Dret penal i societat de la informació

Óscar Morales García (epígrafs de l'1 al 6)
María Rosa Fernández Palma (epígraf 7)

PID_00162529

Universitat Oberta de Catalunya
www.uoc.edu

Índex

Introducció

L'emergència del fenomen tecnològic i la seva generalització –la seva democratització, si es vol– ha oscil·lat entre la llibertat com a màxima en els moments inicials i l'intervencionisme actual, quan la tècnica revela possibilitats de control institucional més que suggeridores. Certament, la denominada *societat de la informació* que neix a l'empara de les tecnologies –no solament de caràcter telemàtic, sinó també d'un altre tipus, com el cable o la televisió digital– transforma les relacions socials i jurídiques d'una manera incontestable i impressionant: el correu electrònic, el teletreball, el comerç electrònic, el vot electrònic, són algunes de les modalitats de relació social, impensables quinze anys enrere i avui part essencial del desenvolupament social i econòmic.

L'evolució i expansió de les tecnologies de la comunicació i la informació repercuteixen en un increment de la qualitat de vida. Però, alhora, les possibilitats enormes de benestar que la tecnologia ofereix obren la porta a noves manifestacions del delicte, en una simbiosi en la qual tot avantatge comporta, com a contrapartida, un preu més o menys elevat. I així, el risc d'intercepció de les comunicacions és més alt com més avançats i senzills siguin els programes que ho permeten: la utilització de targetes de crèdit falsificades o, senzillament, capturades a la Xarxa; la difusió incontrolada d'obres sotmeses a propietat intel·lectual; el sabotatge d'aparells informàtics bàsics per a la feina quotidiana; la falsificació de documents electrònics i un llarg etcètera que de vegades pot aparentar ser fins i tot més important que els avantatges que ofereix.

La resposta jurídica i també juridicopenal que s'hagi d'oposar davant els comportaments més greus requereix una anàlisi de l'abast vertader dels canvis que provoca l'evolució tecnològica i efectuar prognosis ponderades sobre els que vindran i els riscos que comportaran, com a punt de partida en la fixació d'interessos fonamentals en el nou marc de relació. Només així es poden aventurar conclusions sobre la necessitat d'intervenció del dret penal en un sector emergent i d'aparença caòtica, en el qual encara no han penetrat amb decisió els instruments primaris de regulació: administratiu, civil, mercantil, etcètera. I només així sabrem fins a quin punt les normes penals existents són suficients o reclamen la modificació tan urgent i demanada de les tecnologies existents i la seva adaptació. A continuació, desenvoluparem alguns dels problemes fonamentals que les tecnologies de la informació i la comunicació, especialment Internet, plantegen amb relació al dret penal.

Objectius

L'estudi dels materials següents us permetrà conèixer quins són els principals delictes associats al desenvolupament de la societat de la informació i a les seves manifestacions, com ara el teletreball o el comerç i el correu electrònics.

1. Delimitació conceptual i context normatiu

La intervenció del dret penal en el sector de les comunicacions i, especialment, en els processos de transmissió de dades, precisament en funció dels interrogants anteriorment oberts, pateix d'una inèrcia expansiva, fruit de l'escassa reflexió política i jurídica sobre l'ús de les noves tecnologies.

Davant la situació inicial d'anomia i llibertat autocontrolada, posteriorment s'ha generat la imatge de la informàtica com a font permanent de perill, el control del qual només pot ser assumit des de la intervenció de les institucions democràtiques. Tot i ser certa la segona premissa –quant a la idea que les bases del funcionament social han de ser objecte de reflexió política i de l'acció legislativa–, la primera ha de ser matisada. La noció de *risc* sempre és inherent a l'interès que s'intenta salvaguardar o, com s'ha dit, a "una ponderació dels costos i beneficis de la realització d'una conducta" (Silva Sánchez). I, en conseqüència, només una vegada definit l'interès, es pot delimitar el nivell de riscos que pot suportar i es poden delimitar els riscos la perillositat dels quals requereixen tècniques d'intervenció jurídica, no sempre, ni necessàriament, de caràcter penal.

La reflexió en aquest àmbit és, en canvi, inversa, i no mancaria de fonament afirmar que la capacitat de control colossal dels mitjans informàtics, el denominat *poder informàtic*, avui més ampli que en l'accepció original, es troba darrere de les propostes internacionals d'harmonització, que es presenten com a instruments necessaris de control de riscos i de prevenció del delicte informàtic, i sacrifiquen un ampli elenc de garanties; garanties que són formals, materials, generades per analogia o, simplement, que es basen en els usos que la comunitat d'usuaris conforma amb la pràctica diària.

1.1. Delimitació conceptual

El raonament anterior ens situa davant de l'objecte d'anàlisi. I el primer problema de la denominada *criminalitat informàtica* es planteja ja en la mateixa incertesa de la seva definició, una qüestió que ha de ser solucionada per a delimitar l'àmbit d'estudi. Conductes d'una capacitat lesiva extraordinària sobre béns jurídics de primer ordre, com la intimitat, la seguretat col·lectiva o el patrimoni, són estudiades en el mateix marc –la criminalitat informàtica– que d'altres amb un potencial lesiu i un àmbit d'incidència que no és tan evident. D'altra banda, conductes en les quals els mitjans informàtics exerceixen un rol decisiu queden emparentades sistemàticament amb altres en les quals la presència de tecnologies de la informació o de la comunicació és purament accessòria.

Tanmateix, cal sistematitzar les conductes que responen a un mateix patró de risc o, si escau, de lesivitat. I precisament perquè aquest és un sector de criminalitat encara no definit, és preferible partir d'una concepció laxa de *crim informàtic* per a, posteriorment, un cop analitzats cada àmbit d'incidència i la manera com es manifesta la conducta lesiva, delimitar el concepte.

Per *delinqüència informàtica* es pot entendre, llavors, d'acord amb la definició oferta per l'Organització per a la Cooperació i el Desenvolupament Econòmics (OCDE) i més endavant assumida pels principals estudiosos de la matèria (cf. Sieber), "qualsevol comportament il·legal, al marge de l'ètica o fet sense autorització en el marc del procés o de la transmissió de dades".

El que volem dir és que el fenomen de la delinqüència associada als processos de transferència de dades ha de ser abordat d'una manera global, atesa la seva especificitat i complexitat, amb independència que, per raons d'ordre sistemàtic (vinculades a la teoria del bé jurídic) i/o materials (la manca, com succeeix en altres països, de penes directament encaminades a pal·liar la continuïtat delictiva), la seva ubicació en un codi penal no hagi de ser inseparable. En general, la ubicació selectiva d'aquest tipus de preceptes respon a la necessitat d'assegurar la punició de clàssics il·lícits que ara es poden cometre fàcilment mitjançant noves tecnologies però difícilment reconduïbles a la redacció clàssica dels delictes, sota pena d'interpretacions al caire de l'analogia *in malam partem*. Es tracta, doncs, de la determinació de noves modalitats de comissió en delictes de mitjans de comissió determinats o de la implantació de noves figures de resultat en les quals aquest, precisament, està relacionat amb les noves tecnologies. Així les coses, una delimitació de l'àmbit d'estudi com l'assumida en el text presenta l'avantatge de focalitzar l'atenció en els problemes derivats de la societat de la informació i que estan relacionats amb la informació en si mateixa, i n'exclouen els supòsits, mancats d'interès jurídic, en els quals la tecnologia simplement constitueix un més dels mitjans de comissió de realització del fet o el suport afectat amb el resultat material del delicte.

Entre els sectors exclosos del concepte de *delinqüència informàtica* o *cibercriminalitat*, sens dubte, continua el denominat *ciberterrorisme*, que s'entén com el conjunt de conductes que, mitjançant l'ús de la tecnologia i, també de les xarxes telemàtiques, lesiona o posa en perill col·lectivament o d'una manera individual però selectiva, béns jurídics fonamentals. En definitiva, atemptats generalment terroristes, és a dir, guiats per una finalitat ideològica que es pretén imposar violentament, la qual cosa no descarta els atacs purament individuals.

Exemples de ciberterrorisme

Entre els exemples es poden destacar, seguint ara Collin, l'accés remot a una cadena de producció i manufactura de productes cereals inserint ordres en el procés que modifiquin la composició, per exemple, dels nivells de ferro, fins a nivells mortals per als nens; la col·locació de múltiples bombes simultàniament en una mateixa ciutat l'activació de les quals s'efectua d'una manera consecutiva en funció de la transmissió de patrons numèrics, de manera que si la primera bomba deixa de transmetre esclata i n'activa la segona, etc.; l'alteració de les rutes aèries o la manipulació dels controladors aeris, amb la qual cosa es causen accidents múltiples, i l'alteració dels components químics de productes farmacèutics en les cadenes de fabricació, entre d'altres.

Totes aquestes conductes no tindrien interès, com a agressions contra la vida o la integritat física, i ens interessen únicament amb la finalitat d'aquest estudi la dinàmica de comissió considerada aïlladament, és a dir, la rellevància autònoma dels accessos il·legals a sistemes informàtics, les intromissions il·legítimes, els possibles danys en sistemes informàtics, etc., però no el fet principal. Sense que això prejutgi, en aquest moment, la necessitat de legislar per a sancionar penalment de manera autònoma les accions descrites. Precisament, aquest és l'objecte del debat: l'anàlisi del desvalor autèntic que incorporen la determinació de si aquest desvalor ja està considerat en la figura de resultat corresponent o constitueix un plus que reclama l'atenció del dret penal.

1.2. Context normatiu

En la lògica descrita fins al moment, s'han de diferenciar dos àmbits d'actuació normativa.

La seguretat en les xarxes de comunicació i la lluita contra els delictes més greus que es puguin cometre en els processos de transferència de dades, sens dubte s'han de considerar des de la reflexió internacional. En aquest sentit, neix el que fins al moment és el projecte legislatiu més ambiciós en matèria de delinqüència associada a l'ús de les tecnologies de la informació i la comunicació, això és, la Convenció del Consell d'Europa sobre cibercrim, firmada a Budapest el 23 de novembre de 2001.

Juntament amb aquest instrument internacional, la Unió Europea també s'ha dotat de mitjans jurídics per obligar els estats membres a l'adopció de mesures de caràcter penal que puguin fer front al fenomen, segurament creixent, de la delinqüència en els processos de transmissió de dades, en particular amb relació a la difusió de pornografia infantil i als accessos il·legals i pertorbació del funcionament de sistemes informàtics.

Però, a més, la reflexió normativa internacional ha de ser implantada als diversos països membres tant del Consell d'Europa com de la Unió Europea. A Espanya, l'any 2003 va ser un any de reformes penals que, en el context tecnològic, no han estat acompanyades d'un projecte producte del debat previ.

1.2.1. Accions internacionals

a) La Convenció del Consell d'Europa de 23 de novembre de 2001

La Convenció de Budapest, sens dubte, té un abast singular. La seguretat a les xarxes de comunicacions no obtindrà una resposta institucional raonable si no s'aborda en tota la seva complexitat. No n'hi ha prou de sol·licitar la implantació de mesures penals substantives, sinó que cal coordinar les polítiques processals nacionals, en què, sens dubte, hi haurà afectació de drets fonamentals, i, sobretot, la cooperació policial i jurisdiccional. Per això s'ha de destacar, en l'actiu del Consell d'Europa, la decisió de treballar sobre una convenció i no tant sobre una recomanació, atesa la necessitat d'harmonitzar la legislació dels diversos països que pertanyen al Consell d'Europa, no sols en matèria penal substantiva, sinó també en l'àmbit processal i en la col·laboració administrativa i jurisdiccional internacional, això és, coordinació de l'acció policial, recollida de dades en la investigació criminal, etcètera.

El recurs a una convenció permet ampliar satisfactòriament l'elenc de matèries objecte de negociació pels països que hi intervenen i segur que en sacrificarà, en conseqüència, la profunditat, però almenys permet la discussió internacional sobre les necessitats preventives generals en aquest sector i l'equilibri imprescindible de garanties tant a l'hora de legislar com de perseguir el delicte una vegada sigui dret positiu.

La decisió, en canvi, d'obrir no solament a la firma, sinó també a la participació activa en l'elaboració de la proposta, a països aliens al Consell d'Europa, sens dubte ha condicionat part de l'estructura i del contingut de l'articulat, tant respecte del que hi apareix com de les seves omissions flagrants, com veurem immediatament.

La idea de treballar globalment sobre un text que abordi tots els problemes de tipus substantius, processals i administratius (policial) llança com a resultat un text clarament dividit.

- **Qüestions substantives**. En la primera part, s'aborden els problemes substantius, començant pels delictes més freqüents: accés il·legal, intercepció de les comunicacions, fraus i falsedats informàtiques, danys i interrupció de serveis i, en matèria de continguts, propietat intel·lectual (*lato sensu*) i difusió de pornografia infantil. La part general de l'ordre substantiu tanca el capítol amb disposicions que abracen la responsabilitat directa de les persones jurídiques i traça, d'una manera barroera, un esbós de la temptativa i participació.

  Sens dubte, són múltiples les qüestions que es poden abordar aquí, des de la mateixa divisió sistemàtica fins al contingut dels preceptes, l'anàlisi detallada dels quals excedeix amb escreix l'objectiu d'aquest treball, és a dir, donar compte de les posicions nacionals i internacionals entorn dels dèficits de seguretat a la Xarxa i les necessitats (o no) d'intervenció penal.

