometre al món fora de línia o en línia, incloses les de caràcter econòmic.

Enllaç recomanat

En l'àmbit europeu, podeu consultar l'enllaç al document *IOCTA* (*Internet, Organised, Crime, Threat and Assessment*) del 2018. S'hi pot trobar un resum de l'Europol sobre les tendències reportades en cibercrim, inclòs el ciberterrorisme.

Enllaç: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.

Algunes de les estratègies més utilitzades per part de la Unió Europea des del 2005 són:

- Reforçar la legislació en matèria de terrorisme.
- Intensificar els controls a les fronteres exteriors.
- Intensificar el control de la compra i venda d'armes i del material químic susceptible de poder ser utilitzat per a la fabricació d'explosius.
- La creació d'organismes específics destinats a controlar i frenar la proliferació en el ciberespai de llocs que encoratgin el terrorisme com, per exemple, a través de propaganda o publicacions en línia.

1) Reglament de l'ús de les dades del registre de noms dels passatgers (també conegut per les sigles PNR). Aquesta estratègia va ser adoptada per la Unió Europea dins del marc de la lluita antiterrorista a través de la Directiva (UE) 2016/681 del Parlament Europeu i del Consell, de 27 d'abril del 2016, relativa a la utilització de dades del registre de noms dels passatgers i es dirigeix a: companyies aèries, titulars de les aeronaus en el cas de vols privats i entitats de gestió de reserva de vols. Aquestes dades han de servir per a la prevenció, detecció, recerca i enjudiciament dels delictes de terrorisme i de la delinqüència greu.

L'objectiu de la Directiva és elaborar un registre únic integrat per dades personals de passatgers amb la finalitat que puguin ser consultades per qualsevol Estat sempre que la finalitat sigui la prevenció, detecció, recerca i enjudiciament de delictes terroristes i delictes greus i s'hagi fet l'oportuna ponderació entre riscos i beneficis. Per aquest motiu, s'insta a tots els Estats membres a crear una unitat d'informació sobre els passatgers amb una persona al capda-

vant responsable de la protecció de les dades: la Unitat d'Informació sobre Passatgers (UIP). Aquesta s'encarrega de recollir, tractar i analitzar les dades que integraran el PNR, així com de gestionar les comunicacions i els intercanvis amb les autoritats competents nacionals, UIP d'altres Estats membres, i amb l'Europol. Una vegada es recopilen les dades, la UIP té entre 24 i 48 hores abans de la sortida del vol per enviar-les a l'òrgan central. En el cas concret d'Espanya, aquesta pertany al Centre d'Intel·ligència contra el Terrorisme i el Crim Organitzat (CITCO).

La creació del PNR, com hem dit, limita el tractament de les dades a les finalitats legítimes d'acord amb el dret a la protecció de les dades personals. D'acord amb aquesta directiva:

- No es poden recollir o utilitzar dades sensibles dels passatgers.
- Una vegada recollides les dades, passats sis mesos, aquestes han de ser despersonalitzades. És a dir, el contingut de la informació no pot ser susceptible de ser relacionat amb la persona.
- Les dades solament poden conservar-se durant cinc anys; després han de ser eliminades.
- Els Estats membres han d'assegurar-se que els passatgers reben una informació clara sobre la recollida de dades PNR i els seus drets.
- La transferència de dades PNR a tercers països solament podrà produir-se en circumstàncies molt particulars i haurà d'estudiar-se cas per cas.

Enllaç recomanat

Podeu consultar la Directiva (UE) 2016/681 del Parlament Europeu i del Consell, de 27 d'abril del 2016, relativa a la utilització de dades del registre de noms dels passatgers: https://www.boe.es/buscar/doc.php?id=doue-l-2017-80815.

D'aquesta manera, si s'adopten aquests criteris, es protegeix el dret fonamental a la protecció de les dades personals.

