La prevenció del ciberdelicte

Fernando Miró Llinares

PID_00195940

Universitat Oberta de Catalunya

Els textos i imatges publicats en aquesta obra estan subjectes –llevat que s'indiqui el contrari– a una llicència de Reconeixement-NoComercial-SenseObraDerivada (BY-NC-ND) v.3.0 Espanya de Creative Commons. Podeu copiar-los, distribuir-los i transmetre'ls públicament sempre que en citeu l'autor i la font (FUOC. Fundació per a la Universitat Oberta de Catalunya), no en feu un ús comercial i no en feu obra derivada. La llicència completa es pot consultar a http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.ca

Índex

Introducció

El coneixement i l'anàlisi del fenomen de la criminalitat han d'anar lligats a la cerca de solucions per a evitar la comissió delictiva o, si més no, reduir la incidència i minimitzar els efectes nocius que té per a la societat. Per això, aquest mòdul està pensat perquè l'estudiant conegui diverses estratègies per a prevenir la cibercriminalitat.

Hem dividit el mòdul en quatre apartats seguint una estructura lògica d'anàlisi: en primer lloc veurem l'àmbit en què es produeix la ciberdelinqüència i les característiques que el defineixen; en segon lloc estudiarem els comportaments que incideixen en el procés de victimització; en tercer lloc tractarem de les teories aplicades al fenomen de la cibercriminalitat, i, finalment, veurem les estratègies de prevenció.

Objectius

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

1. Conèixer les diverses característiques que constitueixen el ciberespai.

2. Adquirir coneixements sobre la importància de l'actuació de la víctima en procés de victimització.

3. Familiaritzar-se amb els diversos enfocaments de les teories de la criminalitat aplicada al cibercrim.

4. Aprendre a establir estratègies de prevenció.

1. Com podem prevenir el ciberdelicte?

Vivim en la societat de la informació, que es caracteritza per les tecnologies de la informació i la comunicació (TIC) i el gran nombre de canvis que impulsen tant socials com polítics i econòmics. La suma d'evolucions tecnològiques en els camps de la microelectrònica, la informàtica i les telecomunicacions, entre d'altres, juntament amb l'aparició del paradigma d'innovació tecnològica que ha tingut una incidència social més gran, com ha estat Internet –que ha fet que els mercats financers esdevinguin transfronterers, ha multiplicat les opcions d'accés a informació de tota classe, ha permès transaccions econòmiques o personals transfrontereres i en temps real, ha creat noves formes de comunicació personal i ha modificat els contextos i el sentit de qualsevol forma de comunicació– ha desencadenat una gran quantitat de canvis en els àmbits econòmic, cultural i social.

Davant la realitat de l'existència de la cibercriminalitat, el següent pas lògic és plantejar-se com es pot prevenir aquest tipus de delinqüència. Per a arribar a aquest punt caldrà plantejar-se diferents qüestions que anirem responent a mesura que avancem en el tema.

- En primer lloc, Internet com a xarxa global ha significat la creació d'un lloc de comunicació social transnacional, universal i en permanent evolució tecnològica que s'ha anomenat ***ciberespai***, i respecte al qual ens interessa plantejar-nos si es pot definir com un **nou àmbit d'oportunitat delictiva**, un context de risc criminal diferent de l'espai nacional físic tradicional o, per contra, idèntic a aquest pel que fa als trets essencials.

- En segon lloc, caldrà plantejar-se si **el cibercrim és un delicte nou o per contra és un delicte vell però que s'esdevé en un nou àmbit**. En aquest sentit, es plantegen diferents punts de vista. Des d'una visió més extrema, la ciberdelinqüència és un tipus de delinqüència nova per a la qual no són vàlides les teories tradicionals creades per a explicar l'espai físic. En el pol oposat, el ciberdelicte és idèntic estructuralment al delicte comès a l'espai físic, només en canvia l'aspecte, però en cap cas els trets configuradors. I també en una posició intermèdia, la cibercriminalitat comparteix amb la delinqüència tots els elements definidors del concepte de crim, però s'esdevenen d'una manera tal en el nou àmbit, el ciberespai, que pot influir significativament en l'explicació del delicte i, per tant, en la prevenció d'aquest.

- En tercer lloc, també és important plantejar-se **el paper que tenen els actors implicats en la producció de l'esdeveniment delictiu i si s'hi pot**

incidir d'una manera específica per a evitar la producció dels esdeveniments delictius.

- En quart i últim lloc, tenint en compte les qüestions anteriors, caldrà **estudiar si les teories del crim** concebudes **per al món físic es poden traslladar al ciberespai** o si, per contra, **caldrà fer replantejaments** de les teories que s'adaptin a la realitat.

2. El ciberespai com un nou àmbit d'oportunitat criminal

La primera qüestió que hem d'aclarir amb vista a la prevenció és conèixer els canvis del ciberespai respecte de l'espai físic –és a dir, les singularitats que presenta– i identificar-ne les característiques estructurals i de construcció com a àmbit relacional, especialment les que són diferents de l'àmbit espacial o físic, àmbit en què tradicionalment s'han comès les infraccions.

Abans de tot convé explicar que el ciberespai és l'espai virtual, no físic, determinat per la interconnexió de persones per mitjà de xarxes telemàtiques, i dins d'aquest espai, un dels principals catalitzadors és Internet, un sistema global d'informació i comunicació basat en el protocol de control de transmissió (TCP) que uneix ordinadors d'arreu del món i permet l'accés a qualsevol d'aquests per a obtenir i intercanviar informació d'una manera senzilla. Dins d'Internet hi ha molts serveis, un dels quals és el World Wide Web (WWW), com a conjunt de protocols que permet accedir a informació d'una manera remota, i que s'ha superposat com a concepte al mateix terme d'*Internet*, malgrat que inclou altres serveis a part del WWW com el correu electrònic, els canals d'*Internet relay chat* (IRC) de conversa en línia, a més de moltes altres TIC que s'estan integrant avui a Internet, com la telefonia electrònica o la televisió digital.

2.1. Com és el ciberespai?

El ciberespai té com a característiques intrínseques una configuració concreta de les coordenades d'espai i temps respecte de la que té el que podem anomenar *espai real* o *espai físic*.

> Diem que el **ciberespai** és un espai perquè les persones s'hi troben i s'hi relacionen tot i que, mentre que l'espai físic existeix abans que s'acabi la relació i continuarà existint després d'acabar la relació (si més no mentre hi hagi un observador), el ciberespai esgotarà la seva existència quan serveixi per a la comunicació entre les persones, atès que sense interacció no hi ha xarxa.

Així, respecte de l'espai geotècnic com la terra, que existeix independentment dels actes de les persones que hi tinguin lloc, i que només pot ser ocupat alhora per un mateix ens, el ciberespai existeix quan s'hi interacciona i pot ser ocupat per molts ens al mateix temps. De fet, se sol utilitzar com a sinònim de *ciberespai* el concepte d'*espai virtual* com a antitètic a l'"espai real". La simultaneïtat o la unicitat de moments pot portar a la impressió que el ciberespai

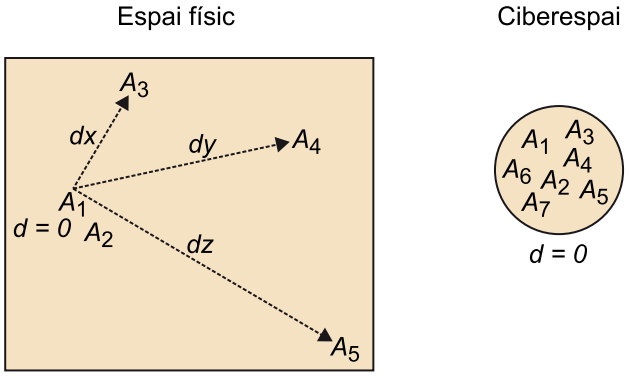
és l'absència d'espai, potser fruit de l'equívoc d'assimilar la idea d'espai a la de distància. Evidentment, el ciberespai és real en el sentit que existeix, però es tracta d'una "espècie nova" d'espai, invisible als sentits directament i en què les coordenades d'espai i temps adquireixen un altre significat i en què l'abast i els límits són redefinits.

En realitat, doncs, la idea de la "virtualitat" del ciberespai deriva de la identificació tradicional entre espai (físic) i distància. En l'àmbit de comunicació configurat per **Internet no hi ha distàncies, però sí espai**. Així, el ciberespai representa la contracció total de l'espai (de les distàncies) i, alhora, la dilatació de les possibilitats de trobada i comunicació entre les persones. Internet ha contret el món i ha apropat a un mateix lloc interactiu persones que poden estar en coordenades espacials separades milers de quilòmetres. L'espai es contreu i la intercomunicació s'expandeix. I això evidentment influeix en la configuració social. Mentre que l'espai de les societats tradicionals estava dominat per la contigüitat, per les relacions de proximitat en els àmbits familiar, veïnal, local i supralocal, en la societat actual les relacions es canalitzen per mitjà de xarxes, cosa que afavoreix un desplaçament de la informació i de la comunicació molt més gran. Així doncs, per mitjà de xarxes es creen noves comunitats virtuals entre persones que poden estar separades per l'espai físic, però que estan unides per uns interessos i unes inquietuds determinats i que, per això, es configuren com a comunitats amb una lògica diferent de la de les comunitats físiques tradicionals.

El ciberespai, en tot cas, conviu amb l'espai físic o terrestre, i en alguns aspectes hi té també una relació directa que no ha de ser obviada: les xarxes telemàtiques que constitueixen el ciberespai uneixen, de manera virtual però també física, terminals o sistemes informàtics que estan situats en espais terrestres concrets en països nacionals determinats amb contextos socials de facilitació de l'accés a Internet específics, i també amb règims jurídics diferents que poden afectar, per exemple, les obligacions dels prestadors de serveis respecte a la identificació dels titulars de les adreces IP. A més a més, també canvia la relació entre l'espai físic i l'espai virtual: fa unes quantes dècades es necessitava un lloc físic fix per a entrar en el ciberespai, mentre que avui, gràcies a les xarxes Wi-Fi i en concret, a la nova tecnologia de la telefonia mòbil, és possible connectar-se des de pràcticament qualsevol lloc físic del planeta i estant en moviment.

Tanmateix, aquest espai geogràfic en què hi ha els terminals és irrellevant per a la comunicació entre les persones en el ciberespai. El fet destacat és que, mentre que per a la comunicació a l'espai físic calia proximitat (en termes de distància) entre l'emissor i el receptor, en el ciberespai ja no cal: ara es pot dur a terme la comunicació al mateix temps (o en temps separats, aspecte de què tractarem després) i en el mateix (ciber)espai, però en diferents espais geogràfics (o a distància).

Figura 1. Contracció de la distància en el ciberespai i expansió de la capacitat comunicativa



A_1 necessita $d = 0$ per a comunicar–se amb A_2, A_3, A_4, etc.

Per tant, la **distància** ja no és cap obstacle per a la comunicació en el ciberespai, de manera que independentment del lloc on sigui la persona a la qual va adreçada l'acció a Internet, el cost de realització serà exactament el mateix, atès que la distància física no té rellevància en el ciberespai.

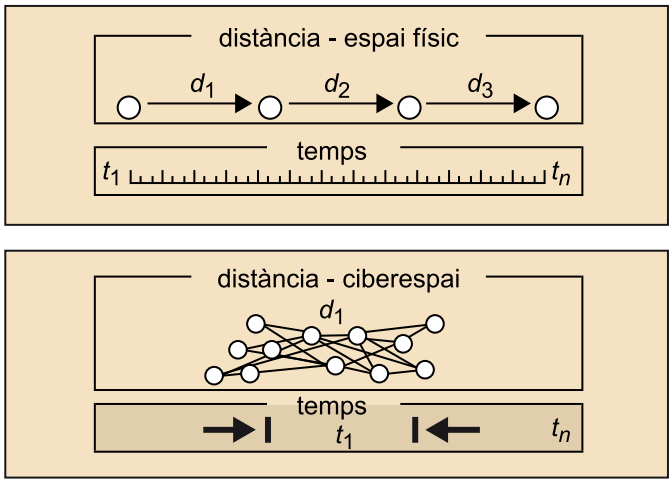
Quan diem que el ciberespai és un "nou espai", estem anticipant la resposta sobre la incidència de l'àmbit en l'altra dimensió, el temps. Internet també canvia el temps, la percepció social d'aquest i la manera com s'organitza aquest temps.

La **contracció de l'espai** comporta, en primer lloc, un augment de la importància del temps, i en segon lloc, una compressió del temps necessari per a la comunicació social. El temps que cal per a la comunicació entre dues persones separades per un espai físic també es contreu davant l'absència de la distància i l'aparició d'un espai virtual d'intercomunicació immediata. Així, el que a l'espai físic nacional exigeix molt de temps, es pot dur a terme de manera immediata en el ciberespai, amb la conseqüent "acceleració de la vivència subjectiva del temps", atès que a Internet els esdeveniments succeeixen molt més de pressa que en la vida no virtual.

En tot cas, amb el temps passa una cosa semblant al que succeeix amb l'espai: la contracció en el sentit de reducció del temps necessari per a dur a terme una tasca determinada comporta un estirament de les relacions socials, ja que l'avenç de les tecnologies de la comunicació ha permès eliminar les "distàncies temporals" entre les societats i apropar-les fins a convertir el contacte entre elles en una cosa instantània. Com es pot veure en la figura 2, com que en el ciberespai no cal recórrer cap distància per a la comunicació, les possibilitats de contacte amb moltes persones augmenten i es redueix el temps necessari per a això.

En darrer terme, es pot dir que Internet redueix els costos temporals exigits a l'espai físic per a qualsevol tipus de comunicació entre les persones.