El cert és que el projecte vira radicalment des de les seves primeres formulacions com a tal fins al text definitiu. No s'hi inclouen disposicions en matèria de protecció de dades de caràcter personal ni sobre apologia del racisme o la xenofòbia, aquestes últimes objecte d'un protocol addicional obert a la firma el 28 de gener de 2003.

En matèria de propietat intel·lectual, la proposta original del Consell d'Europa va consistir a fer taula rasa: els estats membres haurien de tutelar penalment totes les infraccions de propietat intel·lectual derivades de les obligacions assumides en l'Acta de París, la Convenció de Berna i els tractats de l'Organització Mundial de la Propietat Intel·lectual (OMPI) ratificats pels països signants, pretensió mancada de qualsevol reflexió politicocriminal que, encara que es manté en la redacció definitiva de la Convenció, permet als estats l'establiment d'una reserva, sempre que es garanteixi una tutela satisfactòria amb altres mitjans jurídics.

Tampoc la *vis expansiva* del dret penal no va ser absent en la proposta d'incriminació de conductes relacionades amb la pornografia infantil. L'increment de la difusió de pornografia infantil a les xarxes telemàtiques va ser, en efecte, l'excusa per a la moralització de les tendències sexuals en ocasió del fenomen Internet, i va estendre el concepte de *pornografia* i el del seu atribut, *infantil*, fins a estadis completament allunyats de la llibertat o la indemnitat sexual difusa i pròxims a concepcions plenes de càrrega moral sobre les tendències sexuals, de manera que es va assolir la criminalització de la possessió per al consum personal o la difusió de pornografia pseudoinfantil. La versió definitiva de la Convenció (art. 9) permet la formulació de reserva sobre la tipificació de l'autoconsum, la qual cosa en tot cas ha de permetre establir límits en la distància entre la lesió d'un bé jurídic mereixedor de tutela i el fet penalment rellevant.

- **Qüestions processals**. El debat intern al si del comitè d'experts encarregat del desenvolupament de la Convenció va haver de ser formidable, en vista de l'evolució que s'observa. Es passa, en efecte, d'un intervencionisme excessiu en la lluita contra la delinqüència informàtica que ataca els drets i les llibertats dels sospitosos, però en general també dels usuaris, a una lògica de garanties.

  En efecte, en les primeres versions es va plantejar com a necessària, en la tensió eterna entre *llibertat* i *seguretat*, la cessió a les autoritats administratives de parcel·les d'autogovern en l'ús de les tecnologies, com l'accés no autoritzat a màquines, amb la finalitat única de la investigació criminal, sense concessions, als aspectes essencials de preservació de la informació. Així mateix, es preveia una obligació dels prestadors de serveis de la societat de la informació, de registrar l'activitat dels usuaris i emmagatzemar les dades resultants, amb el risc consegüent per a la intimitat i les dades personals dels usuaris i per al funcionament normal de les xarxes telemàtiques. El canvi, que més endavant queda almenys parcialment explicat per les posicions adoptades davant d'això per la mateixa Unió Europea (UE), es tradueix en una màxima d'actuació. Els estats membres del Consell d'Europa han d'adoptar les mesures legals necessàries per a garantir l'existència de

mitjans útils i adequats en la persecució del delicte, d'acord amb el principi de proporcionalitat i, en qualsevol cas, amb els nivells interns de garanties que cada legislació processal nacional pugui preveure.

Recomanacions de regulació del Consell d'Europa

Per tant, l'aspiració del Consell s'acabarà conformant amb el que els estats membres regulin: l'accés en temps real a dades de contingut i dades de trànsit; l'emmagatzemament, durant períodes de temps raonables, de dades de trànsit per les operadores; l'emmagatzemament d'aquestes dades per les mateixes companyies, però en temps real; l'exhibició i el lliurament per les operadores de les dades retingudes, tant de trànsit com de la comunicació mateixa, i, finalment, la intervenció directa sobre màquines.

b) Política criminal de la Unió Europea

Fins i tot en els instruments internacionals per a la regulació (penal) dels problemes de seguretat a les xarxes de comunicació o en els processos de transferència de dades, la Unió Europea constitueix una peça clau pel seu poder polític creixent en l'escena mundial que, tanmateix, no ha tingut un paper harmonitzador. Al contrari, es podria dir que la Unió Europea ha entrat tard en el debat, ho ha fet sobre les bases ja establertes per altres organismes supranacionals (com el Consell d'Europa) i sempre de manera parcial. Encara que, com es veurà, no es pot negar el paper eficaç de contrapunt que ha exercit.

El rol de la UE, en efecte, és tardà. És cert que les directives de la UE s'assemblen més a les recomanacions del Consell d'Europa que a una convenció, però res no hauria impedit a la UE desenvolupar una decisió marc global o una directiva àmplia sobre el fenomen de la delinqüència informàtica i tots els aspectes accessoris, com les qüestions processals i policials en joc. La imposició de criteris penals als estats membres de la UE és una cosa que, històricament, no han rebut bé; el caràcter greu de la reacció penal manté una connexió estreta amb el concepte de *sobirania*, la qual cosa dificulta una acceptació clara dels estats de mesures penals àmplies.

LA UE, amb tot, s'incorpora tard i sobre bases ja existents. Això es manifesta en un doble àmbit.

Amb relació als problemes de tipus processal generats per les primeres versions fetes públiques, la UE reacciona per mitjà de dos instruments més de tipus polític que jurídic. D'una banda, quant a la possibilitat d'accés per les autoritats policials d'un tercer país a màquines d'estats membres de la UE, l'Opinió 4/2001 va sintetitzar la seva preocupació sobre la base de la participació en la Convenció de països aliens al Consell d'Europa i, per tant, a la seva tradició jurídica.

Així, mentre els països pertanyents a la Unió Europea van traslladar al seu dret intern les diverses directives emanades del Parlament sobre la tutela de dades personals, i fins i tot els països que pertanyen a l'òrbita del Consell d'Europa

han hagut d'assumir la política inherent a les recomanacions sobre la mateixa matèria, els estats aliens a la UE o al Consell d'Europa no es troben vinculats a aquesta normativa.

I per això, a més a més de la diversitat filosòfica evident en la tutela de dades personals existent entre Europa i els Estats Units, ens trobem amb la possibilitat que cada estat ofereixi a les dades personals obtingudes en un país de la Unió o el Consell en el curs d'una investigació criminal, una tutela jurídica molt inferior a l'exigida en els entorns territorials, de manera que es trenca la pretensió harmonitzadora i es deixa a la legislació domèstica la salvaguarda efectiva dels drets fonamentals. Més endavant veurem com evoluciona a la UE la valoració de les necessitats de control de les dades de les comunicacions.

Des del punt de vista substantiu, la Unió Europea ha desenvolupat dues grans línies de treball.

D'una banda, amb relació als accessos il·legals i la interferència en el funcionament de sistemes, la UE recomana l'harmonització de la legislació penal per mitjà de la Proposta de decisió marc de la Unió Europea, de 19 d'abril de 2002, sobre els atacs dels quals poden ser objecte els sistemes d'informació. La redacció de la Proposta, tanmateix, no podia ser més desafortunada des del punt de vista de les necessitats de tutela. La mateixa justificació de la Proposta parteix de la falta d'estudis i remet a alguns, no citats, que estableixen estadístiques o bé massa antiquades (final de la dècada de 1990), o bé desorbitades en els perjudicis econòmics que reflecteixen. En la part final d'aquest treball veurem en què es tradueixen aquestes propostes.

D'una altra banda, l'aprovació de la Decisió marc 2004/68, de 22 de desembre de 2003, relativa a la lluita contra l'explotació sexual dels nens i la pornografia infantil, assumeix polítiques de màxims en l'obligació que imposa als estats d'adoptar mesures penals en la lluita contra aquest fenomen difícilment justificables des de les bases per a la construcció d'un dret penal que pivoti entorn de la idea de protecció exclusiva de béns jurídics.

Poc més es pot dir de la UE en aquesta matèria, llevat de les normes dictades fins ara amb relació al frau i la corrupció, que poden contenir disposicions específiques en matèria de defraudacions comeses en les xarxes de comunicació. Tanmateix, no es descarta que la preocupació de la UE per la seguretat a les xarxes comenci a canviar i, en conseqüència, es comenci a obrir un període de reflexió. L'aprovació del Reglament CE núm. 460/2004 del Parlament Europeu i del Consell, de 10 de març de 2004, pel qual es crea l'Agència Europea de Seguretat de les Xarxes i de la Informació, apunta en aquesta direcció, tenint en compte les competències que incorpora. Entre aquests, el director executiu ha de nomenar un grup d'experts d'assessorament permanent que, al seu torn, ha de demanar els serveis de comissions *ad hoc* per a l'anàlisi de problemes

concrets. Entre aquests, potser, l'estudi global i conjunt de la resposta politicocriminal que hagi de merèixer (o no) la delinqüència associada a processos tecnològics.

c) La situació a Espanya

L'aprovació del Codi penal de 1995 (CP 1995) va anunciar una mena de sensibilitat del legislador sobre aquesta matèria, en incorporar alguns tipus penals plens d'elements tecnològics. Una anàlisi sistemàtica del text aprovat llavors revela, en canvi, la falta d'un estudi global del problema i, en conseqüència, la falta de solucions concordes amb els reptes plantejats. No es vol dir amb això que els codis penals hagin de recollir (com succeeix, per exemple, a Portugal) delictes tecnològics agrupats en un mateix títol sobre el factor comú de la tecnologia o els processos de transferència de dades, tal com hem exposat al principi d'aquest treball. Però sí que s'hauria d'haver abordat de manera global el problema per a oferir així solucions –al lloc sistemàtic que li correspongui– a la multiplicitat de problemes que es plantegen.

Bona prova de la falta de perspectiva del legislador espanyol és l'abast de la reforma duta a terme per la Llei orgànica (LO) 15/2003, de 25 de novembre. El Codi penal, en la redacció original de 1995, no tenia unitat sistemàtica en la matèria, i recollia diverses infraccions relacionades amb l'ús de la tecnologia al lloc en el qual l'acció o el resultat típics n'aconsellen la plasmació normativa.

Així succeïa amb la inclusió, en el capítol de les defraudacions, d'una modalitat d'estafa informàtica específica i, posteriorment, de la utilització il·legítima d'equips terminals de comunicació; amb la definició legal de *clau falsa* en el capítol relatiu als robatoris, en el qual s'inclouen les targetes, magnètiques o perforades, i els comandaments o instruments d'obertura a distància; amb el concepte penal nou de *document* contingut en l'article 26 CP, en el qual s'efectua una referència àmplia a tot suport material, en el qual no hi hauria d'haver problemes per a subsumir el document electrònic; amb la referència, continguda en el segon paràgraf de l'article 270 CP, als mitjans capaços de facilitar la supressió no autoritzada o la neutralització de dispositius tècnics que s'hagin utilitzat per a protegir programes d'ordinador, i amb la clàusula de l'article 197.1 CP i, per remissió, també a l'article 278 CP, relativa a la intercepció de comunicacions (telemàtiques) i missatges de correu electrònic.

Malgrat la sensibilització advertida, no tant l'evolució tecnològica, com la falta de perspectiva sistemàtica de la delinqüència associada a processos de transferència de dades, van revelar aviat les dificultats per a oferir resposta a problemes que ja ho eren llavors i que, vagi per davant, la reforma de 2003 i les que s'han succeït després ni tan sols han considerat.

2. Delictes contra la intimitat. Intercepció i accés a sistemes informàtics

Tant la Convenció del Consell d'Europa com la Proposta de decisió marc de la UE sobre els atacs de què són objecte els sistemes d'informació advoquen per la creació d'un delicte d'accés il·legal nu de qualsevol circumstància objectiva o subjectiva que qualifiqui el mer accés no consentit a sistemes informàtics.

L'article 2 de la Convenció estableix el següent:

> *"Accés il·legal*. Els estats part han d'adoptar les mesures legislatives o d'un altre gènere que siguin necessàries per a establir com a infracció criminal l'accés intencional sense autorització a la totalitat o a una part d'un sistema informàtic. Els estats poden requerir que el fet hagi estat comès *infringint mesures de seguretat* o *amb la finalitat d'obtenir dades o una altra finalitat deshonesta* o, amb relació als sistemes informàtics, que es trobin connectats a altres sistemes informàtics".

Proposta de decisió marc de la UE sobre els atacs de què són objecte els sistemes d'informació

La Proposta de decisió marc proposa la tipificació de l'accés il·legal de manera que permeti als estats membres limitar-ne l'abast mitjançant la referència a la vulneració de mesures especials de seguretat, finalitats deshonestes en la conducta de l'autor o la pretensió de causar un dany a una persona física o jurídica. En el cas de la Proposta de decisió marc, la redacció no podia ser més desafortunada: és evident que la referència a les persones jurídiques impedeix relacionar el dany a què es refereix el subtipus amb la integritat física; després, el dany passa a ser eminentment patrimonial i, en aquest cas, el subtipus és una manera d'avançar la intervenció penal respecte a les infraccions patrimonials, i eleva la temptativa de danys a consumació. Sobre això, vegeu *infra*.