2) Estratègia nacional de ciberseguretat. A l'abril del 2019, Espanya va publicar l'Ordre PCI/487/2019, de 26 d'abril, per la qual s'adopta l'Estratègia Nacional de Ciberseguretat 2019, aprovada pel Consell de Seguretat Nacional. A través d'aquesta es van publicar les estratègies nacionals de seguretat aeroespacial, de protecció civil i de ciberseguretat. Hem de remarcar que lluny de la falta de consens en anteriors iniciatives (fins i tot en la definició de «ciberterrorisme»), aquestes estratègies han estat elaborades amb l'assessorament d'experts dels àmbits públic i empresarial en cadascuna de les àrees, i amb el consens de les comunitats autònomes.

Enllaços recomanats

Podeu consultar l'Ordre PCI/487/2019, de 26 d'abril, per la qual es publica l'Estratègia Nacional de Ciberseguretat 2019, aprovada pel Consell de Seguretat Nacional:

https://www.boe.es/diario_boe/txt.php?id=boe-a-2019-6347.

Accés directe a la descàrrega en obert del document *Estratègia Nacional Contra el Terrorisme 2019*:

https://www.dsn.gob.es/es/documento/ estratègia-nacional-contra-terrorisme-2019.

En l'àmbit del ciberterrorisme, el capítol 2 exposa la preocupació cap a aquest àmbit, així com la voluntat d'aconseguir un ciberespai segur que pugui fer front al ciberterrorisme. D'aquesta manera, es justifica la necessitat de reforçar el treball en la prevenció i detecció d'aquest tipus de ciberconductes. Concretament manifesta que:

> «Els grups terroristes intenten aprofitar les vulnerabilitats del ciberespai per realitzar ciberatacs o per a activitats de radicalització d'individus i col·lectius, finançament, divulgació de tècniques i eines per a la comissió d'atemptats, i de reclutament, ensinistrament o propaganda. Íntimament relacionat amb això, hi ha l'amenaça contra les infraestructures crítiques, amb la possibilitat certa de causar un col·lapse a través de les xarxes mitjançant una caiguda en cadena dels serveis essencials».

Per tot això, l'estratègia es basa en quatre principis:

- **Unitat d'acció:** estableix que la resposta a un ciberatac (com pot ser la comesa per una organització terrorista) ha d'implicar els diferents agents de l'Estat. Al seu torn, les seves accions han de ser coherents i estar coordinades.
- **Anticipació:** defensa que les actuacions en matèria de ciberseguretat han de prioritzar l'acció preventiva per sobre de la reactiva. Per a això es requereix un sistema d'informació compartida que pugui ser consultat per qualsevol agent responsable en l'àmbit de la ciberseguretat que permeti prendre decisions en el menor temps possible. Aquest és un aspecte clau si volem reduir les ciberamenaces.
- «**Eficiència**»**:** la ciberseguretat requereix un equip multidisciplinari de professionals i que compti amb programes i programaris amb un elevat nivell tecnològic. Una necessitat que sorgeix davant la complexitat que comporta el terrorista. Recordem la capacitat adaptativa que té el fenomen, fins i tot a la xarxa.
- **Resiliència:** si bé és un terme que utilitzem per referir-nos a la capacitat que tenen algunes persones per sobreposar-se a adversitats traumàtiques viscudes, en l'àmbit de la cibercriminalitat també s'utilitza per referir-se a la capacitat que han de tenir les estructures (informàtiques) crítiques de refer-se dels efectes que poden produir-hi les ciberamenaces i els ciberatacs. D'aquesta manera, l'Estat està obligat a dotar-les de tots aquells elements que consideri necessaris per garantir-ne la protecció enfront d'aquest tipus de ciberatacs.

3.2. Institucions que combaten el ciberterrorisme

1) EUROJUST: en l'àmbit europeu, el 2002 el Consell d'Europa va adoptar la Decisió 2002/187/JHA, per la qual es crea l'EUROJUST, la Unitat de Cooperació Judicial de la Unió Europea, amb seu a l'Haia. El seu naixement va sorgir amb un doble objectiu. D'una banda, reforçar la cooperació i la lluita contra les formes greus de delinqüència, inclosa la informàtica; d'una altra, millorar la cooperació judicial entre els 28 Estats membres. Per aquest motiu, cadascun dels Estats membres nomena un representant d'alt nivell (fiscals, jutges o funcionaris de policia amb competències equivalents) per treballar a l'EUROJUST.