Figura 2. Contracció del temps

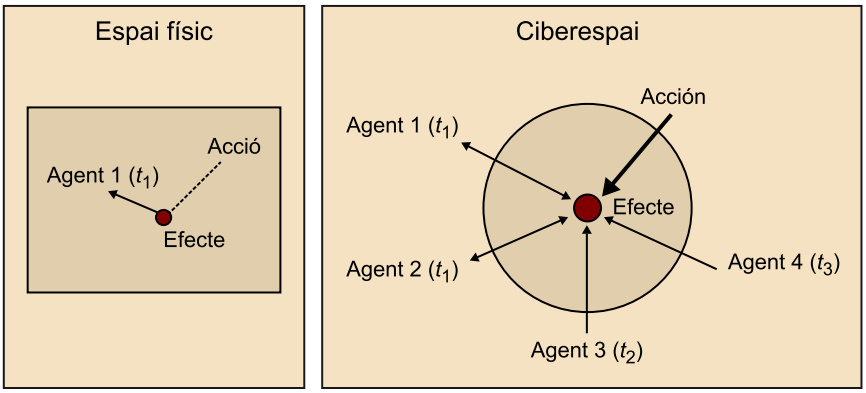


El temps necessari per a la comunicació disminueix perquè en el ciberespai no hi ha distàncies.

I no és l'únic canvi que podríem assignar al "temps" en el ciberespai. La configuració comunicativa d'aquest nou àmbit d'intercomunicació social pot fer que accions els efectes de les quals s'esdevindrien d'una manera instantània però caduca tinguin un funcionament temporal diferent: **que els efectes es produeixin instantàniament però siguin perceptibles de forma perenne**.

Així, les conductes que s'executen pel ciberespai, especialment les de publicitat de continguts, poden quedar fixades durant un cert temps i continuar tenint efectes encara que l'execució només hagi durat un instant. La raó és l'estructura comunicativa d'Internet, de constituir un espai vast que es pot expandir i contreure, en què les coses poden ser en un lloc i després en un altre, i en què la comunicació entre les persones en el ciberespai es pot produir en temps diferents, en el sentit que l'emissor pot enviar un missatge comunicatiu en un moment temporal determinat i no ser rebut fins al cap de molt temps pel receptor. Així, i com es vol reflectir en la figura 3, mentre que a l'espai físic les accions produeixen efectes en un moment determinat, en el ciberespai l'efecte pot quedar fixat durant un temps indeterminat i afectar un agent concret en el moment en què es realitza, però també en un moment posterior quan un altre agent interaccioni amb aquest efecte.

Figura 3. Fixació dels efectes en el ciberespai



L'acció s'executa en un cert moment, però A_3 i A_4 hi interaccionen en moments posteriors.

Certament, a l'espai físic això també és possible, però és indubtable que el ciberespai modifica la capacitat de control per part de l'agent del fet en relació amb l'element temporal. I el mateix succeeix amb l'element espacial: a l'espai físic l'agent dominava, si més no en general, més les coordenades espaciotemporals del fet, en el sentit que podia definir l'àmbit geogràfic en què començaria a produir efectes (encara que després aquests no fossin els desitjats), com també el moment o instant temporal en què ho començarien a fer. També era possible, en molts casos, definir concretament l'espai físic en què el fet de l'agent acabaria de produir efectes, si més no els que en derivaven més directament; i, de la mateixa manera, el temps que duraria el fet. **En el ciberespai és més difícil concretar l'àmbit geograficoespacial en què es desenvoluparà el fet**: algunes accions es poden adreçar concretament contra un usuari, un col·lectiu o una institució determinada, però fins i tot en aquests casos **la propagació dels efectes és més senzilla perquè no cal "recórrer distàncies"**.

Hi ha altres accions que, a més, són incontrolables pel que fa a la dimensió espacial: una vegada es difon un contingut a Internet o es propaga un *malware* a un col·lectiu indeterminat, és gairebé impossible saber qui, des de qualsevol lloc del món, en rebrà els efectes. I si ho observem des de la perspectiva contrària, la complexitat per a concretar la causa a la qual es pot atribuir el resultat o l'efecte és similar: mentre que la concreció de l'espai geogràfic on s'ha fet un dany determinat ens pot ajudar a identificar-ne el responsable, en el ciberespai la identificació geogràfica i temporal d'un efecte o conseqüència no ens assegura cap tipus de proximitat espacial o de temps amb la causa. No és que no hi hagi transferència, que n'hi haurà, i per tant empremta, que serà digital, sinó que **no hi haurà transferència espacial**: la seguretat (o previsibilitat alta) que el criminal ha de ser en un espai determinat simplement pel fet que el dany s'ha produït en un lloc concret.

I passarà el mateix amb el temps; és a dir, que els efectes d'una acció sorgeixin en un moment determinat no assegura, en el ciberespai, que el fet l'hagi iniciat el subjecte en aquell instant temporal. Per contra, els agents passius es poden convertir en agents actius en el ciberespai: és possible que un agent dugui a

terme una cosa i "deixi" el ciberespai, i que una altra persona interaccioni després amb el que ha realitzat el primer independentment de la voluntat del primer.

En tot cas, cal destacar que en el ciberespai les coordenades espaciotemporals es veuen significativament modificades: d'una banda, es comprimeixen les distàncies i el temps que cal per a recórrer-les; de l'altra, a conseqüència d'això anterior, s'expandeixen les possibilitats comunicatives entre les persones i els efectes dels fets que amb prou feines es veuen limitats espacialment o temporalment. De manera simbòlica, tornant a la geografia per a explicar l'efecte de tot això, podríem dir que el ciberespai és un espai més gran, més ampli, i també més durador, de percepció dels efectes més dilatada en el temps, que l'espai físic. Això significa que qualsevol agent en el ciberespai, llevat de l'impediment del contacte físic directe, té menys restriccions espacials i temporals per als actes que dugui a terme que a l'espai físic. També, que els efectes de les conductes, les conseqüències plasmades en unes coordenades espaciotemporals determinades ofereixen menys informació en el ciberespai que les coordenades espaciotemporals de l'acte al qual s'han d'atribuir aquestes i per això, de l'agent causant, que a l'espai físic.

Per descomptat, tot això va a influir en la configuració del (ciber)crim, com a esdeveniment social que és. I si la criminologia ha tractat d'explicar aquest fenomen des de sempre –i especialment en els últims anys ha centrat l'interès en l'entorn en el qual actua, l'arquitectura del qual no és comparable al nou àmbit d'intercomunicació social en el qual també es poden produir esdeveniments criminals–, és evident llavors la necessitat de replantejar la vigència d'aquestes teories per a aquest nou tipus de delictes o, si més no, adaptar-ne els desenvolupaments al nou espai.

Abans, però, convé explicar un altre tipus de característiques que configuren també el ciberespai i que per això determinaran qualsevol fenomen social que hi tingui lloc.

Una de les característiques bàsiques que encertadament se sol atribuir a Internet és la **deslocalització**. Es pot dir que el ciberespai no està situat en cap lloc concret, sinó que, en sentit funcional, és en tots alhora però en sentit físic, no és enlloc. En realitat, aquesta característica no és extrínseca al fenomen, sinó una cosa intrínseca al ciberespai: és la seva essència com a fenomen (no) espacial, i que hem analitzat abans.

No obstant això, no es pot negar que aquesta característica no tindria la importància que té si no portés unit un altre element que podem dir que és accessori, en tant que es podria imaginar un ciberespai configurat sense aquest element, però essencial i definidor del que, per a tothom, constitueix avui aquest nou àmbit social que és Internet: la transnacionalitat.

La **transnacionalitat** és la inexistència de fronteres o distàncies, ni aparents ni reals, en un àmbit digital d'interacció social que no pertany a cap estat nacional concret, però que, alhora, permet accedir als seus serveis des de qualsevol d'ells.

La transnacionalitat del ciberespai es tradueix, als efectes que ens interessen, en l'absència total, per a la comunicació i la interacció entre individus, de barreres que no siguin imposades o configurades pel mateix subjecte. Des de qualsevol estat nacional és possible accedir a qualsevol estat nacional, i un contingut abocat en una pàgina web localitzada en un servidor d'un estat concret i penjada per un individu d'un estat determinat pot ser vista per centenars de persones en centenars de llocs diferents al món. Des d'una perspectiva sociològica, és obvi que la transnacionalitat del ciberespai el configura com un àmbit d'intercomunicació social nou que contrasta amb les possibilitats de comunicació extranacional a l'espai físic. En el ciberespai, la trasnacionalitat es barreja amb la localitat, en el sentit que, per a tenir un contacte o comunicació amb un estat, regió o localitat, diferent de la pròpia, ja no cal traslladar-se físicament, sinó que es pot accedir a allò que és trasnacional des del local, fins i tot des del personal o íntim que, per tant, pot dependre només ja de la decisió del mateix individu, a l'accés de moltes més persones del que era possible anteriorment. Per tant, en el ciberespai augmenten les facilitats per a la multicomunicació social (transnacional), i disminueixen així els impediments per a la comunicació entre les persones, si més no el fet que es limitava les persones que fossin a prop físicament les unes de les altres. El mateix passa amb els béns: en el ciberespai ja no cal el contacte físic entre l'agent i el bé perquè hi hagi l'accés, i per descomptat, no és necessari que se sigui present en el moment de l'intercanvi o de l'adquisició (lícita o il·lícita) en el mateix lloc físic, sinó que és possible que una persona des d'un estat nacional accedeixi a una altra i accedeixi a un bé, digitalitzat, però amb valor econòmic.

Un altre caràcter extrínsec d'importància cabdal és la **neutralitat** en el ciberespai, que implica la llibertat de l'usuari a l'hora de transitar-hi sense fronteres però també sense censures d'accés per part de ningú. El caràcter neutre d'Internet deriva de la impossibilitat de bloquejar connexions entre nodes a la Xarxa, la qual cosa permet que una vegada tinguin accés a Internet ni tan sols el mateix operador pugui impedir l'accés a un web o a un servei triat per l'usuari.

Per bé que es tracta d'un caràcter extrínsec, atès que es podrien establir restriccions per mitjà d'una reconfiguració d'Internet que permetés, per exemple, bloquejar la capacitat d'un usuari per a emetre informació o per a accedir a un lloc web, és consubstancial al ciberespai que coneixem, en què només hi ha les restriccions que s'imposa l'usuari, el seu caràcter neutre. Precisament per això, és obvi que el control d'informacions i continguts, per part de qui el vulgui dur a terme, és complex en el ciberespai, tot i que és discutible que ho sigui més que a l'espai físic. La dificultat de controlar les comunicacions entre usuaris particulars en l'àmbit real pot ser fins i tot més gran, ja que no queda, com en el ciberespai, constància o empremta del que s'ha comunicat. El que sí que és més gran, sense cap mena de dubte, és la capacitat de la informació per a difondre's en un espai universal i popularitzat, i això és el que n'augmenta la importància, també el valor i, en alguns casos, no es pot negar la capacitat que té per a causar dany a béns essencials, cosa que pot servir de raó o d'excusa per als estats o algunes organitzacions per a tractar de crear un ciberespai diferent, amb nodes connectats que en la part central depenguin d'algú i que, per això, li permetin impedir l'accés a uns webs determinats o la navegació a usuaris específics.

En relació amb la transnacionalitat i el caràcter neutre de la Xarxa, com a caràcter extrínsec però configurador del ciberespai, també podem esmentar la **descentralització** o, potser millor, la no-centralització i concretament el caràcter **distribuït** que té, atès que en l'estructuració d'Internet no hi ha nodes centrals però tampoc nodes que facin de centres locals, sinó que es tracta d'una malla i la caiguda d'un node no impossibilita que la informació continuï fluint.

D'altra banda, i relacionat amb això, **a Internet no hi ha cap autoritat centralitzada**, ni tan sols òrgans o institucions de control de la informació circulant que puguin establir algun tipus de censura sistemàtica o control dels continguts. Internet no està sotmès a les lleis nacionals d'un sol país, ni a unes normes pròpies acceptades per tots els que en formen part, i això fa que els controls governamentals siguin poc efectius, ja que hi ha diverses maneres d'evitar els que van imposant els estats nacionals. No obstant això, és clar que l'existència d'aquest espai transnacional, neutre i distribuït, amb les conseqüències que comporta, produeix una tensió, en aquest cas en el terreny jurídic, amb la gairebé contradictòria existència d'estats nacionals amb legislacions diferents reguladores d'un fenomen determinat. Si bé no hi ha cap control global de la Xarxa, els governs nacionals han començat a tractar de regular Internet davant el risc potencial que representa i la seva popularització en totes les escales socials. Però, en tot cas, l'adopció de decisions nacionals amb prou feines soluciona el problema, com és obvi. El risc potencial que comporta la transnacionalitat del cibercrim i que el converteix en un dels desafiaments plantejats actualment més importants deriva de **la complexitat que representa respondre localment a riscos globals**.

Des de la perspectiva criminològica que ara ens interessa, podríem afirmar que això és conegut pels cibercriminals, en el sentit que són conscients que malgrat la realització de conductes que poden ser delictives en l'estat en què produeixen efecte, el fet de fer-ho des d'un estat diferent complicarà enormement la persecució penal per aquestes conductes. A més a més, aquesta transnacionalitat i el caràcter distribuït del ciberespai, units a l'existència d'un gran nombre de normes diferents en estats diversos, i a la característica que després analitzarem relativa a la revolució tecnològica permanent que es produeix en aquest nou àmbit social, comporta que, al contrari del que sol succeir a l'espai físic, no sigui gens fàcil determinar si unes conductes concretes són socialment adequades o fins i tot si són legals o no ho són. El ciberespai difumina l'aparença de legalitat de les conductes.

Una altra característica que cal destacar del ciberespai com a àmbit de risc és el caràcter **universal** que té, i en aquest cas no en el sentit de transnacional, sinó en el sentit de global, col·lectiu o popular. En el món podem parlar de mil milions d'usuaris, aproximadament, i per tant, de milions d'objectius sobre els quals poden actuar els criminals.