Això sí, en ambdós textos es deixa a la millor interpretació dels estats l'oportunitat de limitar la figura delictiva mitjançant la introducció d'aquests elements, i a la fi hi ha entre elles meres diferències de llenguatge (de tècnica jurídica, en realitat) sobre quins poden ser aquests elements de restricció de l'abast del que es prohibeix. El Codi penal espanyol circumscriu la punició de l'accés il·legal als casos en els quals l'accés no consentit es dugui a terme amb la finalitat de vulnerar la intimitat o descobrir els secrets d'un altre; secrets que, en cas que tinguessin naturalesa empresarial, s'han de remetre al que disposa l'article 278 CP.

En definitiva, el legislador va prendre l'opció, en un moment determinat, de restringir l'abast de l'accés il·legal a sistemes informàtics mitjançant la introducció d'un element subjectiu de l'injust que determina una estructura singular de la norma, com a delicte de resultat tallat. Això és, es tractava d'un delicte amb una doble finalitat: d'una banda, és necessari que el frau de l'autor inclogui la voluntat d'accedir al sistema informàtic; de l'altra, tanmateix, aquesta voluntat d'accés requereix una voluntat ulterior, que és la de vulnerar la intimitat o els secrets aliens, voluntat aquesta que, si bé es pot materialitzar en un resultat concret (el descobriment efectiu de secrets o la vulneració de la intimitat), no cal que així succeeixi per a entendre perfeccionat el tipus, i per

això es denomina l'estructura del delicte com de *resultat tallat*, ja que aquest segon resultat, que consisteix en el descobriment o la vulneració, no cal que s'assoleixi, i n'hi ha prou que inspiri la realització del fet base (l'accés no consentit).

I aquesta era, fins a la publicació de la reforma del Codi penal operada per la LO 5/2010, de 22 de juny, l'única norma sobre accessos il·lícits a dades o a sistemes informàtics. La creació de normes penals amb finalitats transcendents, de resultat tallat, com succeeix amb l'article 197.1, segon incís, en el qual es condiciona la punició de la intercepció de les comunicacions (o a l'article 197.2 CP, de la intercepció de dades) a la finalitat de conèixer la intimitat o els secrets, només pot pertorbar l'aplicació ordinària del tipus, de manera que la prova d'aquesta finalitat successiva (que, com ja s'ha avançat, ni tan sols s'ha de fer en un resultat, sinó simplement no inspirar la conducta principal d'accés o intercepció) era poc menys que impossible, i continua en la impunitat la majoria d'accessos il·legals.

En aquest context, la presència d'una finalitat nuclear en l'autor diferent de l'exigida en el tipus (vulneració de la intimitat o descobriment de secrets) podria arribar a excloure de l'àmbit del que és punible conductes el grau de desvalor i capacitat lesiva de la intimitat de les quals es diferencien poc o gens d'aquells supòsits en els quals l'autor busca conscientment aquesta finalitat. I, ja que aquesta no ha de ser assolida per a la perfecció del tipus, senzillament no se'n justificaria l'exclusió de l'àmbit de l'article 197.1 CP. Penseu en la fiscalització de les comunicacions en l'àmbit laboral, emparat en principi pel desig de control del lloc de treball per al qual l'empresari pot estar legitimat (*in extenso*, Morales García), o en l'accés efectuat per un subjecte amb un grau de coneixements tècnics que el fa conscient de la probabilitat enorme de conèixer la intimitat de l'usuari al sistema del qual accedeix.

Ara bé, atesa l'estructura especial d'aquest tipus de preceptes, el nivell d'exigència del *frau específic* podia resultar alleugerit, i amb això s'obria el debat sobre si el frau específic de descobriment de secrets és més intens que el dol del fet base (accés) i, conseqüentment, incompatible amb la concurrència de fets coneguts però no volguts; o, al contrari, la intensitat de l'element subjectiu pot ser mesurada amb paràmetres idèntics als del fet base i, en conseqüència, compatible amb el pur coneixement de l'alta probabilitat que el risc generat s'arribi a materialitzar en un resultat (fora d'això, aquí no exigit per a l'element subjectiu) o amb el dol de conseqüències necessàries. Aquesta segona opció, que relaxa les insuficiències del tipus i de funció excessivament selectiva del dol afegit al dol, situa l'anàlisi de l'element subjectiu en un pla elevat de normativització, és a dir, en termes de dol de conseqüències necessàries o de dol eventual com a representació nuclear del dol (d'especial interès, Picotti, Stratenwerth).

Així, continuant amb l'exemple, un accés permanent i sense el seu consentiment al sistema del treballador al marge de les exigències establertes pel Tribunal Constitucional comporta el coneixement de la probabilitat elevada (generalment al caire de la certesa) o fins i tot la conseqüència necessària, que en aquesta activitat també siguin descoberts la intimitat o els secrets (ara, evidentment, entesos com aquells aliens a l'empresa), cosa que equival a la realització no sols del fet principal –l'accés–, sinó també de l'acte mutilat: el coneixement que amb la seva conducta són (o poden ser) coneguts o descoberts els secrets aliens, i amb això se'n manté la rellevància penal. Consegüentment, la finalitat de l'acció no pot romandre impermeable a objectes de coneixement, que, no obstant això, no han estat directament perseguits; amb això, es determina una tutela de la intimitat més concorde amb el seu contingut constitucional, que no cediria pel pur fet que el coneixement efectiu de la intimitat (no ho oblideu, per mitjà d'una intercepció del contingut de les telecomunicacions, la presència de les quals no es discuteix) o la probabilitat elevada del seu descobriment a partir del fet base no constitueixin la finalitat última en termes volitius o es trobin entre els motius adduïts per l'autor per a la realització de la seva conducta.

Fins a la reforma, doncs, aquesta era l'unica via possible per a concloure que la tutela que dispensa l'estructura de l'article 197.1 CP inclou els supòsits en els quals realment hi havia un risc per a la intimitat o els secrets d'un altre. El legislador, no obstant això, ha posat punt final a les tensions ocasionals de legalitat, i ha redefinit els termes en què la lesió del bé jurídic intimitat es pot portar a terme mitjançant la introducció d'un nou article 197.3 CP descarregat de finalitats en línia amb la Unió Europea i el Consell d'Europa.

El nou article 197 estableix el següent:

> "El qui per qualsevol mitjà o procediment, i vulnerant les mesures de seguretat establertes per a impedir-ho, accedeixi sense autorització a dades o programes informàtics continguts en un sistema informàtic o en part d'aquest o es mantingui a dins d'aquest en contra de la voluntat de qui tingui el legítim dret a excloure'l, ha de ser castigat amb pena de presó de sis mesos a dos anys."

Certament, en matèria d'accés il·legal, la decisió politicocriminal de tutelar o no penalment l'intrusisme informàtic sense una altra finalitat és complexa. La vertiginosa evolució del món d'Internet ha eclipsat el romanticisme inherent a aquelles conductes consistents a accedir a sistemes aliens i informar l'administrador dels dèficits de seguretat, suggerint alternatives per a preservar la integritat del sistema enfront de possibles atacs.

Com s'ha vist, la limitació de l'accés il·legal mitjançant finalitats transcendents al frau complica extraordinàriament la sanció penal de conductes amb desvalor elevat, atesa la naturalesa de l'accés o els coneixements especials de l'autor. La punició de l'accés abusiu, orfe de qualsevol altra finalitat per la qual el legislador s'ha decantat ara, no podia ser una alternativa deu anys enrere, ja que hauria significat un ús promocional del dret penal per a l'educació primària dels usuaris, és a dir, per a la creació d'una consciència col·lectiva d'il·licitud

de l'accés. Avui, la dependència de les xarxes i de la informació que allotgem en els nostres espais en xarxa ha consolidat una idea de privacitat que no està només lligada a la intimitat, sinó també al control sobre l'espai propi, com succeeix amb el domicili.

Per això, el primer que ha de quedar clar en la reflexió sobre els criteris de mereixement i punibilitat d'aquestes conductes és el bé jurídic que volem promocionar. Tant des del Consell d'Europa com des de la UE mateixa (per mitjà de la Proposta de decisió marc), s'assumeix com a tal la seguretat, integritat i disponibilitat dels sistemes d'informació i les dades informàtiques. En aquest cas, els delictes d'intercepció, però sobretot d'accés abusiu, constitueixen un avançament de la barrera que separa la intervenció penal d'un altre tipus d'intervencions jurídiques, ja que la integritat dels sistemes és ja objecte de tutela amb els delictes de danys informàtics i interferència de sistemes dels articles 4 i 5 de la Convenció, com veurem a continuació, o el 3 de la Proposta de decisió marc de la UE. De manera que l'accés abusiu, en constituir en un percentatge majoritari el pas previ a la realització d'un delicte de danys informàtics, passaria de ser una temptativa quan el dany no es produeix finalment per causes alienes a la voluntat de l'autor, a erigir-se en una figura autònoma de consumació; en definitiva, un delicte de perill. Altres béns jurídics fonamentals, com la protecció de dades o la intimitat, no tindrien cabuda aquí o, si es vol només molt remotament, cedint davant del contingut patrimonial de l'atac i mostrant novament la influència d'ordenaments jurídics aliens a la tradició continental, en els quals la tutela de la intimitat o les dades personals no troben criteris sòlids de mereixement i necessitat de tutela penal.

> L'exposició de motius de la Convenció del Consell d'Europa estableix literalment que: "El delicte d'accés il·legal cobreix els atacs contra la seguretat (per exemple, la confidencialitat, integritat i disponibilitat) de les dades i sistemes informàtics". Així mateix, en els considerants de la Decisió marc de 2005 sobre els atacs als sistemes d'informació, a més de les referències habituals al terrorisme com a fórmula de legitimació, es pot llegir que "s'ha comprovat l'existència d'atacs contra els sistemes d'informació, en particular com a conseqüència de l'amenaça de la delinqüència organitzada, i creix la inquietud davant de la possibilitat d'atacs terroristes contra sistemes d'informació que formen part de les infraestructures vitals dels estats membres. Això posa en perill la realització d'una societat de la informació segura [...]".

Per això, la legitimació d'un delicte d'intrusisme informàtic no lligat a un element subjectiu de l'injust és expressió clara de l'evolució d'aquest tipus de conductes que incorporen ja en la seva descripció objectiva la idea d'atac a un bé jurídic que fins ara requeria referències típiques ulteriors per a ser identificat. En aquest sentit, sembla raonable referir-se a un concepte de *domicili informàtic*, del dret a mantenir els espais d'actuació en xarxa i el seu contingut al marge dels accessos no desitjats, tal com succeeix, *ceteris paribus*, amb el domicili "físic": l'entrada i el manteniment al domicili físic són infraccions penals sobre les quals no se'n pot discutir la relació amb la intimitat, malgrat que el precepte no hi exigeixi referències expresses –com a element subjectiu.

Aquest bé jurídic, que ja vam apuntar com a bé emergent en altres treballs el 2002, és possible individualitzar-lo avui en aquests termes sobre la base de la configuració dels elements típics del delicte. Fins ara, la presència d'elements subjectius de l'injust impedia advertir la rellevància intrínseca que desenvolupa per a la intimitat l'espai informàtic. Aquesta tesi, fora d'això, és acceptada àmpliament en altres països del nostre entorn, com Itàlia, on des de la Sentència 1675/2000 de la Corte di Cassazione, entre d'altres, no hi ha dubte de la rellevància del domicili informàtic com a objecte instrumental de tutela.

En el concepte de *domicili informàtic* s'integren els elements essencials de béns jurídics amb rellevància constitucional, directament lligats a l'ús de la tecnologia (en el cas del dret espanyol, no calen els comentaris en relació amb la ubicació sistemàtica, l'article 18 CE, de la clàusula de tutela davant els perills de la informàtica i la intimitat). Només en aquestes condicions és acceptable un tipus de caràcter més objectivat, en els termes recomanats per la Convenció i la Decisió marc.

En aquest sentit, és significativa la referència al manteniment en el sistema contra la voluntat de qui tingui el legítim dret a excloure'l, element que situa el domicili informàtic en un pla de tutela francament similar a la del domicili físic. La referència a la capacitat d'excloure en qualsevol moment el tercer del sistema, al costat de l'establiment de mesures indicatives del desig de ser com a mínim consultat abans d'accedir sobre la possibilitat de fer-ho, desplacen la connexió amb la intimitat des del mer desig intern (art. 197.1) fins a la descripció objectiva del fet desenvolupat dolosament. En definitiva, l'espai informàtic no el configura una màquina determinada, que tal com succeeix amb el domicili físic po ser fungible (una habitació d'hotel o fins i tot una caravana i, en comparació, una Blackberry o l'ordinador d'un cibercafè), sinó la informació vital que se situa en aquests espais que, per aquesta raó, atesa l'absoluta miscel·lània d'elements privats, públics, confidencials, íntims, reservats, compartibles, etc., determina la reserva de l'espai en termes de dret a la intimitat. És, en definitiva, una reacció legislativa davant la convicció del ciutadà de vidre que semblava que imposava la Xarxa; una reacció que cedeix a l'usuari l'opció de compartir informació a les xarxes socials mentre decideix mantenir les portes del seu domicili informàtic tancades a la intromissió de tercers, sense confondre la possibilitat de cedir parcel·les d'intimitat en xarxa amb el dret d'accedir a qualsevol dada, programa o sistema aliè.