En referència al terrorisme, al novembre del 2018, després de la Cimera Europea contra el Terrorisme celebrada a París, l'EUROJUST va acordar una sèrie de mesures, entre les quals destaquen:

- Crear un registre judicial en matèria de terrorisme que permeti als Estats membres poder-lo consultar per identificar elements comuns entre diferents casos oberts en matèria terrorista.
- Desenvolupar eines que permetin l'eliminació de continguts terroristes d'internet amb l'objectiu de prevenir la difusió de la ideologia gihadista.
- Establir el compromís de millorar la cooperació entre els Estats amb la finalitat d'oferir un millor servei de suport a totes les víctimes del terrorisme.

Enllaç recomanat

Podeu consultar els projectes en els quals treballa EUROJUST a:

http://eurojust.europa.eu/pages/ languages/es.aspx.

2) ENISA (Agència de la Unió Europea per a la Ciberseguretat). El Consell Europeu també va crear el 2004 l'Agència Europea de Seguretat de les Xarxes i de la Informació (ENISA) amb seu a Atenes (Grècia). És un organisme encarregat de treballar en favor de la seguretat cibernètica. Per a això brinda el seu suport als Estats membres i a les parts interessades de la Unió Europea (inclosos actors privats), per donar així resposta a ciberatacs soferts, inclosos aquells que poden produir-se entre els propis Estats.

Entre les seves funcions destaquen:

- Analitzar riscos actuals i emergents que puguin posar en perill la resistència i disponibilitat de les xarxes de comunicació electròniques.
- Millorar la cooperació entre els agents que operen en el camp de la seguretat de les xarxes i de la informació.
- Assistir a la comissió i als Estats membres en el seu diàleg amb el sector industrial per fer front als problemes relacionats amb la seguretat en els equips i programes informàtics.
- Promoure activitats d'avaluació de riscos, solucions interoperables de gestió del risc i estudis sobre solucions de gestió de la prevenció dins de les organitzacions dels sectors públic i privat.
- Elaborar i oferir recomanacions sobre ciberseguretat i assessorament als Estats membres i a les parts interessades de la Unió Europea.

Enllaços recomanats

Per conèixer tots els projectes en els quals treballa l'EUROPOL, podeu accedir a l'enllaç següent:

https://www.europol.europa.eu/.

Els informes i més informació sobre terrorisme podreu trobar-los a l'enllaç següent:

https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/terrorism?ct[article]=article&ct[event]=event&ct[guide]=guide&ct[panell]=panell&ct[multimèdia]=multimèdia&ct[news]=news&ct[operation]=operation&ct[page]=page&ct[document]= document.

A més, des del 2019, coincidint amb l'entrada en vigor del Reglament 2019/881, ENISA també prepara els esquemes de certificació europeus de ciberseguretat a través dels quals es garantirà que els productes, serveis i processos que es comercialitzen en territori de la UE compleixen amb uns estàndards, però aquesta certificació no serà obligatòria fins al 2023.

3) EUROPOL: és un organisme de la Unió Europea amb seu a l'Haia (Països Baixos) que centra la seva activitat investigadora a lluitar contra la gran delinqüència, entesa com: el terrorisme, el tràfic de drogues i el blanqueig de capitals en l'àmbit internacional; el frau organitzat; la falsificació d'euros; el tràfic de persones; així com els nous perills que estan sorgint després de la implantació de les TIC, la qual cosa coneixem com a ciberdelinqüència. La seva feina consisteix a assessorar a països de la UE i els que no en són membres però sí associats, brinden el seu suport a operacions policials i publiquen informes sobre la situació i tendència de cadascuna de les tipologies anteriorment citades.

En el cas del terrorisme, ha de tenir-se en compte la informació que contenen els informes *Europol's EU Terrorism Situation and Trend Report* (TE-SAT), que publica anualment a la seva pàgina web i en els quals podreu observar l'evolució que ha tingut el fenomen des del 2007, any en què es va publicar el primer.