Popularització de la informàtica

En les últimes dècades s'ha produït una popularització de la informàtica, un augment de les facilitats per a adquirir terminals o accedir-hi i, molt especialment, per a la interconnexió entre tots ells en un espai de comunicació global que també s'ha generalitzat. A més a més, i malgrat que els primers anys es va pensar que Internet seria utilitzat essencialment per empreses i institucions, l'evolució de les tecnologies per a accedir a la Xarxa ha fet que avui els usuaris particulars siguin els que principalment utilitzen Internet com a vehicle de comunicació personal. L'auge de les xarxes socials i la millora de l'educació en l'ús de les TIC des de la infància ha comportat que els menors des dels nou anys fins als més grans de seixanta-cinc anys siguin usuaris d'una xarxa que en aquest sentit també és global.

La universalització d'Internet també té a veure amb un cost baix i, sobretot, amb l'**anonimat** que confereix. Malgrat que des d'alguns sectors s'està intentant construir algun tipus de sistema que permeti identificar els usuaris, sembla difícil imaginar un ciberespai en què totes o la majoria de les persones que hi intervenen estiguin identificades. Encara que actualment no sembli gaire complexa la determinació del sistema informàtic que navega pel ciberespai, sí que ho és per contra la concreció del subjecte que ha utilitzat aquest sistema per a realitzar la infracció, especialment avui, en què hi ha molts cibercafès des dels quals és possible comunicar-se en el ciberespai, xarxes Wi-Fi que permeten accedir des de llocs oberts, etc. A això, cal sumar-hi els proveïdors de serveis gratuïts que no exigeixen la identificació dels usuaris, els nombrosos sistemes que permeten enviar correus electrònics de manera anònima i, ja més en l'àmbit de l'esdeveniment criminal, les possibilitats actuals d'infectar un sistema informàtic determinat per a convertir-lo en un robot (*bot* o zombi) i utilitzar-lo per a realitzar l'activitat criminal, de manera que ni tan sols sigui possible identificar la IP des de la qual, en realitat, s'ha generat l'atac, a més d'altres factors rellevants, com la transnacionalitat i la diversitat de prestadors de serveis que operen en estats amb règims jurídics diferents, que no sempre

obliguen a la identificació dels terminals en xarxa. L'anonimat té com a conseqüència un augment de la sensació d'impunitat i aquesta, al seu torn, deriva en un increment del risc que l'agent executi el delicte.

Una altra característica que cal tenir present és que el ciberespai està subjecte a una **evolució tecnològica permanent**. Les TIC es caracteritzen perquè experimenten modificacions importants gairebé constantment, de manera que les formes de comunicació social, d'intercanvi econòmic, de difusió de continguts, o qualsevol altra que s'utilitzi en un moment determinat poden ser substituïdes en molt poc temps per evolucions que poden anar des d'una petita modificació fins a una autèntica revolució del sistema. Així, l'evolució d'Internet sembla imparable, tant en l'aparició de nous serveis com en la millora i la modificació de les formes d'accés.

Això té una importància més que evident: d'una banda, les barreres de protecció del tipus que siguin, per als interessos personals i socials que en un moment determinat semblen eficaços, poden deixar de ser-ho en molt poc temps, i béns que semblen intocables pel que fa a les TIC, poden passar a ser susceptibles d'atac en un instant; d'altra banda, el dret avança totalment "a remolc" d'un context social que va canviant, i les solucions jurídiques d'avui semblen obsoletes i d'ahir quan entren en vigor.

D'altra banda, no s'ha de menysprear la importància que el ciberespai estigui sotmès a canvis procedents dels mateixos usuaris. Els usuaris han fet d'Internet el que és, i són ells els que constantment el modifiquen i creen. I això es deu no solament al fet que la interacció social amb qualsevol tecnologia incideix en la seva estructura sinó també al fet que Internet és una tecnologia molt flexible i dúctil que "permet l'efecte de retroacció en temps real". Internet està configurat com un espai obert en què, al contrari que en altres sistemes, els canvis i les modificacions provenen de la mateixa intervenció del conjunt d'usuaris, i no d'un ens central.

Aquesta relació directa entre l'usuari i Internet, entre la seva configuració i ús amb l'agent, és més poderosa que en la realitat de l'espai físic a causa probablement d'altres factors de què hem parlat abans, com la descentralització i la popularització del mitjà. El que importa, en tot cas, és l'efecte que produeix: l'usuari se sent part definidora del ciberespai i, per tant, part decisòria d'aquest, especialment en la configuració com a espai de llibertat. En l'espai fisicogeogràfic, definit per unes fronteres i sota l'autoritat d'un estat concret, el ciutadà té definides molt estrictament les seves possibilitats democràtiques: pot triar els representants polítics o directament els governants, pot proposar de manera més o menys directa l'aprovació de normes jurídiques, etc.; i també

pot configurar els usos socials, si bé com que generalment estan definits amb l'evolució de la societat és complicat per al ciutadà tenir-hi una influència directa. En el ciberespai és diferent.

Quant a la participació en processos formals de decisió democràtica, no és possible en el ciberespai i, no obstant això, la seva democratització (o l'aparença d'aquesta) és molt més gran, ja que, com que no hi ha autoritats i és universal i popular, el conjunt de ciutadans d'Internet és el que decideix les normes socials bàsiques de funcionament intern. Evidentment, això no és dret en un sentit estricte, però és clar que són usos socials que, en un àmbit com Internet en què els interessos econòmics i personals són els que manen, esdevenen regles de conducta vàlides per al funcionament de les relacions a Internet. A més a més, i precisament perquè és un àmbit social nou, canviar-ne i definir-ne les normes (diguem-ho així) ètiques és molt més senzill per a l'usuari, ja que no hi ha uns usos socials imposats sinó que es van creant amb la interacció de tots els nous.

Les conseqüències d'això per a l'entorn social del ciberespai, als efectes que ens interessen, són diverses, però destaca el fet que no hi està tan definida l'ètica o la moral imperant com a l'espai físic subjecte a una sobirania nacional, bàsicament perquè els mateixos usuaris, amb les seves conductes, la poden canviar. És possible, i de fet és el que succeeix amb institucions com la propietat intel·lectual, però no solament amb aquesta, que les regles que regeixin per a l'espai físic es considerin, per part dels usuaris, no aptes per a aquest nou àmbit que ells acaben definint amb la seva manera d'actuar. Això no significa que el dret no hi regeixi, però sí que la seva capacitat d'influència reguladora pot disminuir, ja que, com més correspondència hi hagi entre la norma i el que és acceptat socialment més compliment de les normes es produirà.

Òbviament, tots aquests factors, intrínsecs i extrínsecs, d'aquest nou àmbit que és el ciberespai determinaran tots els fenòmens que s'hi produeixin, entre els quals el que ens ocupa, el crim.

2.2. L'oportunitat delictiva

Les primeres aproximacions de la criminologia al fenomen del cibercrim es van centrar en la discussió sobre les motivacions del *hacker*, potser perquè en aquells moments la criminologia se centrava en l'estudi del subjecte criminal, en la comprensió dels condicionants de la seva conducta i en les modalitats corresponents. En els últims anys s'han fet diferents estudis que han tractat de comprendre el fenomen de la criminalitat aplicant teories de l'oportunitat com la teoria de l'autocontrol, la teoria de la decisió racional, la teoria de l'aprenentatge social, la teoria del control social i la teoria de l'etiquetatge o de les activitats quotidianes.

Si considerem que la teoria de les activitats quotidianes –com a part de l'origen de totes les teories actuals de l'oportunitat o del dia a dia que els últims anys sembla que són al centre dels debats criminològics principals, que han superat les expectatives que es marcaven per a la criminologia ambiental i que han donat lloc, en conjunció amb la teoria de la decisió racional, als desenvolupaments sobre la prevenció situacional del delicte– va partir, com una de les premisses fonamentals, de la idea que la modernitat, i en aquesta l'evolució tecnològica, portava implícit l'augment del contacte entre autors potencials, víctimes potencials i, en alguns casos, la disminució de guardians capaços d'evitar el crim, amb l'augment consegüent en les taxes de criminalitat.

La veritat és que si, en el moment en què es va enunciar aquesta teoria, això es fonamentava en evolucions tecnològiques com l'automòbil i socials com la igualtat entre els homes i les dones, que havien modificat la relació entre l'ofensor motivat, l'objectiu i l'absència de mecanismes de defensa, avui, l'aparició d'un nou espai de comunicació personal transnacional, universal i subjecte a una revolució permanent, com és el ciberespai, anticipa, si no un augment de la criminalitat, cosa que caldrà avaluar a més llarg termini, sí almenys l'existència d'un nou context d'oportunitat criminal que coexistirà en el temps amb el de la realitat física i que, malgrat que pot compartir amb aquest el fet que el delicte dependrà de la relació entre victimari, víctima i mecanismes de protecció, divergirà en la manifestació concreta d'aquests mateixos factors, fruit de l'especialitat del mitjà en què convergeixen.

En tot cas, el que fa especialment apta la teoria de les activitats quotidianes és el fet que posa el focus d'anàlisi de l'esdeveniment criminal ja no tant en l'agressor o criminal com en el mateix espai i en la incidència que aquest pot tenir en l'aparició del delicte. El naixement d'un nou àmbit de comissió delictiva com el ciberespai, amb característiques intrínseques i extrínseques significativament diferents de l'espai físic, on es continua cometent el nombre més gran de delictes, fa que sigui convenient partir de les teories que paren esment en el lloc de comissió delictiva per a comprovar les noves característiques de l'esdeveniment criminal en el ciberespai.

I hi ha un últim punt d'unió entre l'enfocament de l'oportunitat i el cibercrim, que té a veure amb la necessitat de recórrer per a prevenir aquesta nova forma de delinqüència a les teories que es focalitzen sobretot en el control no formal a causa de la ineficiència provada del control formal, i especialment de les normes jurídiques nacionals, respecte d'aquest tipus de crim. Efectivament, d'alguna manera donen per fet que el sistema de la justícia penal té una capacitat limitada per a aconseguir efectes preventius, per la qual cosa centren l'atenció en el món de cada dia per intentar actuar-hi i d'aquesta manera prevenir el delicte. És obvi que aquest enfocament té un especial sentit davant un tipus de criminalitat com el que ens ocupa, que, atès que es duu a terme

en el ciberespai transnacional i en anonimat, contra el qual, d'alguna manera, xocaran l'Administració de justícia i el sistema penal nacional en general, requereix posar el focus d'atenció per a la prevenció pertinent no solament en els terrenys normatiu i formal sinó també, més enllà d'això, en l'aspecte ambiental i en la mateixa actuació quotidiana dels que accedeixen a Internet i hi interaccionen.

Prevenció del delicte

"La prevenció del delicte és una responsabilitat de tots i no solament de les agències de control social formal o del sistema de justícia penal."

J. J. Medina Ariza (1998, pàg. 281)

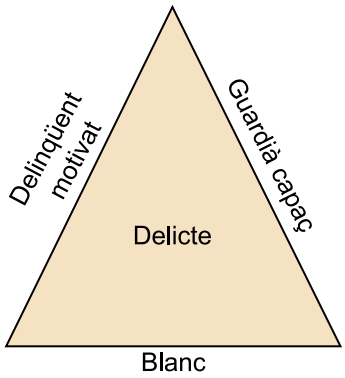
Tot això anterior no implica, per descomptat, considerar que l'enfocament de l'oportunitat és més vàlid com a pensament criminològic que el de les teories criminològiques o del delinqüent tradicionals amb el rebuig conseqüent de les múltiples crítiques adreçades a l'*opportunity approach*, ni considerar que és l'únic possible per a la cibercriminalitat. Simplement serveix per a explicar la decisió presa d'utilitzar aquest enfocament per a comprovar la importància del canvi de l'ajust espaciotemporal en el fenomen criminal i, d'aquesta manera, analitzar l'esdeveniment del cibercrim. És evident la capacitat potencial d'algunes teories de la criminalitat o del delinqüent tradicionals per a explicar moltes modalitats de cibercriminalitat, a més del fet que aquesta visió és perfectament compatible amb una intervenció en l'àmbit de l'oportunitat, però també ho és que les teories que posen més èmfasi en la relació del factor ambiental o espacial amb la motivació del criminal reflectiran més bé els canvis que pot representar per al crim com a esdeveniment el fet que el lloc de realització sigui el ciberespai.

2.3. Teoria de les activitats quotidianes en el ciberespai

Segons la teoria de les activitats quotidianes de Cohen i Felson (1979), el delicte es produeix en un temps i en un lloc, però no exigeix que sigui físic, encara que implícitament es pressuposi. Per descomptat, el lloc de comissió d'un crim pot ser el ciberespai i, com hem vist, difereix estructuralment de l'espai físic, espai en què només es podien cometre els delictes fins fa unes quantes dècades.

Si en el ciberespai es pot cometre un delicte, s'hi hauran de produir també les característiques que se li assignen. És a dir, si el crim, com a esdeveniment, depèn de la presència d'un delinqüent capacitat i motivat per al delicte, d'un objectiu o víctima adequats i de l'absència d'un guardià capaç, en la primera fórmula de la teoria de les activitats quotidianes, i també dels altres elements incorporats en les fórmules següents, s'ha de poder dir el mateix del cibercrim. Això sí, com que canvia la configuració espaciotemporal del ciberespai, la manera com confluiran aquests elements, com es relacionaran entre si i com formaran l'equació del delicte serà diferent. El triangle del crim continuarà igual i amb els mateixos elements, encara que els "angles", valgui l'expressió, poden ser diferents. O en altres paraules, el lloc "ciberespai" no alterarà els factors del crim, però sí l'expressió concreta d'aquests i, per tant, d'un gran nombre d'elements que s'han de tenir en compte amb vista a la prevenció del delicte.

Figura 4. Triangle del crim



Per a analitzar les raons dels diversos angles que formen la interacció de l'agressor motivat amb l'objectiu adequat en el lloc ciberespai, cal contrastar aquests elements amb les característiques intrínseques i extrínseques del ciberespai, i així definir els trets més singulars d'aquest nou àmbit d'oportunitat delictiva i en comparació de l'altre àmbit d'oportunitat criminal, el de l'espai real. El resultat d'aquesta comparació ens haurà de servir per a comprendre les peculiaritats del cibercrim que cal tenir en compte a l'hora de definir els instruments de prevenció corresponents.