El precepte exigeix ara la vulneració de mesures de seguretat establertes pel titular del sistema per a atorgar rellevància típica al fet. El cert és que aquesta fórmula, propiciada pel Conveni i la Decisió marc, ha estat acollida també en altres països del nostre entorn com Itàlia (art. 615 *ter*). Es pot discutir sobre el tipus de mesures de seguretat que han de ser objecte de vulneració i que depen, lògicament, en cada moment, de l'estat de la tècnica, però aquest criteri de selecció de conductes és decisiu en la identificació del bé jurídic. Certament, cada subjecte pot determinar en cada cas sota quines circumstàncies manté els seus espais informàtics. La idea d'una porta tancada que només pot ser oberta per aquells que posseeixen legítimament la clau recorda sens dubte la manera com s'organitza el domicili físic. Les mesures de seguretat són la manera com el subjecte passiu del delicte estableix la vinculació de les seves dades o

programes amb esferes de reserva –*lato sensu*. El criteri de les mesures de seguretat permet seleccionar, doncs, els atacs més directament lligats amb el bé jurídic objecte de tutela, que per mitjà del domicili informàtic acaba essent la intimitat. S'ha d'insistir, això sí, que el nivell de seguretat, que òbviament no pot ser objecte de descripció típica, s'ha de vincular a l'estat de la tècnica en cada moment i als usos o costums de la comunitat. No seria acceptable consagrar l'eficàcia juridicopenal de l'autoposada en perill per mitjà d'una referència vinculant a l'existència de mesures de seguretat –normalment tecnològiques– més enllà del que és raonable per a un usuari mitjà.

3. Infraccions patrimonials en el comerç electrònic

Tal com succeeix en l'àmbit de la contractació tradicional, el negoci electrònic presenta oportunitats de desenvolupament econòmic, però és també una parcel·la sobra la qual es poden projectar conductes d'un grau elevat de desvalor, amb capacitat per a lesionar béns jurídics de transcendència especial de les parts.

Si la contractació electrònica ha de ser regulada per normes de caràcter mercantil, civil i fins i tot, per a determinades qüestions, per normes administratives, el dret penal ha d'entrar, llavors, en els conflictes més greus, en els casos en què les eines primàries d'intervenció manquin de força suficient, o bé per a evitar, o bé per a sancionar, les conductes més greus que puguin posar en perill no sols béns jurídics individuals de transcendència especial (com el patrimoni, la intimitat o el tràfic jurídic), sinó el comerç electrònic en si mateix.

I, de la mateixa manera que en el comerç tradicional els principals focus de perill estan perfectament delimitats, en el comerç electrònic aquests són idèntics encara que el fenomen tecnològic i la distància (entesa sobre manera com a mercat global) aportin un suplement de complexitat que requerirà matisos.

Amb relació al fenomen tecnològic, en efecte, és especialment important observar si les normes penals que tutelen el mercat ordinari són hàbils per a subsumir conductes que puguin afectar el comerç electrònic o, al contrari, la seva utilització en termes idèntics podria comportar una extensió analògica, per definició prohibida en l'àmbit del *ius puniendi*.

Pel que fa a la característica bàsica del comerç electrònic, el seu caràcter globalitzat i a distància, caldrà estar atents a l'estat de la legislació penal amb caràcter general. De res no serviria una legislació avançada penal al nostre país si la resta de la comunitat internacional no estigués en una lògica si més no semblant, ja que això podria contribuir a la generació de paradisos defraudadors.

3.1. Introducció. Les defraudacions en la Convenció del Consell d'Europa i a la UE

La Convenció del Consell d'Europa no encerta del tot amb la regulació de les defraudacions, en una pretensió recurrent de garantir la integritat dels sistemes. Així, la literalitat de la lletra *a* no descriu una estafa en sentit estricte, sinó el que en puritat no és cap altra cosa que un delicte de danys: causar un perjudici a un altre per mitjà del deteriorament o la cancel·lació, etcètera, de dades informàtiques.

D'altra banda, el segon paràgraf, que conté una conducta fraudulenta –satisfeta amb el nostre article 248.2 CP–, tot i així, no ofereix una resposta clara a la utilització abusiva de targetes o a la manera com calgui harmonitzar penalment l'elenc de conductes que convergeixen en aquest problema –ús en terminals punt de venda (TPV), caixers automàtics amb número secret, en dispositius automàtics sense número, etc.– i tot això fins i tot sense adoptar un concepte ampli de *delinqüència informàtica*, referit a "qualsevol conducta il·lícita feta en els processos de transferència de dades", ja que el precepte tan sols obliga a sancionar penalment els casos en els quals s'ha produït una interferència rellevant en el sistema, de manera que el risc penalment rellevant al qual imputar el perjudici patrimonial ha d'actuar directament sobre les dades o el sistema informàtic, de manera que aconsegueixi una actuació diferent del sistema o una d'igual però amb canvis accessoris –d'identitat, quantitat, destinació, etc.

Més preocupació ha desenvolupat la Unió Europea fins al moment. En efecte, la Decisió marc 2001/413/JAI, del Consell, sobre la lluita contra el frau i la falsificació de mitjans de pagament diferents de l'efectiu, ordena normativament les diferents situacions lesives que es poden produir amb relació als mitjans de pagament, d'una banda, i a l'ús fraudulent de tecnologies de la informació, de l'altra. En el primer sentit, la Decisió marc es refereix tant al robatori i furt de mitjans de pagament, com al seu ús no autoritzat o la seva falsificació. En el segon sentit, a la interferència indeguda en el funcionament d'un sistema o programa informàtic.

En definitiva, en els processos de transferència de dades es poden produir esdeveniments en els quals, sense que sigui present una defraudació en el sentit clàssic de posada en escena per a la generació d'un engany, tot i així el patrimoni del subjecte passiu del delicte es vegi minvat en benefici de qui interfereix sense autorització el funcionament normal d'un sistema. Caldrà distingir, doncs, les situacions de defraudació pròpies de l'ús de targetes de crèdit o dèbit o altres mecanismes de pagament diferents de l'efectiu, d'aquelles altres en les quals, sense ser presents aquests elements, es poden produir alteracions patrimonials en perjudici d'un altre.

3.2. La regulació penal del comerç electrònic en el dret intern

Ja al nostre país, la configuració tradicional del delicte d'estafa suscitava, anteriorment a l'entrada en vigor del nou Codi penal, un debat interessant sobre l'aptitud del precepte per a l'assumpció de conductes en les quals l'interlocutor del subjecte actiu era una màquina. Bàsicament, l'estat de la qüestió es pot resumir de la manera següent.

D'una banda, un sector doctrinal entenia l'error com a element independent del delicte d'estafa, la missió principal del qual era delimitar l'àmbit de l'engany típicament rellevant i en funció del qual s'havien de mesurar els paràmetres d'imputació objectiva del resultat, per la qual cosa rebutjava l'aplicació de l'antic article 528 Codi penal de 1973 (CP/1973) als casos en els quals l'interlocutor del subjecte actiu era una màquina (Valle). S'entenia que la màquina no pot ser enganyada: pel cap alt, les ordres que s'introdueixen per a aconseguir un resultat beneficiós per a l'actor són exactament les que la màquina és capaç d'entendre i processar.

En l'àmbit europeu, cap altre país com Alemanya no va saber plantejar els problemes de subsumpció de l'estafa clàssica; problemes que eren fàctics, sobre la manera i lloc de realització de la manipulació i que en tot cas reclamarien una solució específica en funció dels respectius casos concrets, i d'abast típic, en general limitats a l'àmbit de l'engany (*Täuschung*) i l'error de la víctima (*Irrtum des Opfers*): és impossible induir a error l'ordinador, ja que, paradoxalment, l'induïm a actuar correctament conforme als paràmetres introduïts en el sistema (Sieber).

Sentències del Tribunal Suprem sobre presumptes delictes d'estafa electrònica

La jurisprudència va adoptar aviat aquesta via, una vegada començava a fer eclosió al final de la dècada de 1980 l'ús de les tecnologies de la informació. La Sentència del Tribunal Suprem (STS) de 19 abril 1991 és, sense cap dubte, el paradigma d'una doctrina fonamentada. S'hi va negar la qualificació com a delicte d'estafa en un supòsit de múltiples anotacions comptables a l'ordinador que van provocar la transferència d'una suma de diners determinada de comptes corrents de clients del banc.

La qualificació final del fet va discórrer pel tipus d'apropiació indeguda per la relació d'administració que unia el subjecte actiu amb els comptes corrents, però no hi hauria d'haver hagut qualificació per estafa ni apropiació indeguda si l'alteració comptable hagués estat feta per un *extraneus* a les tasques d'administració. Amb tot, la tesi jurisprudencial difícilment arriba a les seves últimes conseqüències, de manera que no és difícil concloure que el Tribunal actua mogut per impulsos de justícia material aliens a la descripció típica. I per això el Tribunal Suprem, davant de conductes d'aquest tipus, difícilment es deixa seduir pel cant de sirena del principi de legalitat, i sempre troba algun precepte al qual ajustar el fet.

La Sentència del Tribunal Suprem (STS) de 19 d'abril de 1991 n'és un exponent clar, en la mesura que la vinculació laboral de l'empleat de banca permetia establir un títol amb obligació de devolució i derivar el supòsit cap a l'apropiació indeguda.

Altres vegades, la via per a mantenir incòlume la justícia material davant agressions patrimonials insuficientment tutelades per les normes penals no és tan clara sense agredir simultàniament el principi de legalitat o, si escau, el principi acusatori quan la causa resideix en una qualificació jurídica deficient del fet.

Un exemple d'això, el constitueix la STS de 30 d'octubre de 1998. Resumidament, els fets són els següents: un funcionari públic de l'INEM introdueix les dades de tres coneguts seus en la base de dades de l'ordinador en el qual es contenen els beneficiaris de pensions públiques. El funcionari no té entre les seves funcions el maneig d'aquestes dades. Com a conseqüència de l'alteració, es produeixen transferències reiterades mensuals d'actius patrimonials durant més de dos anys, i es reparteixen les quantitats entre els falsos beneficiaris i el funcionari. L'acusació del Ministeri Fiscal és per delicte de malversació de cabals públics, l'Audiència Provincial castiga per delicte d'estafa conforme a l'antic Codi penal (art. 528 CP/73), malgrat l'heterogeneïtat processal que regna entre ambdós tipus delictius i malgrat la inexistència de prou engany per a produir error.

El Tribunal Suprem cassa la Sentència i condemna el funcionari per delicte de malversació de cabals públics, de manera que equipara incomprensiblement la tinença a càrrec de l'objecte material per raó de les funcions, que reconeix inexistent i impossible de fonamentar com a element típic aïllat del delicte de malversació, i el càrrec de funcionari exercit.

Una altra part important de la doctrina (Gutiérrez Francés) entenia i encara avui entén que l'engany típic no ha de comportar necessàriament un tipus de relació intersubjectiva amb un tercer, la qual cosa s'afegeix a la configuració de l'error com a element dependent de l'engany típic. Des d'aquesta perspectiva, seria possible l'afirmació d'un error a la màquina malgrat que la mateixa hagués complert, precisament, les instruccions introduïdes.

En tot cas, del que no hi ha dubte des de qualsevol de les dues opcions doctrinals és de la possibilitat de subsumir el fet en el delicte d'estafa quan, malgrat l'existència de manipulacions informàtiques, el destinatari de l'engany i qui sofreix l'error és un ésser humà, és a dir, si en algun moment de la cadena d'exigències típiques es produeix una espècie de comunicació intersubjectiva, encara que diferida, entre el subjecte actiu i un tercer sobre el qual es produeix l'error.

Des d'aquest punt de vista, s'entén que la nova estafa informàtica únicament serveix a efectes d'interpretació autèntica dels supòsits que, en tot cas, ja obtenien col·locació en el tipus clàssic del delicte d'estafa, i així se solucionen els problemes de seguretat jurídica que hi pogués haver en la tasca de qualificació. S'ha d'entendre que el delicte d'estafa, abans i després de la reforma, es manté en el curs del que s'ha anomenat *interpretació clàssica* dels seus elements típics. Des d'aquest punt de vista, el nou delicte d'estafa informàtica no solament aclareix problemes de seguretat jurídica. Més encara: soluciona una llacuna de punició i ho fa en marges més o menys amplis.

En primer lloc, el delicte d'estafa informàtica creat pel legislador de 1995 serveix per a la punició de conductes en les quals no hi ha un apoderament real o físic de la quantitat, sinó la mera alteració comptable de l'element patrimonial. Pot ser, en efecte, que el subjecte actiu no tingui mai en poder seu la quantitat econòmicament avaluable, però ara n'hi haurà prou amb l'existència de la transferència no consentida per a afirmar el trasllat patrimonial. Com veurem més endavant, això no soluciona tots els problemes que els diners comptables plantegen en aquest àmbit i ni tan sols garanteix, en algunes concepcions, la tipicitat de conductes el desvalor de resultat de les quals és evident.