Resum

En aquest mòdul hem pogut conèixer que el ciberespai és més complex del que *a priori* pot semblar. Hem vist que la informació que és subjacent a cadascun dels seus nivells, mitjançant la metàfora de l'iceberg, és immensa. També s'ha pres consciència que solament coneixem una ínfima part de la totalitat i que les activitats dels ciberterroristes es duen a terme a la *Dark Net* mitjançant l'ús de navegadors com el TOR.

D'altra banda, hem estudiat les implicacions que té l'ús d'internet per part d'organitzacions terroristes en el sistema jurídic actual, tant en l'àmbit internacional i europeu com en el cas espanyol; així com l'abordatge que s'està fent des d'institucions i organitzacions com EUROJUST, ENISA i EUROPOL. De manera més concreta, s'han examinat algunes iniciatives que s'estan prenent, com el PNR. No obstant això, de cara al futur, els reptes que se'ns presenten són diversos i complexos, ja que en els propers anys la preocupació sobre ciberseguretat se centrarà en la implementació de la xarxa 5G i els efectes que pugui comportar la seva utilització per part de grups cibercriminals. Per això, la Comissió Europea ja ha començat a preparar estratègies l'objectiu de les quals és aconseguir una cooperació més gran entre Estats que garanteixi l'intercanvi d'informació entre els membres de la Unió.

Exercicis d'autoavaluació

Perquè pugueu comprovar el grau de consolidació que heu aconseguit després de l'estudi del material, us proposem contestar deu preguntes tipus test.

1. Què signifiquen les sigles TOR?

a) *Terrorism On*
b) *The Onion Router*
c) *Terrorism Online Router*
d) *The Origin Router*

2. *Clear net* és...

a) L'internet que utilitzen les organitzacions terroristes per comprar armes.
b) L'internet que representa l'1 % del total de la xarxa.
c) L'internet que utilitza IP emmascarades.
d) L'internet al qual tots nosaltres podem accedir. Per exemple, a través de cerques a Google.

3. Quina característica del ciberespai garanteix TOR?

a) Anonimat.
b) Introjecció solipsista.
c) Invisibilitat.
d) Les respostes a) i b) són correctes.

4. La *Deep Web*...

a) Forma part de la *clear net*.
b) És el segon nivell de la xarxa i no té per què ser sempre sinònim d'activitat criminal.
c) Ocupa la part més profunda en el ciberespai.
d) És el segon nivell de la xarxa en el qual es realitzen tot tipus d'activitats il·legals; la compra i venda d'armes és la més realitzada.

5. Indiqueu quines de les afirmacions següents sobre el PRN és incorrecta:

a) No es poden recollir o utilitzar dades sensibles dels passatgers.
b) Les dades mai s'han d'esborrar del registre, excepte en aquelles circumstàncies que així ho indiqui l'EUROPOL.
c) Passats sis mesos, les dades han de ser despersonalitzades.
d) Cada Estat ha de tenir una UIP.

6. L'Estratègia Nacional de Ciberseguretat s'estructura entorn de quatre principis...

a) Unitat d'acció, anticipació, eficàcia i resiliència.
b) Unitat d'acció, anticipació, solidaritat i resiliència.
c) Unitat d'acció, eficàcia, solidaritat i cooperació.
d) Unitat d'acció, anticipació, eficiència i resiliència.

7. Quina de les convencions elaborades per part del Consell d'Europa és l'única vinculant per a la lluita contra l'ús d'internet amb finalitats terroristes?

a) Decisió Marc de 28 de novembre, relativa a la lluita contra el terrorisme.
b) Decisió Marc relativa als atacs contra els sistemes d'informació.
c) Decisió Marc, de 13 de juny del 2002, sobre la lluita contra el terrorisme, que harmonitza la definició dels delictes de terrorisme en tots els Estats membres de la Unió Europea.
d) Actualment no n'hi ha cap el contingut de la qual sigui vinculant.

8. Indiqueu quina de les afirmacions següents sobre l'EUROPOL és certa:

a) És una institució de les Nacions Unides.
b) Solament atén a països membres de la UE.

c) De la seva activitat investigadora s'elaboren informes que no es publiquen en obert.
d) EUROPOL investiga sobre: el terrorisme, el tràfic de drogues i el blanqueig de capitals en l'àmbit internacional; el frau organitzat; la falsificació d'euros; el tràfic de persones; i els nous perills que estan sorgint després de la implantació de les TIC, la qual cosa coneixem com a ciberdelinqüència.