D'altra banda, i malgrat que tots els elements de l'esdeveniment criminal s'expliquen perquè van units entre si, a l'efecte didàctic per a fer-ne l'anàlisi estudiarem de manera separada la incidència del ciberespai en cadascun dels elements que constitueixen el triangle del delicte (tal com quedaria amb la primera configuració de Cohen i Felson), afegirem els gestors del lloc que s'incorporen en el segon triangle i eliminarem, per motius obvis, el lloc (que és el mateix ciberespai).

2.3.1. El delinqüent motivat

L'agressor en el ciberespai es continua motivant sobre un objectiu determinat i en un lloc. Tanmateix, el camp d'oportunitat d'un agressor motivat (en abstracte) és molt ampli en el ciberespai a causa de la inexistència de la distància física com a barrera o, dit d'una altra manera, de la no-necessitat de proximitat entre l'agressor i la víctima per a la (ciber)delinqüència, com sí que calia generalment a l'espai físic. Mentre que el més habitual en la criminalitat sol ser que el delinqüent cometi el delicte a prop del lloc on viu o si més no que no es desplaci distàncies gaire grans, excepte en cas que l'incentiu derivat de l'atac a l'objectiu adequat sigui especialment valuós, en la cibercriminalitat no cal sortir de casa per a atacar béns jurídics que físicament són molt lluny.

TIC i delinqüència

És cert que ja existien tecnologies que possibilitaven que l'atac criminal es realitzés des d'un lloc i els efectes es produïssin a milers de quilòmetres de distància. Però també és clar que les TIC han creat el ciberespai, en què la distància física ja no és cap barrera infranquejable per a molts delictes, de manera que esdevé un àmbit d'oportunitat més ampli (sempre en termes potencials): augmenta considerablement el nombre de persones que poden contactar les unes amb les altres com a agressors i objectius adequats i s'amplia, per tant, l'àmbit potencial d'oportunitat criminal.

El més rellevant del que hem assenyalat, en qualsevol cas, i des de la perspectiva de l'agressor motivat, és que la compressió de l'espai que representa el ciberespai incrementa les "possibilitats de motivació" d'un potencial agressor motivat. Ho fa com a mínim per dues raons:

1) En primer lloc perquè incrementa els objectius potencials sobre els quals pot prendre la decisió de quin és l'adequat, sense que la distància ni el temps siguin un element essencial de la decisió.

2) En segon lloc perquè redueix el cost espaciotemporal que comporta gairebé sempre cometre un delicte, tant en termes d'arribar a l'objectiu com d'assegurar-se la fugida una vegada s'ha comès el delicte.

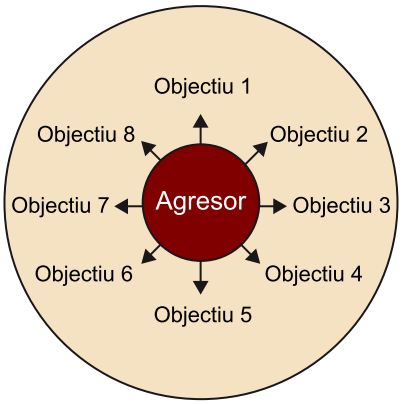
El fet que no hi hagi cap desplaçament espacial i que el subjecte es pugui "estalviar" aquest cost no significa que no hi hagi un cost temporal per a la realització d'un atac en el ciberespai. Sempre n'hi haurà, i serà més gran o més petit depenent del tipus de cibercrim. En el cas concret dels cibercrims econòmics, el desenvolupament de programes i tècniques o la mateixa cerca de vulnerabilitats exigeixen als *hackers* molt de temps, igual que el lladre necessita preparació a l'espai físic.

En realitat, aquest temps de preparació de l'atac i de selecció dels objectius esdevindrà l'autèntic protagonista, en termes de cost, de l'atac en el ciberespai. De fet, la selecció d'objectius és la clau, com hem vist, d'una gran part dels casos de la cibercriminalitat econòmica, especialment del *phishing*, per mitjà de la cerca de vulnerabilitats en els sistemes que es vol infectar, com ara *bots*, o mitjançant la cerca de destinataris finals als quals es vol defraudar. Això sí, es tracta d'un procés de selecció, aspecte que veurem més endavant, en què intervé molt la víctima, ja que sovint el ciberagressor crea el programari i el lloc on el deixa i la víctima amb una certa vulnerabilitat, en interaccionar-hi, serà infectada i "atacada". En qualsevol cas, de costos temporals relacionats amb la preparació i l'execució del crim n'hi ha tant en el cibercrim com en el crim *offline*.

Sí que variarà en els **costos de desplaçament i de fugida**, que són presents en el crim a l'espai físic, però **no en el cibercrim**. Així, mentre que el criminal a l'espai físic ha de tenir en compte el cost, en termes de distància i temps, de fugir del lloc des d'on ha comès el delicte cap a un lloc segur (de la mateixa manera que ha de tenir en compte la distància i el temps des del lloc d'origen on es troba fins al lloc on comet la infracció), el cibercriminal "s'estalvia" aquests costos.

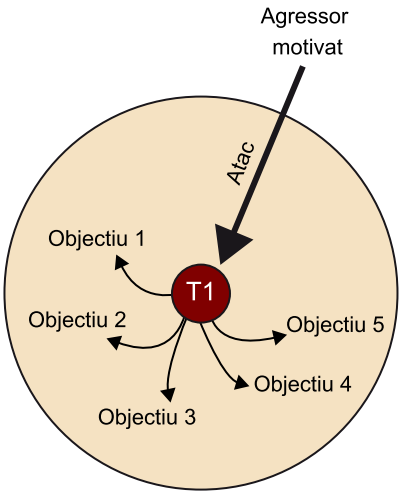
També en relació amb l'agressor i la incidència en aquest de l'estructura del nou àmbit en què actua, el ciberespai, cal assenyalar que les TIC poden actuar com un "multiplicador de força" que fa que persones amb uns recursos mínims puguin generar un gran dany per a moltes persones i béns en el ciberespai. A més a més, l'expansió de l'àmbit comunicatiu al qual pot accedir un agressor motivat que representa el ciberespai comporta una multiplicació de la potencialitat lesiva d'una conducta en comparació del que succeeix a l'espai físic. És a dir, malgrat que a l'espai físic i real hi ha armes sofisticades que permeten causar danys a múltiples béns, en general, la producció de danys a béns que són en llocs diferents (i, per descomptat, en països diferents seria també vàlid com a excepció per a les armes) requereix el trànsit del cibercriminal d'un lloc a un altre, cosa que en el ciberespai no cal. Això ja passava amb els delictes "de paraula" relacionats amb la televisió i altres mitjans de comunicació. En el ciberespai encara és més significatiu: com s'observa en la figura següent, l'agressor no solament pot seleccionar entre moltes víctimes potencials sinó que també en pot atacar diverses en el mateix instant i des del mateix espai, encara que aquestes víctimes potencials es trobin en llocs situats a milers de quilòmetres de distància entre si; i fins i tot encara que els efectes dels atacs no es despleguin (o sí) en el mateix moment.

Figura 5. Una multiplicitat d'objectius per a un mateix atacant: un agressor actua alhora sobre diversos objectius



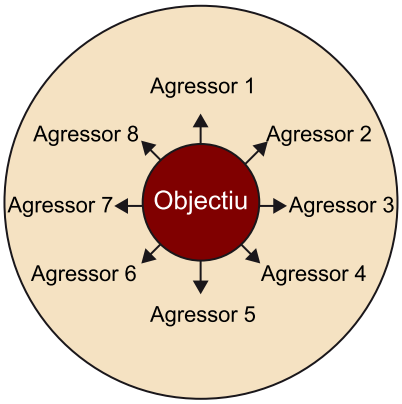
A més a més, el ciberespai no solament permet a l'agressor motivat seleccionar entre diverses víctimes l'objectiu del seu atac, sinó que la contracció de les distàncies li ofereix la possibilitat d'atacar-ne unes quantes amb una única conducta. Això també és possible en el cas de la criminalitat duta a terme a l'espai físic o real, si bé les facilitats per a això en el ciberespai són molt més grans, especialment en el cas de la modalitat de cibercrims en què la il·licitud esdevé del contingut i en què el simple fet de fer publicitat d'una pàgina web amb contingut nociu o prohibit (ciberterrorisme, *hatespeech*, pornografia infantil, pirateria intel·lectual, etc.) ja implica l'afectació de múltiples béns jurídics o del mateix bé supraindividual, tot i que amb una dimensió més gran en la lesió.

Figura 6. Un atac múltiple: amb la mateixa acció s'ataquen diversos objectius (i en el mateix temps)



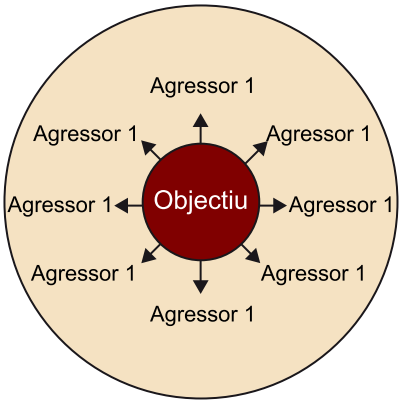
També és perfectament possible en el ciberespai que una mateixa víctima sigui atacada de manera simultània i en el mateix espai que ocupa per molts agressors diferents. En aquest cas, l'atac es produeix en el mateix (ciber)espai però des d'espais (físics) diferents i en moments temporals que poden ser idèntics pel que fa al desplegament d'efectes tot i que no ho han de ser necessàriament en relació amb el moment d'atac.

Figura 7. Una multiplicitat d'atacants per a un mateix objectiu



Finalment, l'agressor pot utilitzar un o múltiples sistemes informàtics situats també en múltiples llocs (infeccions de *bot*) des dels quals realitza atacs que es poden produir de manera simultània o seqüencial i contra un sol objectiu o contra objectius que poden ser múltiples i fins i tot indeterminats, sense que calgui per a això fer cap esforç de trasllat.

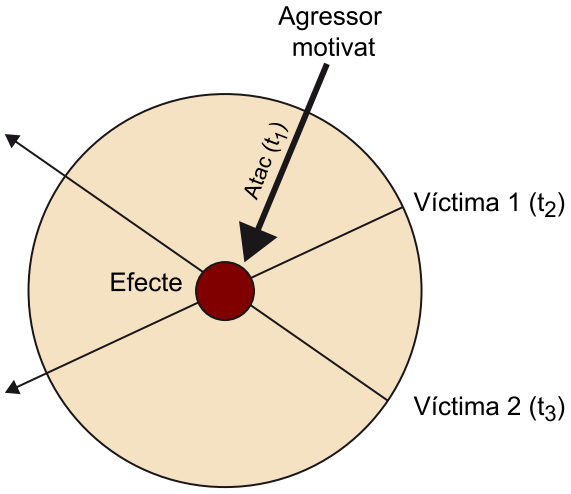
Figura 8. Una multiplicitat de llocs en el ciberespai que utilitza l'agressor per a atacar la víctima des d'un sol punt a l'espai físic



I tot això, per descomptat, executat per l'agressor des de (i sobre) qualsevol lloc del món. Al cap i a la fi, la compressió o la contracció de les distàncies i l'expansió comunicativa consegüent en el ciberespai no seria tan rellevant si aquest no fos transnacional ni s'hagués popularitzat de la manera que ho ha fet. En el ciberespai, els ofensors amb inclinacions criminals ho poden ser de (i des de) qualsevol estat nacional i poden actuar sobre víctimes d'estats (o cap a estats) diferents, de manera que es redueixen les barreres que l'espai sol imposar per a això. Però, a més a més, com que augmenta la quantitat de persones que utilitzen Internet, també ho fa el nombre de delinqüents potencials, i atès que el ciberespai uneix milers de milions de ciutadans en un "lloc comú" en què hi ha relacions comercials i personals, s'incrementen també els "objectius adequats" i, per tant, les possibilitats de contacte entre els uns i els altres amb l'augment potencial consegüent de la criminalitat. En aquest sentit, el ciberespai és, des d'una perspectiva quantitativa, un espai de risc criminal amb un efecte multiplicador "potencial" sense cap precedent en la història.

D'altra banda, i com hem avançat, la disminució de la distància comporta una reducció del temps com a cost. Tots els atacs a un o diversos objectius es poden realitzar en el mateix moment, de manera que no cal utilitzar temps per a transitar la distància que separa els objectius perquè tots es vegin afectats. A més a més, i continuant l'anàlisi de la incidència de les noves condicions ambientals en el factor "agressor motivat", però posant atenció ara en el factor temporal, les característiques especials del ciberespai i de determinats instruments de comissió dels ciberatacs com els virus permeten que en unes condicions concretes la presència de l'agressor motivat es produeixi en un moment de temps anterior al perfeccionament de l'atac. Pròpiament, l'agressor motivat no desapareix, sinó que simplement l'atac comès es produeix en un àmbit (i en un moment temporal) en què la concreció d'aquest atac ja no dependrà tant de la conducta de l'agressor com de la conducta de la víctima. Això és el que succeeix especialment en el cas dels virus que són descarregats en una determinada pàgina web de descàrrega amb una falsa aparença d'arxius de música o vídeo. L'agressor motivat realitza l'atac deixant en el ciberespai l'instrument pertinent com una cosa estàtica que espera la conducta de la víctima perquè l'atac s'acabi perfeccionant. Però això no significa que no hi hagi agressor, sinó que aquest pot actuar multiplicant la seva capacitat lesiva a Internet sense les limitacions temporals i espacials tradicionals que caracteritzen l'espai físic. Ho farà, això sí, sempre que la víctima hi interaccioni o, més ben dit, sempre que la víctima interaccioni amb l'efecte que ha estès.