En segon lloc, la referència a manipulació informàtica o artifici semblant obre el precepte als avenços tècnics dels quals són un bon exponent sectors de desenvolupament vertiginós com l'informàtic. L'extensió de la manera de comissió, tanmateix, no ha d'induir a error, ja que la seva amplitud queda íntimament vinculada a la capacitat del mitjà per a l'obtenció d'una transferència d'actius no consentida. Amb tot, aquest últim apunt sobre la base del paral·lelisme que es pot exercir amb l'engany i l'error en el tipus clàssic, ha

de mantenir oberts, tanmateix, altres interrogants d'interès amb relació a la imputació objectiva del resultat, especialment en els casos en els quals la transferència no consentida d'actius patrimonials es trobi remotament vinculada a la manipulació o a l'artifici informàtic.

És el cas de la modificació rellevant de dades en el sector borsari, que posteriorment deriva en un increment dels valors del subjecte actiu, que obté així una quantitat notòriament superior a la que hauria obtingut si no hagués manipulat els fitxers –supòsit, per cert, esdevingut a la pràctica. En aquests casos, l'alternativa passa per estendre els criteris de risc de la manipulació amb relació al benefici obtingut o, si es nega aquesta via i la subsumpció en l'estafa informàtica, només resta acudir al delicte de danys (Choclan), però els problemes que planteja aquesta opció no són de menor envergadura i s'allunyen, sens dubte, del nucli d'aquest comentari. En definitiva, amb l'article 248.2 CP s'ha intentat cobrir llacunes punitives i satisfer les exigències de justícia material sense necessitat de recórrer a expedients interpretatius no sempre adequats, com hem vist.

En paral·lel, el CP 1995 també va implicar canvis en la redacció del robatori amb força i, particularment, en l'ampliació del concepte de *clau falsa*, que en la redacció vigent conté "les targetes magnètiques o perforades". No hi ha cap dubte que la pretensió del legislador ha estat enfortir els recursos legals per a una cobertura millor de les possibles hipòtesis de depredació patrimonial en què són presents elements tecnològics, amb dinàmica de comissió defraudadora (art. 248.2 CP, manipulació informàtica o artifici semblant) o sense (art. 237 CP, amb relació a l'art. 239 CP, robatori amb força a les coses mitjançant l'ús de targetes magnètiques com a clau falsa). I tampoc no hi ha cap dubte, en vista de la disputa doctrinal i jurisprudencial sobre l'abast de cadascun d'aquests preceptes amb relació als grups de casos més greus i freqüents, que el resultat no podria haver estat menys satisfactori.

Comentari sobre els buits legals relacionats amb el frau informàtic

Al llarg del mòdul s'efectuen referències al dret penal alemany, que en matèria d'ús il·lícit de targetes de crèdit o dèbit conté una regulació molt més satisfactòria del fenomen. No es comprèn la raó per la qual el legislador penal de 1995 no va tractar integralment d'aquest fenomen i va proposar una regulació harmònica que diferenciés el desvalor divers de cadascun dels grups de casos. Menys encara es pot comprendre que, en el moment actual (2009) i amb una reforma integral en germen del Codi penal, el Projecte no prevegi una solució al problema, com ho feia el Projecte de reforma de 2007, i s'ignorin així els greus conflictes de proporcionalitat que la multiplicitat de tipus genera.

El legislador sembla haver quedat satisfet amb la introducció del tercer paràgraf a l'article 248 CP, que permet sancionar la fabricació, introducció, possessió o facilitació de programes d'ordinador específicament destinats a la comissió de les estafes dels números precedents. Però és obvi que amb el precepte no se solucionen els esculls interpretatius que plantegen els articles 248 i 237 CP (i, més enllà, el 387 CP). La consumació anticipada d'actes preparatoris o la formalització a títol d'autor d'actes de mera participació resolen poc o res. Però és que, a més, l'articulació dels verbs entorn de programes d'ordinador oblida un altre tipus de mecanismes que podrien facilitar la comissió dels delictes anteriors (per exemple, els elements de maquinari que suportin els programes d'ordinador). Sense oblidar que referir la destinació específica als programes, i no a la possessió, fabricació, etcètera, impedeix subsumir en la norma la tecnologia de doble ús, sempre possible i altament freqüent, en el sector informàtic.

3.3. Tractament jurídic penal de les depredacions patrimonials en el comerç electrònic

Examinem en aquest apartat l'ús il·lícit de les targetes de crèdit o dèbit i també el robatori d'identitat.

3.3.1. Ús il·lícit de targetes de crèdit o dèbit

L'ús indegut de mitjans de pagament aliens és una modalitat més de delinqüència informàtica, segons el criteri dibuixat a l'inici d'aquest treball: es tracta d'una conducta jurídica penalment rellevant en la qual es veu afectat un procés de transferència de dades.

L'ús de targetes de crèdit o dèbit alienes està històricament mal resolt al nostre país. Ho estava en el CP de 1973, en el qual ni hi havia delicte d'estafa informàtica, ni el delicte de robatori amb força en les coses incorporava cap referència a les targetes magnètiques. I ho està en el CP de 1995, en el qual hi ha totes dues coses, a més d'una referència a les targetes de crèdit en el delicte de falsificació de moneda que complica encara més la situació.

És possible usar una targeta de crèdit aliena a Internet, només posant les dades de la targeta. És possible usar-la en un caixer sabent els números secrets o sense saber-los. És possible copiar la banda magnètica d'una targeta per a usar-la posteriorment. És possible usar-la en un comerç amb falsedats documentals o sense, però en tot cas enganyant el comerciant. I és possible, finalment, usar-la en un comerç en connivència amb el comerciant. Totes aquestes conductes poden tenir continguts de desvalor diferent, però no podem oblidar que, al cap i a la fi, es tracta d'obtenir el patrimoni d'una targeta aliena sense el consentiment del titular. I és aquest desvalor principal el que ha de ser objecte de retret penal per a no confondre l'accessori amb el principal.

La jurisprudència ha estat vacil·lant entre la qualificació d'aquests supòsits (de vegades d'un mateix supòsit) com a delicte de robatori amb força a les coses o estafa informàtica, i ha generat tensions del principi de legalitat que entren dins de l'analogia prohibida, per exemple, en sostenir que l'ús d'una targeta aliena en un caixer o en un comerç en connivència amb el comerciant és estafa informàtica, ja que fer-se passar davant el terminal per qui realment no som constitueix un artifici semblant a la manipulació informàtica, en termes de l'actual 248.2 CP; o en sostenir que l'ús de la targeta en un caixer és robatori amb força, malgrat que no s'accedeix al lloc en el qual es troben les coses.

L'entrada en vigor del CP 1995 semblava solucionar el problema de l'ús il·lícit de targetes de crèdit o dèbit en les hipòtesis en les quals els delictes d'estafa clàssica i l'estrenada estafa informàtica no poguessin ser aplicables. Però la realitat és sempre superior a la ficció. Si anteriorment a l'entrada en vigor del

nou Codi penal van ser apuntades totes les hipòtesis possibles amb relació a la utilització il·lícita de targetes de crèdit, la situació actual és idèntica però amb més eines i segurament amb supòsits fins ara no previstos.

- S'ha passat, així, de reinterpretar el concepte de *clau falsa* a entendre que el CP 1973 contenia un concepte funcional de *clau* en el qual cabrien les targetes de crèdit o dèbit encara que no fossin esmentades expressament en el tipus penal per descriure en el CP 1995 les targetes magnètiques o perforades, i es descuiden així altres elements tecnològics, com les targetes amb xip però sense banda magnètica o amb banda magnètica inútil als efectes del funcionament de la clau. Si durant la vigència del CP 1973 era plausible una interpretació funcional del concepte de *clau* que inclogués les targetes magnètiques (Romeo; en contra, De la Mata), ja que no hi havia cap referència típica a les targetes, aquesta possibilitat disminueix en el CP 1995, ja que l'article 239 CP incorpora una interpretació autèntica del que s'ha d'entendre per *clau falsa* des del punt de vista tecnològic.

- D'altra banda, l'esment dels mitjans que poguessin funcionar com a clau no defuig altres problemes en la lectura del tipus, com és l'abast de la fórmula "per a accedir *al lloc* on es troben les coses", també posat en qüestió per un sector doctrinal i reinterpretat en clau funcional (com anteriorment ho va haver de ser el concepte de *clau*) per un altre (González Rus).

- La nova redacció dels delictes de robatori i furt, ara menys vinculats típicament ja que el furt no es descriu negativament per absència de força en les coses o violència o intimidació en les persones, no elimina les objeccions d'un sector doctrinal i jurisprudencial sobre l'abast de l'expressió "sense la voluntat del seu amo", exprés en el furt però encara implícit en el robatori amb força.

- En la mateixa línia, la descripció de l'objecte material com a cosa moble i els verbs *prendre* o *apoderar-se* el furt i el robatori amb força, respectivament, mantenen vigents les objeccions sobre la idoneïtat d'ambdós preceptes per a assolir l'apoderament de diners comptables (Orts).

- Finalment –potser de moment–, la manipulació de la banda magnètica de les targetes de crèdit o dèbit constitueix, o almenys així ho va acordar el Ple no jurisdiccional adoptat per la Sala Segona del Tribunal Suprem el 28 de juny de 2002, un delicte de falsedat de moneda recollit en l'article 387 CP amb relació a l'article 386 CP, amb la conseqüent determinació de la competència a l'Audiència Nacional i l'increment del marc penal fins a dotze anys, i això sense comptar amb els problemes concursals que aquesta qualificació origina.

Sobre el concepte de *clau falsa*

En definitiva: si l'alteració de la banda magnètica d'una targeta de crèdit o dèbit és falsificació de moneda; si els delictes de furt i robatori amb força no serveixen per a subsumir les conductes d'ús il·lícit de targetes en TPV i caixers automàtics; si l'estafa clàssica

requereix una relació intersubjectiva i si l'estafa informàtica reclama una manipulació informàtica que sembla que és diferent de l'alteració de la banda magnètica; si aquesta és la panoràmica: amb quins criteris de certesa jurídica operem? Quin delicte es comet en usar una targeta de crèdit en un caixer? I en un TPV amb el coneixement del venedor? I sense el seu coneixement? I en terminals automàtics que no requereixen número secret addicional? I quan s'usa el número de targeta a Internet? I si es falsifiquen algunes o totes les dades d'una banda magnètica? I si la targeta porta un xip incorporat, en lloc de banda magnètica? I si els instruments d'obertura ni tan sols són targeta però no són a distància?

Amb tota probabilitat, el legislador va tractar de resoldre el problema amb la inclusió en el concepte de *clau falsa* de les targetes magnètiques i els mecanismes d'obertura a distància (Bolea i Robles). És cert que la *mens legislatoris* adquireix després sentit propi una vegada plasmada en una norma de dret positiu, i la dicció "per a accedir al lloc" continguda en el delicte de robatori amb força no facilita les coses. Però les alternatives tampoc no són raonables en termes d'estricta legalitat.

Sentència del Tribunal Suprem sobre un cas d'estafa informàtica

La Sentència del Tribunal Suprem de 21 de novembre de 2001 (ponent: Martínez Arrieta), protegida doctrinalment (recentment, Rovira del Canto), va qualificar d'estafa informàtica la mera simulació davant del TPV de ser el titular de la targeta quan això no és així. I aquesta qualificació va operar sobre el concepte d'*artifici semblant* la manipulació informàtica. És clar que l'equivalència a efectes típics entre la suplantació i l'artifici semblant és nul·la (Mata Martín), però en el cas d'interlocutòries calia donar resposta (en termes de justícia material) a un acte de depredació patrimonial que, per principi acusatori, hauria quedat impune. Aquesta equivalència entre *suplantació* i *artifici semblant* constitueix el fonament, com veurem més endavant, per a qualificar els supòsits de pesca bancària (*phishing*) com a delicte d'estafa informàtica.

Finalment, amb relació a l'ús il·lícit de targetes de crèdit, la reserva del delicte de falsificació de moneda per als casos en els quals es falsificava la banda magnètica de la targeta, complica encara més l'escenari. En aquests casos, l'artifici semblant a una manipulació informàtica és clar: no s'opera sobre el sistema, ni sobre les dades, sinó que mitjançant un sistema informàtic extern es permet copiar-ne la banda. No hi havia, tampoc, un desvalor material equivalent entre la creació de moneda falsa (no existent ni autoritzada en el mercat per l'òrgan emissor) i l'aprofitament d'un crèdit o un saldo ja existent en el mercat. Perquè aquesta equivalència en el desvalor material de la conducta fos present, seria necessària una creació *ex novo* del crèdit o el saldo sobre una targeta, i això a la pràctica és, fins al moment actual, gairebé impossible. Se sanciona igual, tanmateix, una conducta de falsedat de moneda que copiar una banda magnètica, amb la remissió de competència consegüent a l'Audiència Nacional i el risc de col·lapse de l'òrgan, tenint en compte la senzillesa amb què la targeta pot ser copiada.

Tot això insistia en la necessitat d'un nou tipus penal que recollís els problemes de l'ús il·lícit o no consentit de targetes alienes. Per això, en un context de dispersió com el descrit, s'ha de saludar positivament la recuperació en el text definitiu de la reforma d'una previsió específica per a l'ús de targetes de crèdit o dèbit en perjudici del titular, ja que efectivament això hauria de contribuir a posar ordre en un panorama certament desolador. El nou article 248 estableix el següent:

1) Cometen estafa els que, amb ànim de lucre, utilitzen prou engany per a produir error en un altre, induint-lo a fer un acte de disposició en perjudici propi o aliè.