9. El reglament de l'ús de les dades del registre de noms dels passatgers es dirigeix a...

a) Companyies aèries, titulars de les aeronaus en el cas de vols privats i entitats de gestió de reserva de vols.
b) Companyies aèries internacionals i heliports.
c) Companyies aèries, titulars de les aeronaus en el cas de vols privats, entitats de gestió de reserva de vols i titulars de drons.
d) Els passatgers que han d'identificar-se i emplenar un formulari cada vegada que comprin un bitllet d'avió o tren.

10. La novetat que va introduir la LO 2/2015 en el Codi Penal espanyol ha estat...

a) L'eliminació de l'exigència que imposava l'article 575.3 que el desplaçament es produeixi cap a una zona controlada per l'organització terrorista.
b) Una definició unànimement compartida per tots els països de la UE sobre el que s'ha d'entendre per terrorisme.
c) El delicte d'autoadoctrinament recollit a l'article 575.2.
d) Que introdueix quatre conductes ciberterroristes com a penalment punibles.

Solucionari

Exercicis d'autoavaluació

1. b

2. d

3. a

4. b

5. b

6. d

7. c

8. d

9. a

10. c

Bibliografia

Agudo Fernández, I.; Jaen, M.; Perrini, A. (2016). «Los delitos de terrorismo en el Código Penal». En: *Terrorismo en el siglo xxi: La respuesta penal en el escenario mundial*. Madrid: Dykinson.

Akhgar, B.; Brewster, B. (eds.) (2016). *Combating cybercrime and cyberterrorism: challenges, trends and priorities*. Springer.

Bergman, M. K. (2001). «White paper: the deep web: surfacing hidden value». *Journal of electronic publishing* (núm. 1, vol. 7).

Cano, M. A.; Castro, F. J. (2018). «El camino hacia la (ciber)yihad. Un análisis de las fases del proceso de radicalización islamista y su interpretación por parte de los tribunales españoles a partir de los datos suministrados por sentencias judiciales». *Revista electrónica de ciencia penal y criminología* (núm. 16, vol. 20).

Cuerda Arnau, M. L.; Hernández Fernández, A. (2019). *Adoctrinamiento, adiestramiento y actos preparatorios en materia terrorista*. Cizur Menor: Thomson Reuters Aranzadi.

Dinniss, H. A. H. (2018). «The Threat of Cyber Terrorism and What International Law Should (Try To) Do about It». *Georgetown Journal of International Affairs* (vol. 19, págs. 43-50).

García Albero, R.; Quintero, G. (dir.) (2016). *Comentarios a la parte especial del Derecho Penal* (7.ª ed.). Cizur Menor: Aranzadi.

García Albero, R. (2019). *Las reformas penales de 2019*. Cizur Menor: Aranzadi.

González Cussac, J. L. (2006). «El Derecho Penal frente al Terrorismo». En: J. L. Gómez Colomer; J. L. González Cussac. *Terrorismo y proceso penal acusatorio*. Valencia: Tirant lo Blanch.

Guirao, M. C. (2019). «El Delito de autoadoctrinamiento: ¿adelantamiento de la intervención penal a la mera ideación subjectiva? Análisis de sentencias». *Indret*.

Liang, I.; Chi, Z. (2018). «Analytical Insights on Criminal Law Legislation of Anti-Cyberterrorism». *China Legal Sci.* (núm. 69, vol. 6).

Presidencia de Gobierno (2019). *Estrategia Nacional Contra el Terrorismo 2019*. <https://www.dsn.gob.es/es/documento/estrategia-nacional-contra-terrorismo-2019>.

UNODC (2013). *El uso de internet con fines terroristas*. Naciones Unidas. <https://www.unodc.org/documents/terrorism/publications/use_of_internet_for_terrorist_purposes/use_of_internet_ebook_spanish_for_web.pdf>.