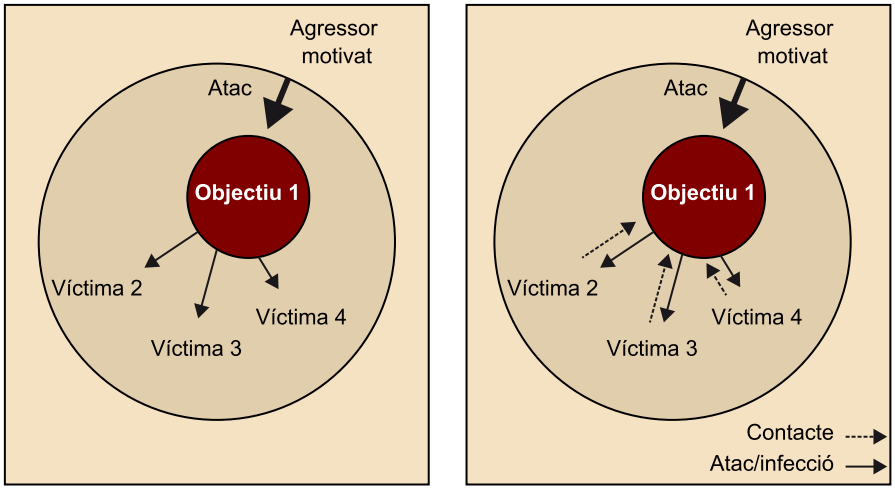
Figura 9. Fixació de l'atac i interacció de la víctima: l'atac deixa un efecte fix en el ciberespai, i la víctima és la que hi interacciona



I és que la contracció de l'espai també pot tenir conseqüències importants en relació amb els efectes del delicte, molt especialment amb algun tipus de criminalitat en el ciberespai caracteritzada per la dinàmica segons la qual la víctima receptora de l'atac es converteix immediatament, i sense voler-ho, en emissora d'un nou atac en una cadena successiva que ni tan sols és controlada pel mateix autor del crim. Això és el que succeeix amb la transmissió de virus, també amb l'enviament de *spam*, i fins i tot, encara que d'una manera diferent, atès que en aquest cas el receptor del missatge és el que ha d'accedir a la comunicació, amb la transmissió de continguts il·lícits o nocius (pornografia

infantil, obres protegides, *hatespeech*, etc.) en pàgines web. Si els continguts o els missatges es transmetessin de manera física, la distància entre l'emissor i el receptor complicaria la multidifusió del que és il·lícit. En el ciberespai és diferent, ja que la contracció de l'espai i la interconnexió de tots els sistemes fan que la multiplicació dels efectes de la conducta sigui pràcticament immediata. En la criminalitat realitzada a l'espai físic o real és difícil trobar una cosa semblant, tret que es tracti de la contaminació alimentària o d'algunes formes de delinqüència ambiental, excepcions a la regla que el delicte produeix els efectes danyosos d'una manera controlada i que depèn essencialment de l'actuació del criminal.

Figura 10. La víctima com a instrument de difusió de l'atac



Finalment, s'ha relacionat encertadament l'augment del risc criminal derivat de la potenciació del factor "agressor motivat" amb l'**anonimat** a Internet, que atorga una sensació de seguretat a l'infractor, ja que li ofereix un refugi aparentment segur en el qual es pot ocultar, cosa que, al seu torn, li permet reinventar-se i adoptar nous personatges virtuals amb els quals, potser, cometrà delictes. Amb l'anonimat succeeix, doncs, una cosa molt semblant al que hem comentat en relació amb la transnacionalitat, que incideix en la desaparició de la por de ser identificat i en la minimització consegüent del temor de ser detingut, frens de la motivació criminal que el converteixen en un *motivated offender*.

Des de la perspectiva de la teoria de la decisió racional, per tant, entre els riscos potencials que el ciberdelinqüent ha de sospesar respecte dels beneficis derivats de l'agressió inclouria l'enorme dificultat que planteja avui dia la identificació, en termes judicials probatoris, del cibercriminal. Perquè no solament es tracta de la identificació de l'adreça IP sinó també de la concreció posterior de l'usuari concret del sistema informàtic al qual s'ha concedit aquesta adreça. És obvi que hi ha mitjans per a evitar aquests riscos. Així, els mecanismes electrònics d'identificació, com l'ID d'usuari, sistemes automatitzats de control de l'accés o càmeres de vigilància, poden servir d'elements de dissuasió pel fet d'augmentar el risc percebut de ser detinguts.

Anonimat

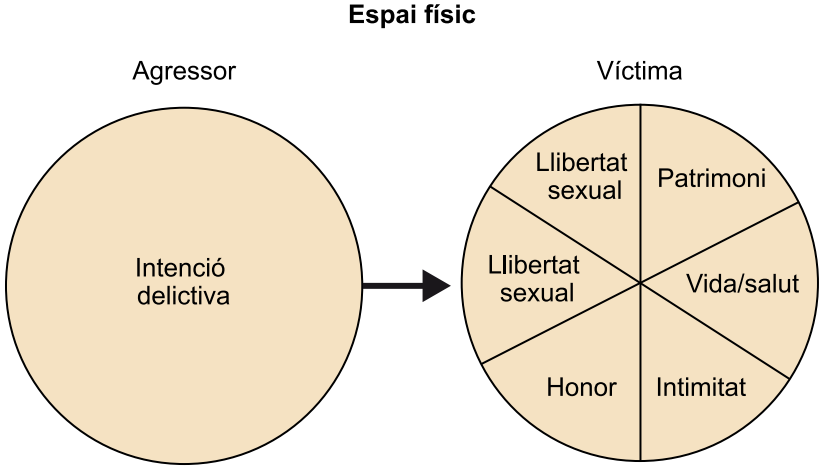
De moment, però, això no sembla possible, ja que l'anonimat no solament serveix a propòsits criminals sinó també a altres aspectes lícits relacionats amb la facilitat d'accés al ciberespai que difícilment seria compatible amb altres sistemes d'identificació que, a més, es podrien falsejar fàcilment.

2.3.2. L'objectiu adequat

El que hem afirmat fins ara de l'agressor motivat té conseqüències directes en l'element "objectiu adequat": el creixement de l'àmbit de risc no és solament per l'agressor sinó també per les víctimes potencials, que també són moltes i més tenint en compte que no cal una immediatesa temporal i una proximitat física entre l'agressor i l'objectiu; de la mateixa manera, les dinàmiques dels ciberatacs i la potenciació de les facilitats per a l'agressió que comporta el ciberespai incideixen en l'objectiu adequat d'aquesta agressió, i el mateix es pot dir dels efectes del ciberdelicte. Al cap i a la fi, com hem dit, la separació entre l'agressor motivat i l'objectiu adequat tan sols és figurativa: **no hi ha motivació sense objectiu, i viceversa**.

En qualsevol cas, convé precisar què comporta l'increment potencial de les possibilitats de contacte entre l'agressor i la víctima en el ciberespai. El contacte entre l'objectiu i l'agressor a l'espai físic generalment és un contacte físic directe i immediat, en què tots els béns personals de la víctima i els patrimonials que porti damunt estan exposats i esdevenen objectius potencials adequats per a l'atac de l'agressor. Certament, la víctima potencial pot determinar en gran part el que es pot convertir en un objectiu adequat, i seleccionar per exemple els béns amb valor econòmic que porta al damunt; però no pot eliminar de l'àmbit de contacte amb les persones altres béns personalíssims que hi estan indissolublement units. Pràcticament tot el que una persona és com a tal, tot el que en forma part, es posa en contacte amb l'agressor a l'espai físic.

Figura 11. Contacte a l'espai físic



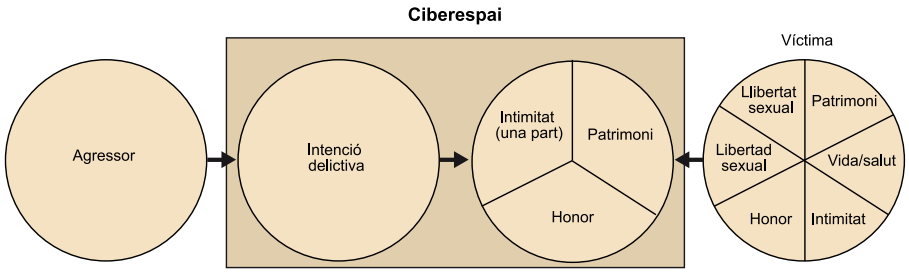
En l'espai virtual o ciberespai, el contacte entre persones és diferent, de manera que la persona física no es comunica directament en un context espaciotemporal determinat amb una altra persona, sinó que és una representació de la persona, en el més essencial que la defineix, la que contacta en l'àmbit comunicatiu d'Internet. La persona no entra al ciberespai amb tots els béns i valors que té, sinó bàsicament amb els que tria entre els que pot triar. Al cap i a la fi, el primer límit que té la víctima per a comunicar-se amb una altra persona o per a contactar en el ciberespai és que no pot posar a disposició dels altres la seva entitat física, de manera que els atacs a la persona adreçats directament contra béns com la vida o la salut no podran ser duts a terme a Internet.

A més a més, i malgrat que la persona pot veure atacats alguns béns personalíssims encara que ella no els vulgui posar a disposició de terceres persones en el ciberespai, en altres béns com els relacionats amb la privacitat o el mateix patrimoni la víctima és la que decideix, pel fet d'incloure informació personal en el ciberespai o de compartir-la amb d'altres, realitzar activitats econòmiques, etc., situar-los en aquest nou àmbit de risc.

Béns a disposició de terceres persones

Com succeeix amb la lliure formació de la sexualitat dels menors, que pot ser atacada en rebre una imatge de contingut sexual o similar.

Figura 12. Contacte en el ciberespai



Per tant, els usuaris del ciberespai poden eliminar de l'àmbit d'atac els béns que no incorporin en el ciberespai. Així doncs, el crim, pel que fa a l'objectiu concret a què s'adreça, pot ser evitat per la mateixa víctima en el ciberespai des del moment en què no el situa en l'espai virtual. Independentment del valor que tingui, si la víctima no s'incorpora al ciberespai, l'objectiu no existeix; per contra, la introducció d'elements a Internet comporta immediatament el

risc que puguin ser victimitzats. En aquest sentit, hi ha estudis empírics que demostren que pràcticament totes les modalitats d'atac es configuren entorn d'una dinàmica semblant en què el pas inicial sol ser l'enviament previ (la introducció), per part de la víctima, d'informació personal a persones desconegudes. Ara bé, i com aprofundirem després, la simple introducció de l'objecte no és perillosa *per se*, si bé constitueix un primer pas que, si s'uneix a la interacció de la víctima en el ciberespai, ja pot comportar risc de victimització.

Objectiu involuntari

La introducció d'un objectiu en el ciberespai, no obstant això, no sempre és voluntària. En alguns casos es tracta d'un procés gairebé fortuït; així, el simple fet de disposar d'un sistema informàtic i d'utilitzar-lo comporta la introducció d'elements relacionats amb la privacitat que, sense voler-ho, poden provocar afectacions a la intimitat o al mateix patrimoni. La resposta a un correu electrònic amb el número d'un compte bancari implica la introducció del patrimoni disponible en aquest compte, en el ciberespai, de la mateixa manera que l'acte de compartir una fotografia familiar a Facebook o informació sobre un viatge recent comporta el risc que això sigui utilitzat en contra de la dignitat o la intimitat de la persona.

En qualsevol cas, el primer condicionant perquè un objectiu sigui adequat a l'efecte de la fórmula del cibercrim és que s'hagi introduït al ciberespai. A partir del moment en què un objectiu s'introdueix en el ciberespai, de manera voluntària o involuntària, es pot convertir en adequat segons la valoració que en faci l'agressor motivat. Aquesta és, doncs, la primera divergència de les condicions que fan adequat un objectiu per al cibercrim, amb les quals, amb l'acrònim ***VIVA***, Felson va definir com a condicions o criteris que reflecteixen l'adequació de l'objectiu per al delicte:

- El **valor de l'objectiu** del crim
- La seva **inèrcia**
- La **visibilitat física** del crim
- La seva **accessibilitat**

La diferència és que, prèviament a tot això, la introducció de l'objecte per part de la mateixa víctima en el ciberespai és la condició primera i principal per a l'adequació al cibercrim.

Ara bé, i els altres caràcters de l'acrònim VIVA? Són vàlids per al cibercrim? Doncs bé, el primer element que cal analitzar és el del valor de l'objectiu.

Independentment del tipus d'objectiu de què es tracti (patrimoni, intimitat, llibertat sexual, etc.), en el ciberespai es dóna la particularitat que coses amb poc valor per si mateixes poden adquirir un valor molt important gràcies a la facilitat per a obtenir informació, relacionar-la amb l'obtinguda i convertir-la en un objecte de risc.

Així, quatre dígits sembla que no són valuosos, però si a aquests dígits, per mitjà de la *data mining*, s'associa el concepte *pin*, i es relaciona amb un usuari determinat, i si després es fa el mateix amb els nombres d'un compte bancari, etc., finalment aquests nombres tenen molt de valor. En qualsevol cas, és evident que com més valor té l'objectiu més possibilitat hi ha d'atac, i això serà igual en el ciberespai: els nombres de vint dígits són més buscats que els de quaranta, i les empreses més valuoses seran més buscades pels seus secrets comercials que les que no són conegudes, per posar-ne un exemple, i el cibercriminal decidirà segons el valor que ell mateix atorgui a l'objectiu.

Per contra, és més discutible que els altres elements de l'acrònim *VIVA* siguin vàlids per a la fórmula de l'adequació dels objectius en el ciberespai. Començant per la inèrcia, Felson la definia com les propietats intrínseques dels objectius que poden fer que ofereixi un grau diferent de resistència a l'atac.

Sense entrar en la discussió sobre la dificultat de separar inèrcia i accessibilitat, la veritat és que en el ciberespai els objectius generalment oferiran poca resistència, atès que es tracta de béns informacionals que es poden baixar fàcilment sense cap resistència.