2) També es consideren reus d'estafa:

a) Els que, amb ànim de lucre i valent-se d'alguna manipulació informàtica o un giny semblant, aconsegueixin una transferència no consentida de qualsevol actiu patrimonial en perjudici d'un altre.

b) Els que fabriquin, introdueixin, posseeixin o facilitin programes informàtics destinats específicament a la comissió de les estafes previstes en aquest article.

c) Els que, utilitzant targetes de crèdit o dèbit, o xecs de viatge, o les dades que hi figuren en qualsevol d'aquests, facin operacions de qualsevol classe en perjudici del titular o d'un tercer.

Ara bé, la reforma es queda curta i no és clar que, a la fi, la introducció d'un nou precepte no acabi generant més confusió.

En primer lloc, a la introducció del delicte d'ús de targetes de crèdit com a delicte d'estafa no la segueix una modificació dels delictes de robatori amb força a les coses que deixi clara la preferència normativa. De manera que sembla que hi ha un nou precepte que juga a qualificar, i no un nou precepte que aclareixi la qualificació.

En segon lloc, i ja que el legislador no ha afrontat tampoc en la reforma dels delictes d'estafa l'aclariment del règim jurídic penal de la pesca (*phishing*), s'hauria de mantenir la tesi del Tribunal Suprem que usar les claus d'Internet autèntiques davant el terminal és estafa informàtica, la qual cosa buidarà de contingut la nova disposició sobre l'ús de targetes de crèdit.

Finalment, al costat del nou article 248.2c CP el legislador ha previst la mateixa conducta en l'article 399 bis CP, però reservada als casos en els quals les targetes emprades en perjudici del titular són falses i qui les usa no ha participat en la sostracció; la conducta en tots dos casos té un desvalor material idèntic, ja que l'origen d'una targeta a les mans de qui la posseirà després podria ser lícit o il·lícit als efectes del 248.2c; per exemple, s'hi podrien subsumir conductes d'abús de confiança basades en l'engany clàssic de l'estafa sense arribar a serho o la dels qui, després de la sostracció, les aconsegueixen utilitzar o, finalment, la dels qui han comprat un número de targeta encara vigent per mitjà de qualsevol mecanisme tecnològic. Atorgar a aquestes conductes un tractament més benigne que a la de qui utilitza, en lloc de l'original de la targeta, una targeta doblada, manca de sentit llevat que s'estigui pensant en les targetes com a moneda, com succeïa fins ara. És més, en aquest cas, és necessari insistir

que la falsedat de la targeta i l'ús posterior només són capaços de suportar un tractament punitiu tan dispar en casos de creació de nou saldo o crèdit, que al cap i a la fi és el que succeeix quan es posa en circulació diner fals.

3.3.2. Robatori d'identitat

1) La identitat a Internet

L'evolució ràpida –i de vegades atropellada– de la tecnologia afavoreix la generació de tendències en el comportament i, conseqüentment, també la de fórmules criminògenes per a aprofitar-les il·lícitament.

És el cas del rol de la identitat a Internet. Si en la gènesi d'Internet l'anonimat va constituir un poderós estimulant per al seu ús, aquesta tendència va ser posteriorment desplaçada pel valor de la pròpia identitat. Aquest valor es manifesta en un doble sentit: el dret a la utilització de la identitat pròpia a Internet, sense restriccions però sobretot sense suplantacions, i el dret a la reserva en el cas d'identitats fingides, també al marge de la curiositat aliena.

L'eclosió de les xarxes socials (Twitter i Facebook, entre d'altres) i la identificació constant en portals d'accés a serveis en línia (la banca electrònica com a *primus inter pares*) han generat, en definitiva, una revaloració de la identitat (real o fingida) i, al mateix temps, un augment exponencial dels riscos de suplantació i de la suplantació específica.

Exemples de suplantació d'identitat a Internet

Els exemples són variats, però tots tenen com a eix central la identitat d'un tercer: l'ús de les claus d'accés i la signatura electrònica d'un tercer per a accedir als seus comptes bancaris i obtenir així un benefici il·lícit sense el consentiment del titular (pesca, descaminament [*pharming*]); l'ús de les claus d'accés (inici de sessió i contrasenya) a xarxes socials i comptes de correu electrònic (especialment els comptes web gratuïts) amb la finalitat d'extorsionar-ne els titulars, i, en l'àmbit més estret de la joventut i la infantesa, per a aconseguir en línia i fins i tot físicament determinats favors de naturalesa sexual, aprofitant la informació així obtinguda (fenomen conegut com a *ciberassetjament a menors* [*grooming*]).

El debat que arriba del món anglosaxó (fonamentalment, dels Estats Units) es decanta per l'anticipació de la tutela penal i la creació de tipus penals adreçats a la sanció autònoma del robatori d'identitat, de la mera suplantació. Sens dubte, els problemes que veurem a continuació en l'àmbit patrimonial amb la pesca avalarien una solució d'aquest tipus, ja que no és gens fàcil trobar una figura que absorbeixi el desvalor total de la infracció realment comesa.

Ara bé, l'atomització del comportament desenvolupat pel subjecte per a referir cada part del desvalor a un tipus penal diferent podria no ser tampoc una solució adequada. En primer lloc, perquè aquesta atomització requereix punts de referència entre els quals el bé jurídic és essencial. En aquest sentit, s'ha de tenir present que, o bé som davant d'un bé jurídic (vell i alhora) emergent (alguna cosa així com la identitat), i en aquest cas crearíem figures penals tendents a la tutela d'aquest bé davant la seva lesió; o, al contrari, el bé jurídic de referència

es troba en el resultat efectivament produït (la despatrimonialització, el favor sexual obtingut, la contraprestació de l'extorsió, etcètera), i en aquest cas la creació d'un tipus penal específic estarà dibuixant una figura de risc.

Sobre el primer aspecte s'ha tractat de trobar una referència en el delicte clàssic d'usurpació d'estat civil. La jurisprudència ha estat tradicionalment garantista en la interpretació de l'article 401 CP, de manera que la usurpació dels elements integrants de l'estat civil (naixement, filiació, veïnat, etcètera) haurien de ser objecte d'apropiació absoluta i permanent en el temps perquè el tipus penal entrés en joc. És obvi que aquest precepte podria resultar aplicable en determinades hipòtesis de l'entorn tecnològic. Particularment, en aquelles en les quals la usurpació dels elements integrants de l'estat civil és, en efecte, quasi absoluta (penseu en l'apoderament de les claus del Facebook, la seva modificació posterior per a impedir que el titular hi accedeixi i l'ús posterior del perfil real –amb nom, data de naixement, veïnat, etcètera– en l'entorn de xarxa).

Però no ho seria, perquè constitueix una aplicació analògica prohibida, en casos en els quals la identitat en xarxa no és la real, sinó una simulada (concretament, comptes no identificatius de correu electrònic), o en aquells casos en els quals no hi ha utilització de la identitat *stricto sensu*, sinó dels elements que donen accés a la identitat (claus d'accés i signatura electrònica en la pesca). De la mateixa manera, l'article 197 CP continua essent una referència quan el robatori d'identitat té per objecte un entorn íntim o privat (comptes de correu).

La creació amb aquest efecte d'entorns de correu web idèntics als clàssics gratuïts (hotmail, gmail, etcètera) amb la finalitat d'accedir al contingut de la comunicació, tant si el nom d'usuari emula l'anonimat com si reprodueix l'estat civil del titular, ha estat reconeguda als tribunals com a delicte contra la intimitat i de falsedat documental (sentències –fermes– dels jutjats penals núm. 20 de Barcelona de 7 d'octubre de 2009 i núm. 22 de Barcelona de 13 d'abril de 2010).

El debat, doncs, es projecta des de l'àmbit anglosaxó a ordenaments continentals que segueixen una lògica normativa diversa, la qual cosa impedeix traslladar els seus resultats *mutatis mutandis*. Això no obsta, però, per a continuar reflexionant sobre el valor de la identitat real o fingida en xarxa i sobre les necessitats efectives de tutela en vista de l'increment de les agressions externes.

2) Pesca i descaminament: concepte i qualificació jurídica

L'operativa bancària s'ha vist seriosament compromesa des de la posada en funcionament de la denominada *banca en línia*. En efecte, la possibilitat que l'usuari té d'operar sobre els comptes propis per Internet (només similar a la

possibilitat d'operar sobre els propis comptes pel caixer automàtic) ha multiplicat l'ús de la banca en línia i, alhora, ha provocat nous perills en l'operativa mateixa del patrimoni així administrat.

El producte bancari té un atractiu innegable no sols per als inversors, sinó també per als qui se situen al marge de les regles de joc. Des de l'inici de l'activitat bancària, centrada en grans dipòsits de moneda, títols i paper comercial, s'han desenvolupat totes la tècniques imaginables per a aconseguir il·legítimament els actius custodiats per les entitats bancàries: des del robatori violent, particularment amb ús d'armes, passant per tècniques més depurades, com el col·laboracionisme dels empleats de banca o el robatori amb força en qualsevol de les seves manifestacions, fins a arribar a l'estafa, en la qual l'individu desplega un ritual formidable dirigit a enganyar el bancari per obtenir el botí.

Les tecnologies de la informació han obert un model de relació nou entre bancs i clients i, alhora, han estimulat la creació de noves fórmules per a accedir al patrimoni aliè aprofitant el nou model. La posada en circulació de targetes de crèdit i dèbit, sens dubte, va representar una fita en aquest sentit. Les tècniques criminals basades en el plàstic han explotat totes les possibilitats: la falsificació del plàstic mateix, o sols de la identitat associada a la targeta, o la falsificació de la banda magnètica mitjançant el doblegament de targetes, l'ús il·lícit de targetes reals en caixers automàtics o en TPV dels comerços, són només algunes de les tècniques desenvolupades aprofitant la tecnologia emergent en cada moment.

La pesca (*phishing* o pesca de l'incaut) constitueix una barreja de tècniques d'enginyeria social, combinades amb l'ús de tecnologies de la informació que tendeixen a obtenir dels usuaris d'Internet les claus d'accés als productes contractats amb l'entitat bancària, amb la finalitat d'accedir després a aquests serveis i obtenir-ne el benefici il·lícit corresponent.

Normalment, la pesca electrònica incita a les tècniques d'enginyeria social i la tecnologia només és el vehicle necessari per a arribar al nombre de persones més gran possible i, sens dubte, per a accedir posteriorment al producte contractat per l'usuari.

Així, entre les tècniques de pesca més conegudes destaquen els missatges de correu electrònic, en els quals, imitant la capçalera del missatge (és a dir, l'adreça electrònica) d'una entitat bancària i fins i tot imitant determinats símbols propis de la marca de l'entitat, se sol·licita al subjecte que "renovi" les seves claus introduint-les en l'espai creat per a això en el cos d'aquest missatge de correu electrònic. Una vegada enviada la informació a l'atacant, aquest aprofita per a accedir als comptes i, posteriorment, via transferència electrònica, aconseguir la màxima quantitat possible de diners. El punt fonamental de

l'esforç resideix en l'obtenció del que es coneix com a *signatura electrònica*. Si l'accés al producte requereix l'inici d'una sessió i una contrasenya, la signatura electrònica és el tercer element que permet operar amb els productes contractats. L'esforç del pescaire (*phisher*) és aquí màxim, perquè ha de convèncer l'usuari que faciliti una informació (la signatura electrònica) que les entitats bancàries no sol·liciten mai.

També el descaminament constitueix una modalitat amb una perillositat especial amb la qual obtenir les anhelades claus. Si la pesca pivota especialment en l'enginyeria social, el descaminament en desplega la perillositat en incitar sobretot l'element tecnològic.

Bàsicament, el descaminament consisteix en la imitació de la pàgina web de l'entitat bancària (falsejament d'identitat o *web spoofing*). De manera que, una vegada teclejada a la barra d'eines del navegador l'adreça de la pàgina web, on realment s'accedeix és a una còpia gairebé exacta de la pàgina web vertadera que, en lloc de sol·licitar només el nom d'usuari i la clau d'accés (inici de sessió i contrasenya), sol·licita, a més, la signatura electrònica. El sistema funciona fins i tot quan la manera d'accedir-hi és a partir d'enllaços (*linking*) o de favorits.

Són múltiples els sistemes que les entitats financeres poden emprar per a impedir la pesca i múltiples les tècniques que el pescaire inventarà per esquivar els obstacles nous.

Sistemes de les entitats financeres per a impedir la pesca

Algunes entitats van optar pel que es coneix com a *teclats virtuals*, per evitar així que programes maliciosos introduïts normalment mitjançant troians a la màquina de l'usuari copiessin claus emmagatzemades a l'equip o desxifressin les pulsacions del teclat en introduir-les. Aquest sistema, que sens dubte presenta avantatges, plantejava el greu defecte que si el teclat romania quiet a la pantalla, determinats programes informàtics aconseguien desxifrar les pulsacions mitjançant l'estudi del moviment del ratolí. Es van crear llavors els teclats virtuals mòbils, que es van movent per tota la pantalla i l'usuari els ha de perseguir amb el ratolí fins a completar la sèrie numèrica de la contrasenya d'accés. Aquest sistema, molt útil en general, era no obstant això poc usable per a la comunitat invident, de manera que algunes entitats permeten triar a l'usuari entre teclat ordinari o virtual per a la introducció de claus, encara que això rebaixi les exigències de seguretat.