Els béns en el ciberespai amb prou feines es diferenciaran entre si per unes condicions intrínseques més o menys importants (i no relacionades amb els guardians, ja que això és un altre tema); és a dir, per l'anomenada *inèrcia*, per a ser adequats a rebre un atac.

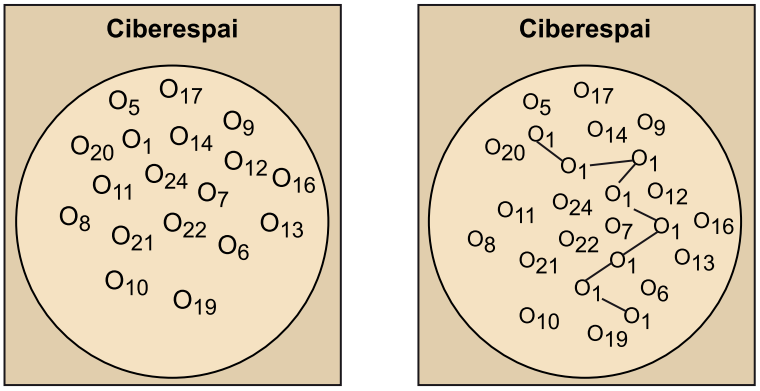
Passa una cosa semblant amb l'accessibilitat, definida per Felson com l'habilitat d'un agressor per a contactar amb un objectiu i emportar-se'l de l'escena del crim.

Com es pot comprendre, atesa la contracció de la distància en el ciberespai, tots els objectius que entrin en el ciberespai són, en aquest sentit, accessibles.

Hi pot haver observació del delinqüent per mitjà de sistemes de rastreig o de senyalització, però això no converteix l'objectiu en menys adequat, sinó el gestor del lloc (o el guardià si prové de la mateixa víctima el sistema i impedeix l'atac) en més eficaç. Si a això afegim que, en realitat, aquesta característica està més associada a l'agressor que a les particularitats de l'objectiu, podem afirmar que la característica en qüestió no és condicionant de l'adequació d'un objecte en el cibercrim.

Succeeix una cosa semblant, però no idèntica, amb el que Felson anomena *visibilitat de l'objectiu*, ja que si una cosa no és percebuda per l'agressor no la pot tenir com a blanc. El ciberespai és tan gran i tan universal, que és difícil fer-se visible, fins al punt que tots els usuaris constitueixen un garbuix en què és difícil distingir els uns dels altres. El que fa visibles els subjectes en el ciberespai és la seva interacció amb altres individus i amb altres serveis. Com més interacció amb altres agents, amb diferents pàgines web, amb diversos serveis, més possibilitat hi ha de ser percebut (ser visible) per part dels altres.

Figura 13. Visualització d'objectius en el ciberespai i interacció



Els objectius es dilueixen en el ciberespai, però l'objectiu 1 esdevé més visible quan interacciona i es mou per Internet.

La relació entre la interacció més gran d'un subjecte en el ciberespai amb la probabilitat de ser victimitzat es podria donar per provada a partir de diversos estudis empírics de victimització en el ciberespai:

- Així, **Alshalan** aconsegueix relacionar la victimització per virus informàtics, d'una banda, i de l'altra, per cibercrims com el ciberfrau en les diverses formes, *identity theft*, *phishing*, fraus de seguretat, *cyber-stalking*, *cyber-harassment*, extorsió i *hacking*, amb la interacció de la víctima en el ciberespai concretada en la seva freqüència d'accés i el temps que passa a Internet. Efectivament, i a partir de la hipòtesi que el comportament de la víctima en el ciberespai és un predictor important de la seva victimització, conclou que com més alta és la freqüència d'accés a Internet més risc hi ha de victimització; i el mateix succeeix amb la quantitat de temps més gran connectat en el ciberespai, com també amb la realització d'activitats a Internet que comporten la divulgació de dades personals de tipus financer i, exclusivament per a la infecció per virus, amb el fet de tenir fills que accedeixen al ciberespai.

Ús freqüent d'Internet

En un estudi d'Ybarra i Mitchell es relaciona de manera significativa l'ús freqüent d'Internet o l'ús de sales de xat amb una exposició més alta a la pornografia per part de menors d'edat, i ja hem vist anteriorment que també hi havia una relació intensa entre la interacció de la víctima en xats i d'altres amb la victimització per *online grooming* o delictes similars.

- Per la seva banda, **Yucedal**, que examina els factors que incideixen en la victimització per conductes de *spyware* i *adware*, conclou que el comportament quotidià en relació amb l'ús d'Internet és un element determinant de la victimització per aquests delictes que exigeixen, generalment, que

el mateix subjecte, en visitar un web determinat o en descarregar-se un programa, carregui involuntàriament el virus.

- Finalment, **Choi** duu a terme una identificació interessant entre els comportaments quotidians a Internet i la teoria dels estils de vida i la utilització de sistemes de protecció amb diversos tòpics relacionats amb la teoria de les activitats quotidianes. Arriba a la conclusió, després confirmada per Yucedal, que el *hacking* és més factible en persones amb ordinadors personals que utilitzen molt Internet i que realitzen conductes de risc en línia. I això és així amb un altre tipus de cibercrims.

Per tant, en el ciberespai com més interacció d'un subjecte, plasmada en més temps en línia o una varietat superior d'activitats a Internet, més aptitud d'aquest individu per a ser un objectiu adequat. És obvi que això s'ha de precisar i concretar de manera empírica i diferenciant cadascuna de les activitats. Però també ho és que només amb la interacció es produirà el contacte (necessari per al delicte) en el vast ciberespai entre l'agressor motivat i la víctima, i també que es produirà segons que aquesta "es mogui" per Internet, especialment si recordem que molts atacs a Internet queden estàtics en espera que la víctima entri a la pàgina o baixi l'arxiu, de manera que amb la seva conducta es converteixi en un objectiu adequat.

Exemple d'activitats en xarxa

Baixada d'arxius, entrada en plataformes P2P, realització de compres en línia, creació de perfils en xarxes socials, etc.

Podem concloure, doncs, que les condicions per a l'adequació de l'objectiu del crim VIVA no són transportables al ciberespai, excepte en el cas del valor. Així, caldrà sumar el valor a la primera condició essencial, i és que l'objectiu hagi estat introduït en l'espai virtual. S'hi ha d'afegir la interacció del titular de l'objecte en el ciberespai com a condicionant fonamental de la victimització.

Si sumem els tres elements ens queda l'acrònim ***IVI***, com a definidor de les condicions que determinaran que una persona o algun dels seus béns pugui ser objectiu adequat d'un cibercrim:

- **Introducció**: que el bé o la persona hagi estat introduït en el ciberespai.
- **Valor**: que tingui un valor que el faci atractiu per al cibercriminal.
- **Interacció**: que la persona amb la titularitat del bé interaccioni a Internet de manera que hi esdevingui visible i pugui contactar amb l'agressor motivat.

2.3.3. Guardians capaços

L'últim element que cal analitzar dins la teoria de les activitats quotidianes és el guardià capaç. La unió dels factors que hem analitzat, la compressió espaciotemporal per a la comunicació entre les persones, la popularització i el nivell transnacional d'aquest àmbit, etc., dificulten en el ciberespai l'actuació del guardià (que ha de ser) capaç de protegir la víctima, cosa que, al seu torn, interacciona amb el factor agressor motivat en percebre aquesta reducció d'obstacles i disminuir la percepció de risc de ser caçat que tindrà el (ciber)criminal.

La noció de *guardià capaç* esdevé important, però també complexa, quan pensem en el cibercrim. Potser en aquest sentit és més útil la diferenciació entre el mànager, o gestor del lloc, i el guardià que opera directament sobre la víctima o l'objectiu potencial. L'absència de mecanismes centrals de concessió dels serveis d'Internet, i també de sistemes de control formal supranacional que prenguin decisions relatives als serveis que estiguin per sobre de les legislacions estatals, comporta la impossibilitat d'uns "gestors centralitzats" que vigilin el ciberespai d'una manera global i, així, protegeixin les víctimes potencials. No és que a Internet no hi hagi policia, ni que no hi hagi gestors de llocs en alguns d'aquests, sinó que estan molt focalitzats i tenen un àmbit d'incidència molt reduït, si bé és indubtable que en determinats llocs web, com les xarxes socials, els gestors poden i han de funcionar tutelant la interacció dels usuaris d'aquestes xarxes. Aquestes dificultats de gestió d'un lloc tan vast, d'altra banda, són perfectament conegudes pels usuaris d'Internet, que perceben que "navegar pel ciberespai" és una activitat en què la intervenció dels mitjans de control formal està molt més diluïda.

A banda dels gestors del lloc, tenim els guardians dels objectius adequats. Ho pot ser qualsevol altre sistema personal o no, aliè a la víctima o imposat per ella mateixa, que serveixi com a forma de protecció. De la mateixa manera que els sistemes de seguretat físics, com les alarmes o els forrellats especials, s'han mostrat eficaços davant la criminalitat, també ho poden ser els sistemes que exerceixen la mateixa funció en el ciberespai, com els antivirus o qualsevol altre sistema de seguretat. Els estudis empírics demostren que aquests sistemes poden ser molt eficaços per a evitar la victimització pel cibercrim. En qualsevol cas, es tracta d'uns guardians capaços estretament relacionats amb l'element objectiu adequat; no són sistemes de protecció incorporats o que funcionin de manera autònoma al comportament del mateix subjecte que protegeixen, sinó que, per contra, tots els elements de protecció esmentats depenen de la víctima per a funcionar i actualitzar-se. Els que Cohen i Felson definien com a guardians capaços generalment eren propers a la víctima (veïns, ciutadans anònims, etc.), però no "part d'ella", com sí que ho és el *software* que la víctima posa en el seu ordinador. En el cas del ciberespai, la mateixa víctima, per tant,

el mateix objectiu, és la que ha d'incorporar els seus guardians capaços. Així doncs, el guardià capaç, en el ciberespai, és pràcticament un autoguardià que depèn de la mateixa víctima.

Certament, els sistemes d'autoprotecció imposats per la víctima no són els únics que poden desenvolupar la seva eficàcia en relació amb els cibercrims. En altres delictes adreçats contra menors poden ser interessants altres vigilants capaços com ara el control familiar sobre l'activitat a Internet o la creació de perfils específics que impedeixin l'accés a determinats recursos web. A això caldrà sumar en el futur mitjans de control i de protecció institucional, atès que la seguretat en el ciberespai exigeix una intervenció i un esforç plural de les institucions i els usuaris. En qualsevol cas, això sembla més llunyà.

Davant la inexistència actual de mitjans de control formal més institucionalitzats, com les forces policials, la funció preventiva (no la reactiva) de les quals sembla impossible en el ciberespai, l'autodefensa continua essent, davant d'aquests crims, com potser també respecte dels altres, la millor forma de protecció.

3. El paper de la víctima en la prevenció del ciberdelicte

Generalment, l'element central per a analitzar i comprendre el crim és l'agressor, ja que en la motivació que té també hi ha definit l'objectiu sobre el qual es produirà l'atac i les condicions de defensa d'aquest. Això podria fer pensar que l'agressor tria completament la víctima independentment de l'actuació d'aquesta i que, per a ella, el fet de ser-ho és una cosa aleatòria. Però si això no és així a l'espai físic encara sembla que ho és menys en la cibercriminalitat. Són molts els ciberatacs que es realitzen en el ciberespai sense cap objectiu determinat, de manera que la interacció concreta de la víctima és el que la converteix en objectiu adequat, i no la voluntat del cibercriminal, i això és així perquè el ciberespai és un àmbit d'oportunitat nou (diferent).

La diferència principal de l'ampolla del crim en el ciberespai és que, com que es tracta d'un àmbit comunicatiu vast i immens, sense barreres ni dimensions, en què el contacte depèn de les voluntats d'interacció entre els individus, de manera que sense la interacció de dues persones no hi haurà contacte per més que un dels dos ho vulgui, l'agressor ja no és l'únic i principal subjecte que defineix, des de la seva intenció, l'àmbit de risc. Ho fa, sens dubte, perquè actua amb una voluntat criminal, però només ho farà sobre l'objecte (per a ell valuós) que sigui en el ciberespai, que interaccioni amb ell i que no estigui protegit, de manera que tot això converteix la víctima en un element explicatiu (*a posteriori*) de l'esdeveniment delictiu molt expressiu.

Hi ha tres factors que fan que la víctima adquireixi una importància especial per a explicar i prevenir el delicte en el ciberespai:

- En primer lloc, com hem vist, la víctima potencial del ciberdelicte té, sobretot, una gran capacitat per a deixar fora de l'àmbit de risc allò que no vol que es vegi afectat pel delicte, de manera que determina, des del primer moment, quan incorpora determinats béns i esferes de la seva personalitat en el ciberespai, els marges genèrics de l'àmbit de risc al qual estarà sotmesa. Si no entra en el ciberespai o no hi té relacions personals, aquests béns no podran ser afectats, igual que no ho podrà ser el seu patrimoni si no utilitza la banca electrònica i no comunica les seves claus a Internet. Es pot dir que això és idèntic al fet que si la víctima no surt al carrer no pot ser-hi víctima de cap robatori.

- En segon lloc, la víctima defineix amb la interacció que efectua en el ciberespai el grau de visualització dels seus objectius i, per tant, les possibilitats de contacte amb un agressor motivat en un mateix temps i espai o en un altre de diferent. Hi ha estudis que demostren la importància especial del comportament de la víctima en la victimització per la cibercriminalitat

informàtica. Tots confirmen un aspecte que ja havíem afirmat, i és que la víctima defineix l'àmbit de risc al qual pot accedir l'agressor motivat. Es pot argumentar que això ja és el que succeeix a l'espai físic amb l'augment de les possibilitats de ser víctima de delictes en el cas de visitar uns llocs concrets, fer-ho en determinats moments del dia, etc. Certament és semblant, ja que es basa en el fet que les activitats quotidianes de la víctima són part de l'explicació de l'esdeveniment criminal. L'única diferència és que en el ciberespai no cal temps ni distància física per a la interacció, i que la interacció a Internet depèn igualment de tots els agents, de manera que, una vegada hi ha una conducta criminal iniciada, el fet que afecti una, dues, centenars o milers de persones dependrà molt del que facin aquestes.