Altres entitats van optar pel que es coneix com a *targetes de coordenades*, és a dir, un sistema físic en el qual es recullen un conjunt de claus associades a una xifra. El sistema informàtic sol·licita de l'usuari una de les múltiples claus que conté aquesta targeta física, clau que pot no tornar-se a repetir mai. El sistema és altament beneficiós com a mesura tecnològica que impediria la pesca, però és poc usable, ja que l'usuari ha de portar sempre a sobre aquesta targeta. A més, les tècniques de l'atacant inclouen la sol·licitud per correu o fax a l'usuari perquè enviï escanejada per correu electrònic o fotocopiada per fax la targeta de coordenades.

Altres tècniques, com la introducció d'una segona signatura electrònica que es generaria automàticament en intentar una transferència d'actius i que s'enviaria al telèfon mòbil de l'usuari, aconsegueixen reduir sensiblement el risc, ja que al mateix temps que alerten l'usuari titular del telèfon que s'està operant amb els seus comptes, impedeixen al pescaire aconseguir el patrimoni. A canvi, tanmateix, encareixen el model de relació client-entitat, que no serà aliè a les comissions com a fórmula per a amortitzar la despesa en seguretat.

Establert l'anterior, el cert és que l'ordenament jurídic penal no ofereix una resposta clara a aquestes conductes. Vegem-ho:

a) Estafa ordinària (art. 248.1 CP). La pesca consisteix a pescar claus a partir d'engany (bastant propi de l'estafa). Però no la segueix un error del subjecte del qual derivi un acte de disposició patrimonial, requisit també bàsic en l'estafa. És el pescaire qui, després d'usar les claus, agafarà la cosa.

Per tant, no és senzill entendre que aquest delicte sigui hàbil per a aquesta finalitat, ja que la successió d'elements concatenats que històricament incorpora el delicte d'estafa farien inviable, pràcticament, aquesta possibilitat. En efecte, el delicte d'estafa ordinària requereix un engany prou considerable per a produir error a un subjecte, error derivat del qual aquest subjecte que pateix l'error i no un altre –el subjecte que comet l'error– farà un acte de disposició patrimonial. No hi ha cap dubte que els supòsits habituals de la pesca en els quals es llança una campanya contra el titular de les claus d'accés, contra el titular dels productes bancaris als quals s'accedeix mitjançant determinades claus, són perfectament capaços de complir les exigències de l'engany de l'article 248.1 CP, ja que, en definitiva, és una posada en escena prou rellevant per a induir a error un subjecte determinat.

I precisament també és present la relació intersubjectiva, independentment de quin sigui el canal de comunicació i independentment que la relació s'estableixi de manera directa i immediata en el temps, ja que el cert és que aquesta posada en escena desenvolupada per l'autor és capaç d'arribar a un ésser humà a tall d'interlocució i generar un error en el subjecte que li impedeixi advertir que és davant d'un engany prou important que busca aquesta finalitat. Ara bé, el subjecte que pateix l'engany tan sols està lliurant, com a línia de principi, les claus d'accés als productes bancaris que permetran a l'autor del delicte conèixer quins productes té contractats i quins són els seus imports, i juntament amb això, la signatura electrònica que també ha de permetre a l'autor del delicte operar sobre aquests productes bancaris contractats per la víctima de l'engany.

En definitiva, el que el subjecte passiu de l'engany i de l'error lliura a l'autor del delicte són les claus per al coneixement i per a operar sobre els seus productes bancaris, però no el contingut del producte bancari. No és, doncs, la víctima de l'engany –la persona que pateix l'error, en definitiva– qui fa l'acte de disposició patrimonial. Per tant, l'estafa clàssica no sembla l'instrument adequat per a reprimir la pesca.

b) Estafa informàtica. L'article 248.2 CP castiga a qui, valent-se d'alguna manipulació informàtica o artifici semblant, aconsegueixi una transferència no aconseguida de qualsevol actiu patrimonial en perjudici de terceres persones. Les conductes catalogades com a pesca electrònica, caracteritzades per

l'obtenció de les claus bancàries de la víctima a partir de mètodes d'enginyeria social i el seu ús posterior per a la verificació de la depredació patrimonial, difícilment resulten enquadrables en el tenor gramatical del delicte d'estafa informàtica. En efecte, la manipulació informàtica, en el cas d'estar present, es duu a terme, no per a obtenir l'actiu, sinó les claus que donen accés als actius. La segregació de la conducta en dos moments diferents (l'obtenció de les claus i l'ús posterior), juntament amb el fet que per a l'obtenció de l'actiu, en puritat, no es produeix manipulació informàtica ni artifici semblant, impediria subsumir les conductes pròpies de la pesca en el delicte d'estafa informàtica.

Similars inconvenients, doncs, que els detallats per a l'estafa tradicional, trobarem si tractem de sotmetre les conductes en estudi al marge propi del delicte d'estafa informàtica recollit en l'article 248.2. CP. Si a primera vista sembla clar i evident que hi ha una manipulació informàtica i que posteriorment s'obté una transferència no consentida d'actius patrimonials, el cert també és que serà molt complicat vincular la manipulació informàtica amb l'obtenció no consentida d'una transferència d'actius patrimonials, llevat d'interpretació, al nostre judici, analògica del concepte de *manipulació informàtica* o *artifici semblant*.

Estafa informàtica i pesca

El delicte d'estafa informàtica, per tant, tampoc no es mostra hàbil per a la persecució de les conductes de pesca electrònica.

Sembla poc discutible que la manipulació informàtica s'ha de referir a qualsevol alteració de les dades, dels programes o dels sistemes sobre els quals operar per a poder aconseguir una transferència d'actius patrimonials. En aquest sentit, la manipulació que efectua el subjecte actiu és prèvia a l'obtenció de qualsevol transferència d'actius patrimonials, prèvia i molt distant a aquesta situació. L'autor del delicte crea un entorn virtual, o bé per mitjà del correu electrònic, o bé per mitjà de les tècniques conegudes com a *descaminament*, és a dir, emulació de l'entorn virtual de l'entitat bancària en la qual la víctima té contractats els productes bancaris, i també tractarà, amb aquesta manipulació, de comunicar-se amb la persona a la qual pretén expropiar els actius patrimonials. Però no es pot perdre de vista, tanmateix, que, com a conseqüència d'aquesta manipulació informàtica o dels artificis duts a terme pel subjecte actiu, no es produeix l'obtenció d'una transferència patrimonial, ja que el resultat de la maniobra és normalment l'obtenció de les claus, igual que succeïa en l'article 248.1 CP, per a accedir als productes bancaris i per a poder-hi operar.

Sentència del Tribunal Suprem sobre pesca com a estafa informàtica

No és aquesta, però, la línia seguida pel Tribunal Suprem en la Sentència, de 12 de juny de 2007, l'estudi de la qual s'aborda més avall, en què es qualifiquen pràctiques de pesca com a estafa informàtica. La via interpretativa assumida en aquesta resolució apareix afavorida per una línia jurisprudencial prèvia articulada entorn del concepte d'*artifici semblant* i que permet englobar gairebé qualsevol conducta que requereixi mecanismes informàtics i acabi en expropiació. D'acord amb això, constituiria artifici semblant la conducta de fer-se passar davant el terminal per qui realment no s'és (Sentència de 21 de novembre de 2001; ponent: Martínez Arrieta).

D'aquesta manera, l'acte preparatori previ, que consisteix en la creació de l'entorn, passa a ser un fet secundari (si bé, en principi, rellevant per a la finalitat de l'article 248.2 CP), i s'erigeix, tanmateix, en nucli de l'engany, la conducta de fer-se passar davant el terminal per qui no s'és (ja que ja es tenen les dades d'accés –inici de sessió, contrasenya– i d'operació sobre els comptes en què consisteix la signatura electrònica).

En aquest escenari és fàcil vincular causalment i normativament l'acció defraudadora, fer-se passar davant el terminal per qui no s'és, amb el resultat defraudador (l'obtenció d'una transferència no consentida d'actius patrimonials). Això sí, a costa d'un preu extraordinàriament alt: el principi de legalitat.

La interpretació esbossada estén, al nostre entendre, el concepte d'*artifici*, que, no ho oblidem, ha de ser semblant a una manipulació informàtica, més enllà del tenor literal possible de la norma.

Sentència de l'Audiència Provincial de Burgos sobre pesca com a estafa informàtica

No són gaires els supòsits de pesca electrònica que han conclòs en sentència als nostres jutjats i tribunals. Però entre ells, val la pena ressenyar la Sentència de l'Audiència Provincial (SAP) de Burgos de 14 de desembre de 2007, que resol un supòsit de pesca adoptant un criteri interpretatiu anàleg al sostingut per la STS de 12 de juny de 2007, que qualifica com a estafa informàtica no sols el fet principal d'apoderament de les claus bancàries i transferències posteriors, sinó també el de la conducta de qui va rebre el contingut d'aquestes transferències per després enviar-lo a un altre compte diferent controlat pel pescaire, a canvi de la retenció d'un 7% de comissió (vegeu *infra*).

Sentència de 19 de desembre de 2005 del Jutjat Penal núm. 3 de Màlaga

Amb tot, no es poden deixar d'esmentar solucions diferents, com la recollida en la Sentència de 19 de desembre de 2005 del Jutjat Penal núm. 3 de Màlaga, en què es descarta l'apreciació d'estafa informàtica en un supòsit en el qual es va emprar en un acte de comerç electrònic el número d'una targeta de crèdit aliena, i també el nom a què s'associava i la data de caducitat, de manera que amb això es va consumar una compra. D'acord amb la resolució, no hi ha estafa, ja que no hi ha manipulació informàtica, ni tan sols pel fet de fer-se passar a Internet per qui no s'és.

c) Robatori amb força (art. 237 i seg. CP). L'accés als comptes i al contingut econòmic dels comptes s'efectua mitjançant les "claus" del propietari, encara que no es corresponen amb cap de les eines descrites en l'article 238 CP quan delimita el concepte de *clau falsa*. Per això, llevat que s'entengués que el *numerus clausus* en què consisteix la definició de *clau falsa* és, en realitat, un *numerus apertus*, el delicte de robatori amb força tampoc no sembla útil per a subsumir aquestes conductes. A més, no s'accedeix al lloc on es troben les coses, almenys no físicament.

d) Delictes contra la intimitat (art. 197 CP). La captació de claus alienes podria constituir un delicte contra la intimitat, ja que el consentiment prestat pel titular de les dades està viciat per l'error patit com a conseqüència de l'engany. Tanmateix, el nom d'usuari i la clau d'accés (inici de sessió i contrasenya) no

són dades que s'obtinguin de fitxers (únic supòsit previst en l'article 197.2 CP), sinó que són cedides pel mateix subjecte, la qual cosa en principi exclouria aquesta opció, llevat que posteriorment el pescaire les incorporés a una base de dades il·legalment construïda (pel vici del consentiment), de manera que, cada vegada que hi accedís per prendre un parell de claus i usar-les, fos considerat autor d'un delicte contra la intimitat.

e) Delictes contra la propietat intel·lectual i industrial i falsedats documentals (art. 270, 274 i 390 CP). Particularment, el descaminament permetria parlar de *delicte contra la propietat intel·lectual*, en la mesura que seríem davant de la reproducció d'una obra aliena, en perjudici de terceres persones i sense consentiment del titular dels drets d'explotació. El mateix es podria dir respecte a les marques emprades, especialment quan l'objecte d'aquestes sigui prou ampli per a incloure també l'activitat per Internet. Així mateix, la pesca, però sobretot el descaminament, poden donar lloc a un delicte de falsedat en document privat, ja que aquí el document electrònic creat duu a terme tots els elements del document per a ser considerat així amb la finalitat de ser objecte material de les falsedats: es compleixen, doncs, la funció probatòria, ja que el web serveix per a provar relacions jurídiques al mercat, la funció de garantia, ja que és atribuïble a un ésser humà, i la funció de perpetuació, ja que no solament és perpetuable en el temps pel tipus de suport (un prestador de serveis que allotja la informació en un disc dur), sinó que a més és intel·ligible com a expressió del pensament humà. La falsificació del seu contingut serà determinada, a més, per la falsedat en tot o en part dels elements essencials de la pàgina.

f) Blanqueig de capitals (art. 301 CP). Finalment, la pesca, capaç de produir grans beneficis, genera una porta al blanqueig de capital. El reciclatge de diners normalment segueix una tècnica pautada. Es recluten individus per la Xarxa disposats a acceptar pagaments per a la realització líquida dels pagaments i la seva transferència posterior a la seva destinació final mitjançant la Western Union. Això obre el debat sobre el control dels comptes corrents pels quals circulen els diners. En l'actualitat, coexisteixen dues tendències a la Sala Segona del Tribunal Suprem, que es corresponen, al seu torn, amb sengles resolucions en les quals s'al·ludeix al problema del blanqueig per imprudència greu i, en particular, a si aquesta conducta és només atribuïble a professionals amb obligacions reglamentàries (això són, professionals que, pel rol que desenvolupen, tinguin atribuïts deures de diligència concrets) o també a particulars. En la STS de 17 de juny de 2005 (ponent: Martín Pallín) es nega aquesta possibilitat, encara que pràcticament tots els comportaments del particular (per exemple, un trasllat de maletes alienes a canvi d'una remuneració) es catalogarien, a canvi, com a doloses, en la mesura que per a això n'hi hauria prou de "conèixer o intuir la procedència il·lícita dels diners encara que sigui d'una manera genèrica o abstracta"; en la STS de 14 de setembre de 2005 (ponent: Monterde Ferrer), s'admet clarament la possibilitat que el particular pugui cometre el delicte de blanqueig per imprudència greu. Òbviament, no es discu-

teix la possibilitat de cometre el delicte imprudent per les entitats bancàries, la qual cosa pot succeir, òbviament, en cas que no s'efectuïn les comunicacions corresponents en els supòsits reglamentàriament taxats.