- Finalment, i en tercer lloc, la víctima és pràcticament l'única que pot incorporar guardians capaços per a l'autoprotecció. Com que en aquest àmbit criminològic no hi ha distàncies físiques ni guardians formals institucionalitzats, l'ús quotidià que faci de les TIC, i especialment la incorporació (o no) de sistemes digitals d'autoprotecció, seran determinants a l'hora de convertir-se en víctima del cibercrim. Si tenim en compte a més que a Internet, també, com que no hi ha distàncies, el desplaçament del cibercriminal cap a altres objectius resulta, no solament fàcil, sinó fins i tot en molts casos (virus i altres) també instantani, i que l'adreça del nou objecte de l'atac la marcarà l'absència de sistemes de protecció o les vulnerabilitats de l'objectiu (aleshores adequat), sembla evident concloure el protagonisme de la víctima en el procés d'autoprotecció i, en cas de no tenir-ne, de victimització.

Per tant, en resum, si la conducta de la víctima és un factor determinant especialment significatiu del delicte, també serà, per això, un condicionant important per a prevenir-lo. L'educació de la víctima en seguretat informàtica, la seva conscienciació per a adoptar programari de protecció i de rutines segures en l'actuació quotidiana en el ciberespai, a més de la informació real sobre els riscos en el ciberespai, serien els primers passos que cal adoptar per a prevenir el cibercrim.

4. La prevenció situacional del ciberdelicte

Una vegada s'han estudiat les característiques del ciberespai i aquest s'ha determinat com un àmbit d'oportunitat, a més de la importància de l'actuació de la víctima per a delimitar el seu àmbit de risc, el pas següent per a concloure el temari és fer una repassada breu de les mesures que es poden dur a terme per a prevenir el cibercrim.

Partint de la teoria de les activitats quotidianes, si no hi ha agressor motivat o hi ha guardià capacitat no hi haurà delicte en línia, independentment del que faci la víctima o el titular de l'"objectiu adequat". Però, com que hi ha pocs gestors del lloc i pocs guardians capaços a Internet, i la compressió de la distància situa en un mateix pla milers de potencials agressors motivats, sembla obvi que la conducta de la víctima determinarà significativament el risc criminal a què estigui sotmesa. Ho farà des del moment en què entri en el ciberespai, amb la selecció dels béns patrimonials i relacionats amb la privacitat, continguts en el seu sistema informàtic i que entren en aquest espai de risc nou; també quan tria el tipus d'activitats que realitza a Internet (socials, personals, econòmiques, etc.) i quan decideix els llocs que visita, els contactes personals que realitza, els arxius que baixa, i, molt especialment, els mitjans tecnològics (programari antivirus, *firewalls* i altres sistemes de protecció i de detecció d'accessos no autoritzats, de l'entrada de programari maliciós i d'altres atacs; però també els sistemes de control parental, etc.) que incorpora al seu sistema informàtic com a autoguardians per a protegir les seves dades i altres aspectes.

No obstant això, partint de les premisses de la prevenció situacional, que posa l'èmfasi en la importància dels factors ambientals, a més de treballar amb els aspectes més relacionats amb la víctima, es pot intervenir en les característiques que constitueixen el ciberespai que fan d'aquest un nou àmbit delictiu, per a reduir la delinqüència amb una sèrie de mesures sobre les quals es pot incidir, com veurem tot seguit.

1) El primer bloc de mesures està destinat a reduir l'àmbit d'incidència, entre les quals s'inclouen quatre mesures específiques:

- **No introducció d'objectius**. És la primera mesura i, al seu torn, la més significativa. Es tractaria que l'usuari, víctima potencial, no posi a disposició de terceres persones béns o informació que, mitjançant tècniques com la mineria de dades, poden aportar als ciberdelinqüents informació amb la qual poden organitzar els ciberatacs, o bé impedint a la mateixa víctí-

ma que baixi arxius que poden estar infectats de virus (controladors de seguretat ActiveX) o que, mitjançant els diferents sistemes de filtratge de continguts, accedeixi a pàgines web en les quals es difon material perillós, cosa que en el cas dels menors es concreta en les diverses formes de programari de control parental.

- **Separació d'objectius en el ciberespai**. Aquesta segona mesura es podria plasmar amb la creació de ciberespais tancats i separats de la Xarxa (n'és un exemple Internet2).

- **Identificació de riscos**. La tercera mesura, la identificació de riscos per part dels usuaris, es podria realitzar mitjançant campanyes d'informació sobre els perills que implica l'exposició a determinats àmbits del ciberespai (baixada de continguts amb drets d'autor, suport a grups ciberactivistes, els webs de pornografia, etc.)

- **Descontaminació de residus**. Finalment, la descontaminació o neteja de residus, com esborrar virus latents, que impediria el creixement il·limitat dels perills d'Internet, de manera que, com si es tractés d'una malaltia suposadament extinta que trobés un nou portador, augmentés la virulència i s'estengués en progressió geomètrica.

2) El segon bloc de mesures tracta d'augmentar l'esforç percebut per l'ofensor motivat:

- **Control d'accés als sistemes**. S'inclourien per tant, en primer lloc, les mesures destinades a controlar l'accés als sistemes amb la incorporació per part de la víctima potencial de tallafocs, claus d'accés al sistema i a les xarxes a més de la renovació periòdica pertinent, l'actualització de sistemes operatius, etc.

- **Detecció de l'atac**. En segon lloc, s'inclouen mesures que, una vegada que la víctima és atacada, ho detecti i impedeixi que finalitzi amb èxit. Per a això hi ha tots els sistemes antivirus que intervenen un cop la infecció s'ha produït i que tracten d'identificar l'amenaça, de bloquejar-la i finalment d'eliminar-la. D'una manera semblant actuen els programes *antispyware* respecte del programari que no infecta el nostre sistema però tracta d'adquirir informació valuosa (*keyloffers*, *sniffers* i d'altres) i que són bloquejats per aquest tipus de programari defensiu. Pel que fa a l'*antispam*, es tracta d'un tipus de programari que filtra els correus electrònics de manera que detecta l'entrada de correus *spam* i els situa a la carpeta de *spam*.

- Un altre tipus de mesures que pot augmentar l'esforç percebut, objectiu que també es pot aconseguir si el transgressor és retirat, encara que sigui temporalment, de manera que hagi de tornar a començar per perpetrar l'atac. Això es pot fer de maneres diverses en el ciberespai:

– Tancament de pàgines web per part de les autoritats estatals competents.

– Sol·licitud de retirada de contingut il·lícit com a primer pas per a tancar la pàgina web.

– Mecanismes de denúncia en xarxes socials que permeten que un contingut o una pàgina web siguin retirats immediatament pel controlador de la xarxa social, o tallant l'accés a una determinada IP identificada prèviament com a perillosa. Aquest tipus de mesures poden aconseguir temporalment l'objectiu final, però, en qualsevol cas, l'agressor ha de tornar a començar i això implica una reiteració d'esforç.

– Finalment, quedaria controlar els elements que faciliten la comissió del delicte. Es tracta de mesures com ara que els prestadors de servei tinguin obligacions de vigilància o que les xarxes socials controlin més bé l'accés a les dades personals dels usuaris.

Altres formes de detecció d'atacs

Juntament amb els antivirus i els programes *antispyware* que es poden instal·lar en el sistema per a l'autoprotecció, també hi ha altres formes de detecció de l'atac que actuen quan ja s'ha produït l'atac contra l'usuari però encara no s'ha perfeccionat del tot, de manera que pot ser identificat pel vigilant víctima per a evitar que tingui èxit. És el que succeeix amb els sistemes de protecció de la banca electrònica, que vigilen no solament l'accés als comptes sinó fins i tot, una vegada s'ha produït una transferència, la legalitat d'aquesta abans que els diners s'hagin retirat definitivament.

3) El tercer grup de mesures tenen com a objectiu augmentar en l'agressor la percepció que la seva conducta comporta un risc per a ell, concretament, el de ser detingut:

- **Nous guardians**. Les primeres mesures han d'anar orientades a augmentar el nombre de guardians. El ciberespai no és un àmbit en què hi hagi guardians formals derivats d'una autoritat centralitzada, però si que existeixen un altre tipus de vigilants en llocs concrets com les xarxes socials o els fòrums d'Internet, moderadors que hi actuen i que poden vigilar la realització d'expressions injurioses o de proposicions sexuals i altres activitats d'assetjament. Juntament amb això, també hi ha altres sistemes de vigilància la legitimitat de la qual, però, és més discutida. Es tracta dels sistemes d'intel·ligència com Echelon o el seu equivalent europeu Enfopol que, de manera no oficial, capten totes les transmissions d'informació realitzades per mitjà de xarxes telemàtiques amb selecció de termes i conceptes clau i que podria ser que violin la intimitat de les persones d'una manera flagrant.

- **Reducció de l'anonimat**. Després s'inclouen totes les que tracten de reduir l'anonimat amb què generalment actua l'agressor. Es podria aconseguir mitjançant el registre previ amb la utilització de dades personals, com ja es fa en algunes pàgines web i xarxes internes que exigeixen als usuaris

una identificació amb dades o claus personals en l'àmbit institucional estatal, en l'empresarial, en l'educatiu, en el social i en d'altres. Més sofisticada i llunyana, però no impossible ateses les experiències que hi ha en altres mitjans, seria la implantació de sistemes d'identificació i autenticació biomètrics, entre els quals hi hauria el reconeixement facial, el reconeixement d'empremtes dactilars, l'escàner de la geometria de la mà o el reconeixement de l'iris.

- **Reforçament de la vigilància formal**. Altres mesures adreçades a incrementar el risc percebut pel criminal a l'espai físic són el reforçament de la vigilància formal i la introducció de gestors de llocs. Encara que no hi hagi cap autoritat centralitzada en el ciberespai, els diferents estats estan obligats a investigar i perseguir la criminalitat que s'hi produeix i que pot danyar els béns jurídics dels seus nacionals, i per això cada vegada més utilitzen els mitjans tecnològics per a la vigilància del ciberespai per mitjà d'equips especialitzats de persecució d'aquest tipus de delinqüència. Actualment, la intervenció policial davant la cibercriminalitat se centra en la persecució de la pornografia infantil a Internet, tant de les pàgines que es dediquen a la distribució d'aquest material com dels que posseeixen aquest tipus de material prohibit.

- **Millora dels sistemes de vigilància**. Finalment, i com a mesures complementàries a les anteriors, també és possible l'aplicació de mesures tendents a facilitar els mitjans de vigilància, a millorar-los perquè siguin més eficaços. En aquest sentit, la millora de la identificació de les adreces IP i en general la millora dels sistemes de detecció de l'empremta digital serien essencials per a la identificació dels infractors. Com a mesures de facilitació dels mitjans de vigilància també se sol esmentar la millora del disseny de l'espai per a fer-lo més defensable.

Contraatacs

I, a aquestes quatre classes de mesures, darrerament se n'hi afegeix una altra que no està institucionalitzada però que sens dubte alguns tipus de cibercriminals la tenen en compte. Es tracta de l'augment dels riscos derivats de la realització d'il·lícits a Internet no consistents a ser detingut o jutjat sinó a ser víctima de danys o atacs als seus sistemes a causa del que han realitzat ells. Això succeeix amb algunes formes de *hacking*, que porten associades contraatacs dels sistemes que es defensen infectant el sistema agressor, però molt especialment amb algunes conductes il·lícites relacionades amb els drets d'autor, atès que alguns dels arxius compartits que aparentment contenen obres de l'enginy més aviat són virus en alguns casos carregats pels interessats en què aquests llocs web no prosperin i que poden causar danys greus al subjecte que els baixa.

4) El quart grup de mesures tracten de disminuir els guanys que l'agressor percep que obtindrà de la conducta criminal:

- **Ocultació dels objectius**. En primer lloc hi ha maneres d'ocultar els objectius als "ulls" de l'agressor motivat. Es pot fer mitjançant la utilització de sistemes d'encriptació, i ho ha de fer la mateixa víctima a les xarxes socials si no vol compartir aquesta informació amb els altres. També és convenient la no-utilització de les claus bancàries, dels números de comp-

te i d'altres dades necessàries per a la defraudació final a Internet, en el ciberespai, ni per correu electrònic ni en altres sistemes d'enviament telemàtic. Finalment, una forma eficaç d'ocultació dels objectius pot constituir en general el perfeccionament dels sistemes de pagament per Internet que permetin la no-utilització de claus o dades bancàries o, fins i tot, l'exigència d'un altre tipus d'informació que no sol ser necessària per a les transaccions comercials, com ara els nombres impresos en la targeta, i d'altres.

- **Desplaçament d'objectius**. En segon lloc, una altra manera de disminuir els guanys percebuts és desplaçant objectius. A Internet el desplaçament s'ha d'entendre en un sentit diferent del tradicional de moviment de l'objecte que cobreix una distància determinada, més aviat com a canvi en la ubicació electrònica en què hi ha una cosa continguda cap a un àmbit nou dins (fins i tot fora, encara que aleshores estaríem més prop de la retirada de l'objectiu) del ciberespai. Així, en alguns casos caldrà realitzar un canvi en les adreces web, adreces de domini i d'altres amb una finalitat defensiva, com també utilitzar discos durs diferents en un mateix sistema per a tenir separada i més protegida la informació, i fins i tot en discos durs extraïbles en el cas que es tracti d'informació confidencial que es pot utilitzar i retirar quan s'accedeix al ciberespai. També es desplacen els objectius quan es creen sistemes de pagament alternatius als tradicionals (sistemes bancaris de targeta de crèdit, per exemple). Amb això s'aconsegueix que un objectiu sigui, per si mateix, menys atractiu.

- **Eliminació de beneficis**. En tercer lloc, l'atac cibercriminal pot ser combatut eliminant els beneficis que l'agent n'obté, i influir així en la valoració sobre les possibilitats futures d'obtenció de guanys per aquestes conductes. En la cibercriminalitat econòmica és important la persecució dels que permeten obtenir els beneficis al delinqüent. En el cas de la pornografia infantil, això es pot aconseguir amb la punició de la tinença d'aquests materials, de manera que al subjecte que decideix tenir aquest material després de pagar el que el distribueix li costi més la decisió pel fet d'incrementar el perjudici que es pot derivar d'aquest fet. De la mateixa manera, i atès que, la majoria dels cibercrims econòmics són duts a terme per bandes organitzades, la persecució del blanqueig de capitals d'aquestes organitzacions criminals pot ser molt eficaç.

- **Foment de mitjans lícits**. Finalment, es tracta de fer atractius i més rendibles els mitjans lícits. Això seria especialment útil en intercanvis de material protegit pels drets de propietat intel·lectual, per exemple potenciant formes de distribució lícita, i fer poc rendible per al consumidor accedir al mercat il·legal quan per un preu baix s'obté un producte millor en el mercat legal.

5) L'últim grup de mesures estan adreçades a eliminar les excuses o justificacions morals, de manera que incrementen els sentiments de vergonya o culpabilitat en el delinqüent:

- **Fixació de regles**. Per a això, és important la fixació de regles que poden ser normes jurídiques, ja que hi ha sectors de la població que donen valor ètic al que és normatiu, o també regles socials que responguin a la moral col·lectiva. En aquest sentit, és important en el ciberespai l'enfortiment de regles del bon ús d'Internet, que serviran perquè qui accedeixi a aquest nou àmbit de comunicació social en comprengui els usos bàsics i el funcionament acceptat per la societat que el constitueix. A més a més, seria recomanable l'harmonització del dret que regula el ciberespai a escala internacional, ja que en cas contrari sempre es pot utilitzar l'"excusa" que en aquest altre país no se sanciona un comportament determinat.

- **Respecte del *copyright* o del *copyleft***. És important també que en les pàgines web s'incloguin referències clares a les llicències *copyright* o *copyleft* i d'altres, i que en les xarxes socials s'avisi sobre la privacitat de les imatges i altres elements personals dels usuaris d'aquestes.

- **Reforç d'actituds positives**. Una altra forma de conscienciació és el reforç de les actituds positives, en aquest cas dels negocis lícits, amb vista al debilitament moral dels que no ho són.

- **Foment del comportament lícit**. Finalment, dins d'aquesta categoria es poden incloure mesures que facilitin el comportament lícit, com la creació de competicions legals per a *hackers* o el mateix enfortiment i difusió del programari lliure com una manera de fomentar la modificació i l'evolució dels sistemes informàtics; servirien perquè moltes persones continuessin realitzant les seves activitats en el ciberespai però d'una manera lícita.

Resum

El ciberespai és un àmbit virtual que té unes dimensions espaciotemporals diferents de les del món físic i que es caracteritza per la transnacionalitat, la neutralitat, la universalització del mitjà i la seva popularització en totes les societats i estrats, a més d'estar subjecte a una revolució permanent, d'atorgar facilitats per a l'anonimat i de presentar dificultats per a perseguir les activitats criminals.

Tot això fa que la víctima adquireixi un protagonisme més gran en el procés de victimització. Com hem vist, la víctima defineix el seu àmbit d'oportunitat criminal atès que ella mateixa determina des del primer moment, quan incorpora determinats béns i esferes de la seva personalitat en el ciberespai, els marges genèrics de l'àmbit de risc al qual estarà sotmesa i atès que, a més, com que en aquest àmbit criminològic no hi ha distàncies físiques ni guardians formals institucionalitzats, l'ús quotidià que faci de les TIC i especialment la incorporació (o no) de sistemes digitals d'autoprotecció seran determinants a l'hora de convertir-se en víctima del cibercrim. Si, d'altra banda, tenim en compte que a Internet, també, com que no hi ha distàncies, el desplaçament del cibercriminal cap a altres objectius resulta no solament fàcil sinó fins i tot en molts casos (virus i d'altres) també instantani, i que l'adreça del nou objecte de l'atac la marcarà l'absència de sistemes de protecció o les vulnerabilitats de l'objectiu (aleshores adequat), sembla evident concloure el protagonisme de la víctima en el procés de victimització.

Per a combatre aquest tipus de delinqüència per mitjà de l'anàlisi de les teories de l'oportunitat delictiva, es proposen una sèrie de mesures generals a partir de les quals s'estableixen unes mesures més concretes. Entre aquestes mesures trobem més formació dels usuaris per a adoptar rutines segures, a més de potenciar la utilització de sistemes d'autoprotecció, la implantació de guardians capaços en el ciberespai, el trasllat al ciberespai de sistemes de prevenció comunitària informal i la influència en la decisió de l'agressor motivat perquè finalment no cometi el delicte.

Exercicis d'autoavaluació

1. En el ciberespai...

a) les distàncies s'expandeixen i, per tant, la comunicació s'expandeix.
b) les distàncies es contreuen i, per tant, les possibilitats de comunicació es redueixen.
c) les distàncies es contreuen i, per tant, la comunicació s'expandeix.
d) Cap de les respostes anteriors no és correcta.

2. Perquè un objectiu sigui considerat adequat en el ciberespai...

a) ha de ser introduït i ha de tenir valor.
b) ha d'interaccionar per passar desapercebut.
c) ha de tenir sempre valor econòmic.
d) ha de ser introduït, ha d'interaccionar i ha de tenir valor.

3. Quina de les característiques següents no és configuradora del ciberespai?

a) Localitzat.
b) Anonimitzat.
c) Neutral.
d) Universal.

4. Des d'una posició mixta, el cibercrim...

a) és idèntic estructuralment al delicte comès a l'espai físic; només en canvia l'aspecte, però no els caràcters configuradors.
b) comparteix amb la delinqüència tots els elements definidors del concepte de crim, però s'esdevenen d'una manera tal en el nou àmbit que és el ciberespai que pot influir significativament en l'explicació del delicte.
c) és un tipus de delinqüència nova per a la qual no són vàlides les teories tradicionals creades per a explicar l'espai físic.
d) és un tipus de delinqüència nova, però s'hi poden aplicar les mateixes teories creades per a l'espai físic.

5. Indiqueu la resposta correcta entre les opcions següents:

a) En el ciberespai no hi ha barreres per a la comunicació i la interacció entre individus.
b) El ciberespai està situat en un lloc concret, però en un sentit funcional és en tots alhora.
c) A Internet no hi ha nodes centrals, però sí nodes que actuen com a centres locals.
d) L'usuari d'Internet pot navegar pel ciberespai a qualsevol hora, però no pot accedir a totes les zones del ciberespai.

6. L'enfocament de les activitats quotidianes explica a escala micro l'esdeveniment criminal. Perquè es produeixi un delicte han de coincidir en l'espai...

a) un objectiu adequat i un agressor motivat.
b) un delinqüent motivat i un guardià capaç.
c) un agressor motivat i un objectiu adequat amb l'absència d'un guardià capaç.
d) un agressor motivat i un objectiu adequat amb la presència d'un guardià capaç.

7. Des de la perspectiva de la teoria de les activitats quotidianes, podem considerar un objectiu adequat...

a) les víctimes.
b) les víctimes i l'objecte del delicte.
c) l'objecte del delicte.
d) Cap de les respostes anteriors no és correcta.

8. Un agressor en el ciberespai...

a) pot atacar diverses persones amb una única conducta.
b) pot atacar des del lloc físic on es troba i que els efectes de l'atac es produeixin a milers de quilòmetres de distància.
c) pot realitzar un atac i que els efectes no es despleguin a l'instant.
d) Totes les opcions anteriors són correctes.

9. Indiqueu l'afirmació correcta entre les opcions següents:

a) La introducció d'un objectiu en el ciberespai no sempre és voluntària.
b) En el ciberespai és difícil passar desapercebut.
c) El cibercrim té costos de desplaçament i de fugida per a l'agressor.
d) El cibercrim no té cap cost temporal.

10. L'actuació de la víctima és important amb vista a la prevenció perquè...

a) pot deixar fora de l'àmbit de risc el que no vol que es vegi afectat.
b) amb la seva interacció defineix en el ciberespai el grau de visualització dels seus objectius.
c) pot incorporar guardians capaços per a l'autoprotecció.
d) Totes les respostes anteriors són correctes.

Solucionari

Exercicis d'autoavaluació

1. c

2. d

3. a

4. b

5. a

6. c

7. b

8. d

9. a

10. d

Glossari

adware *m* Programa autoexecutable que, generalment sense el coneixement ni el consentiment de l'usuari, mostra publicitat a l'ordinador en instal·lar-se o en interaccionar amb determinades pàgines web, i que pot servir per a espiar els seus hàbits a Internet.

antispyware *m* Aplicació que s'encarrega de buscar, detectar i eliminar espies en el sistema.

bot *m* Tipus de virus que permet l'accés remot del sistema informàtic per mitjà de la Xarxa.

IP (protocol d'Internet) *m* Codi emprat en xarxes de comunicacions per a identificar de manera inequívoca la procedència d'una connexió.

IRC *m* Programa que permet desenvolupar converses en línia en temps real amb persones d'arreu del món en què s'escriuen missatges per Internet.
en Internet relay chat

ordinador zombi *m* Ordinador personal que després d'haver estat infectat per algun tipus de *malware* pot ser utilitzat per una tercera persona per a executar activitats hostils.

spyware *m* Virus que captura informació dels sistemes informàtics.

TCP (protocol de control de transmissió) *m* Protocol fonamental a Internet.

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

WWW *m* Sigla que identifica l'expressió en anglès World Wide Web, literalment, 'xarxa informàtica mundial'. Xarxa global d'intercanvi de documents per mitjà d'hipertext comunament coneguda com a Internet.

Bibliografia

Aguirre Romero, J. M. (2004, juliol-octubre). "Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI" [en línia]. *EREL* (núm. 27). Madrid: Universitat Complutense de Madrid. <http://www.ucm.es/info/especulo/numero27/cibercom.html>

Alcantara, J. (2011). *La neutralidad en La Red, y porqué es una mala idea acabar con ella*. Madrid: Biblioteca de Las Indias.

Alshalan, A. (2006). *Cyber-Crime Fear and Victimization: An Analysis of A National Survey*. Mississipí: Universitat Estatal de Mississipí.

Bossler, A. M.; Holt, T. J. (2009, gener-juny). "Online Activities, Guardianship, and Malware Infection". *IJCC* (vol. 3, núm. 1).

Brantingham, P. J.; Brantingham, P. (2001). "The implications of the criminal event model for crime prevention". A: R. F. Meier; L. W. Kennedy; V. F. Sacco (eds.). *The Process and structure of Crime. Criminal events and crime analysis*. New Jersey: Transaction Publishing ("ACT", vol. 9).

Castells, M. (2006). *La era de la información*. Vol. 3: *Fin de milenio*. Madrid: Alianza.

Choi, K. (2008, gener-juny). "Computer Crime Victimization and Integrated Theory: An Empirical Assessment". *IJCC* (vol. 2).

Clarke, R.; Felson, M. (eds.) (1993). *Routine activity and rational choice*. New Brunswick, NJ: Transaction Publishers ("ACT", vol. 5).

Cohen, L.; Felson, E. (1979). "Social change and crimen rate trends: a routine activity approache". *ASR* (vol. 44).

Cornish, D. V.; Clarke, R. V. (2003). "Opportunities, precipitator and criminal decisions: A reply to Wortley's critique of situational crime prevention". A: M. Smith; D. B. Cornish (coords.). *Theory for Practice in Situational Crime Prevention*. Monsey, NY: Criminal Justice Press ("CPS", 16).

Grabosky, P. (2001). "Virtual Criminality: Old Wine in New Bottles?". *SLS* (núm. 10).

Graham, P. W. (2002). "Space and Cyberspace: on the enclosure of consciousness". A: J. Armitage; J. Roberts (eds.). *Living with cyberspace: technology & society in the 21st century*. Londres: Continuum International Publishing Group.

Gutiérrez Puebla, J. (1998). "Redes, espacio y tiempo". *AGUC* (núm. 18).

Kitchin, R. M. (1998). "Towards geographies of cyberspace". *PHG* (vol. 22, núm. 3).

Medina Ariza, J. J. (1998). "El control social del delito a través de la prevención situacional". *RDPC* (2a. època, núm. 2).

Miró Llinares, F. (2011). "Cibercrímenes económicos y patrimoniales". A: I. Ortíz de Urbina Gimeno (dir.). *Memento práctico penal y económico de la empresa 2011-2012*. Madrid: Francis Lefebvre.

Miró Llinares, F. (2011). "La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen". *RECPC* (núm. 13-07). <http://criminet.ugr.es/recpc/13/recpc13-07.pdf>

Miró Llinares, F. (2005). *Internet y delitos contra la propiedad intelectual*. Madrid: Iberautor Promociones Culturales.

Pease, K. (2001). "Crime futures and foresight: Challenging criminal behaviour in the information age". A: D. Wall (ed.). *Crime and the Internet*. Londres: Routledge.

Serrano Maíllo, A. (2009). *Oportunidad y delito*. Madrid: Dykinson.

Serrano Maíllo, A. (2009). *Introducción a la criminología* (6a. ed). Madrid: Dykinson.

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

Ybarra, M. L.; Mitchell, K. (2005). "Exposure to Internet Pornography among Children and Adolescents: A National Survey". *CpB* (vol. 8, núm. 5).

Yucedal, B. (2010). "Victimization in cyberspace: An application of routine activity and lifestyle exposure Theories" [en línia]. <http://etd.ohiolink.edu/send-pdf.cgi/yucedal%20behzat.pdf?kent1279290984>