3) Excurs: la solució a la pesca adoptada per la STS de 12 de juny de 2007

La Sentència del Tribunal Suprem de 12 de juny de 2007 va qualificar com a *estafa informàtica* conductes pròpies de pesca, tant les referides al fet base, com les que consisteixen en la participació posterior en aquest fet delictiu i ho fan sols pel que fa a l'estratificació del benefici obtingut mitjançant les pràctiques de pesca electrònica.

> Malgrat la contundència amb què el Tribunal expressa la seva opinió favorable a qualificar aquests supòsits com a delicte d'estafa informàtica de l'article 248.2 CP, el cert és que aquesta visió no es pot considerar pacífica. Com s'ha vist, des de la perspectiva que aquí s'ha definit, ni el delicte d'estafa ordinari, ni el delicte d'estafa informàtica, ni les modalitats de robatori amb força, ni els delictes contra la propietat intel·lectual i industrial, que també convergeixen, o de falsedat documental, que també poden convergir, són capaços d'absorbir la totalitat del desvalor i moltes vegades ni tan sols són capaços d'entrar en escena com a conseqüència de la falta de vinculació entre l'acció desenvolupada pel subjecte i el resultat obtingut.

En el cas que ens ocupa, el Tribunal Suprem va condemnar dues persones com a autores del delicte d'estafa informàtica atesa la seva participació en la trama dissenyada per a l'obtenció de les transferències no consentides d'actius patrimonials.

En realitat, i segons es pot contrastar en el relat de fets provats reproduït en la Sentència del Tribunal Suprem, la participació dels recurrents es limita a rebre determinades quantitats de diners obtingudes dels comptes de les víctimes i a operar-hi en el mercat, és a dir, a situar-les en la primera fase d'estratificació dels diners per a generar amb això una aparença de licitud d'origen.

Així, doncs, crida poderosament l'atenció que una conducta que comença una vegada perfeccionada la conducta base, sigui tot i així sancionada precisament amb el tipus base, per mitjà del delicte d'estafa, i no per mitjà del delicte de receptació o de blanqueig de capital.

Prova de l'anterior és que, en el fonament jurídic segon de la resolució objecte de comentari, el Tribunal estableix literalment el següent:

> "En aquest escenari probatori, via prova d'indicis es pot, com li va resultar al tribunal sentenciador, concloure que ells estaven al corrent almenys de manera limitada de l'operació, la qual pel que fa a ells es concretava en: a) obertura de compte; b) recepció de transferències per persones desconegudes; c) origen d'aquests fons de comptes autèntics d'altres titulars als quals persones desconegudes als Estats Units havien accedit mitjançant l'accés fraudulent de les claus necessàries, fet que ha quedat acreditat en la denúncia inicial i en la declaració dels representants del banc, i d) una altra dada que cal tenir en compte és l'explicació donada pels altres condemnats per una operativa idèntica, explicació que consistia a cobrar una quantitat per aquest servei lliurant la resta a altres persones desconegudes."
>
> (Sentència del Tribunal Suprem de 12 de juny de 2007)

Com es pot apreciar, la participació criminal a la qual es refereix el Tribunal Suprem no té res a veure amb el delicte d'estafa, ja que ni l'obertura d'un compte corrent, ni la recepció de les transferències per persones desconegudes, ni el fet que els fons rebuts provinguin de comptes d'altres titulars residents als Estats Units, té cap relació amb el delicte d'estafa previ. Al contrari, semblen conductes que s'iniciarien específicament en el moment en què el delicte d'estafa previ, si és que aquesta és la qualificació adequada, s'hagués consumat. Malgrat que la participació que s'està imputant als recurrents no té res a veure amb els elements típics del delicte d'estafa, el Tribunal entén que, com a mínim, els recurrents tindrien coneixement de l'operativa. En efecte, en un altre passatge del mateix fonament segon es determina:

> "En aquesta situació construir un judici d'inferència que partint d'aquests fets acreditats permeti arribar a la conclusió que els recurrents van participar i estaven al corrent en el necessari de tot l'operatiu, és conclusió que en aquest control cassacional, s'ofereix com a plausible que flueix per si sola dels indicis exposats i que no és contrària a les màximes d'experiència i no és arbitrària."
>
> (Sentència del Tribunal Suprem de 12 de juny de 2007)

Fixeu-vos que, fins al moment, el Tribunal delimita els actes de participació dels recurrents com a actes que començarien immediatament després del perfeccionament dels elements del delicte d'estafa i dóna per cert, a més, que els recurrents estarien al corrent de la totalitat de l'operatiu.

Amb independència de quina sigui la via de coneixement de la totalitat del disseny delictiu, a la qual cosa ens referirem a continuació, el que veritablement fa singular aquesta resolució és que la confluència d'ambdós elements, és a dir, la participació en actes que començarien després de la consumació del delicte d'estafa i el coneixement de la totalitat de l'operatiu, serveixen al Tribunal precisament per a la imputació del delicte d'estafa i no d'un delicte posterior d'afavoriment real, per tant de receptació o de blanqueig de capital.

La informació anterior podria fer pensar que el coneixement a què es refereix l'Alt Tribunal en la resolució és un coneixement participatiu del subjecte actiu, de manera que entenem per *coneixement participatiu* el que situa el subjecte actiu no solament en el mer coneixement del pla, sinó en la creació intel·lectual del pla. Res més lluny de la realitat, tanmateix: davant l'argument dels recurrents del seu desconeixement de la resta de la xarxa d'implicats, l'Alt Tribunal descarta que aquest coneixement fos necessari per a la imputació suportada en la part dispositiva de la Sentència.

Es diu així, en el fonament jurídic segon de la resolució, que atès que s'està davant d'un:

"[...] cas de delinqüència econòmica de tipus informàtic de naturalesa intencional en el qual els recurrents ocupen un nivell inferior i només tenen un coneixement necessari per a prestar la seva col·laboració, la ignorància de la resta de l'operatiu no n'esborra ni en disminueix la culpabilitat perquè van ser conscients de l'antijuricitat de la seva conducta en prestar la seva conformitat amb un ànim d'enriquiment evident amb independència que sabessin, no volguessin saber –ignorància deliberada– o els fos indiferent l'origen dels diners que en quantitat tan rellevant van rebre. El que és rellevant –continua el Tribunal– és que se'n van beneficiar amb tot, o més probablement, en part, com a pagament dels seus serveis. És obvi que van prestar la seva col·laboració eficient i causalment rellevant en una activitat antijurídica amb ple coneixement i cobrant; per això, no poden ignorar cap indefensió. Per la seva part, l'explicació que van donar que no pensaven que efectuaven alguna cosa il·lícita és d'un angelisme que s'enfonsa per si sol."

(Sentència del Tribunal Suprem de 12 de juny de 2007)

El Tribunal finalitza l'argument establint el següent:

"En la societat actual l'acerbitat de coneixements de qualsevol persona de nivell cultural mitjà coneix i sap la il·licitud d'una col·laboració que se li pugui demanar del tipus que s'observa en aquesta causa i sobre això cal recordar que els recurrents vivien a Madrid i no consta en les interlocutòries res que pugui ser suggestiu d'un desconeixement de la il·licitud de la col·laboració que se li demanava sobretot quan no es tractava d'una col·laboració gratuïta sinó que portava annexa [insisteix el Tribunal] un enriquiment personal clar. No hi ha, per tant, cap possibilitat de derivar a cap supòsit d'error l'acció dels recurrents."

(Sentència del Tribunal Suprem de 12 de juny de 2007)

Recapitulant, som davant de conductes que consisteixen en l'obertura de comptes corrents i en l'ingrés en aquests comptes corrents de les quantitats obtingudes per terceres persones procedents de la comissió d'un fet qualificat d'estafa informàtica, sense participació material de les persones que van obrir els comptes corrents en els actes típics, nuclears o no, del delicte d'estafa informàtica.

Aquests fets són, no obstant això, qualificats tant pel Tribunal d'Instància, com pel Tribunal Suprem com a delicte d'estafa informàtica sobre la base del coneixement de la totalitat de l'operació, coneixement que, al seu torn, no serà un coneixement participatiu, sinó un coneixement basat en una ignorància deliberada (concepte que pot representar una extensió excessiva del frau i, en particular, del frau eventual i desdibuixa la distinció clàssica d'aquell amb la imprudència), en un coneixement genèric de la procedència il·lícita de les quantitats objecte de les transferències. El coneixement genèric o fins i tot la ignorància deliberada a què fa referència el Tribunal es correspondria amb un coneixement previ o simultani, d'una banda, o simplement posterior, de l'altra, dels fets constitutius de delicte d'estafa.

No oblideu que el tipus de coneixement que tindrien els recurrents sobre la totalitat de l'operativa no és documentalment acreditat, tampoc no és testificalment suportat, sinó que l'afirmació que els subjectes "estaven al corrent en el necessari de tot l'operatiu, és conclusió, que en aquest control cassacional s'ofereix com a plausible que flueix per si sola dels indicis exposats i que no és contrària a les màximes d'experiència ja que no és arbitrària".

Sens dubte, costa entendre que qui adquireix, converteix o transmet béns sabent que tenen el seu origen en un delicte o fa qualsevol altre acte per ocultarne o encobrir-ne l'origen il·lícit o per ajudar la persona que hagi participat en la infracció o infraccions a eludir les conseqüències legals dels seus actes, en realitat està cometent un delicte d'estafa informàtica i no un delicte de blanqueig de capital de l'article 301 CP.

La lectura serena dels fonaments jurídics de la resolució comentada no deixa lloc a dubtes sobre la realització d'un delicte de blanqueig de capitals en lloc d'un delicte d'estafa informàtica per part del recurrent. Així resulta, sens dubte, d'afirmacions segons les quals la intervenció dels acusats es concretava en:

> "[...] obertura de comptes, recepció de transferències per persones desconegudes, origen d'aquests fons de comptes autèntics d'altres titulars als quals les persones desconegudes als Estats Units havien accedit mitjançant l'accés fraudulent de les claus necessàries" o altres com "el rellevant és que se'n van beneficiar amb tot o més probablement en part com a pagament dels seus serveis" o "és obvi que van prestar la seva col·laboració eficientment i causalment rellevant en una activitat antijurídica amb ple coneixement i cobrant per això".

Delicte previ de naturalesa patrimonial

> Aquest tipus d'expressions, en definitiva, certifiquen la qualificació jurídica dels fets com a delictes de blanqueig de capital d'afavoriment real, en definitiva, de la comissió d'un delicte previ de naturalesa patrimonial.

I crida l'atenció encara més, si és possible, perquè precisament en la jurisprudència del Tribunal Suprem ha estat objecte de debat la qualificació jurídica que s'ha d'oferir als supòsits en els quals el particular rep quantitats de diners determinades per a estratificar-les en el mercat i tractar de reintegrar-les posteriorment de manera neta sense fer-se preguntes sobre la seva procedència lícita o no, especialment quan de la concurrència d'algunes circumstàncies es podria inferir, d'acord amb màximes d'experiència, una procedència il·lícita eventual. Tanmateix, el debat obert en el Tribunal Suprem ho ha estat als efectes de la consideració d'aquestes conductes com a doloses o imprudents, però no, sens dubte, als efectes de la seva qualificació d'acord amb el delicte previ que motivaria el blanqueig de capital.

Tot l'anterior, en resum, desvia el vertader centre del debat: el que s'hauria d'haver qualificat com a blanqueig ha estat qualificat com el delicte previ a què es refereix el blanqueig. I, d'aquesta manera, afirmant que s'efectua el delicte previ i no el de blanqueig, no ha estat necessari explicar quin és el procés d'argumentació jurídica per a establir que l'ús de les claus alienes per a transferir fons és estafa informàtica.

La clàusula d'analogia legalment definida en l'article 248.2 CP ofereix un avantatge excepcional a l'intèrpret: pot estendre analògicament el contingut del precepte sense per això lesionar el principi de legalitat; ara bé, ho estaria fent en els estrictes límits que li marca, precisament, el principi de legalitat.

Però fins i tot una clàusula d'analogia *ex lege* està sotmesa a límits i no és ni pot ser un xec en blanc perquè l'intèrpret n'empleni el contingut com vulgui. Al contrari, l'extensió típica ha d'estar estretament vinculada amb la seva referència: l'artifici ha de ser semblant no a qualsevol cosa, sinó a una manipulació informàtica. Fer-se passar per qui no s'és davant un terminal, com al seu dia va afirmar per a un supòsit similar la STS de 21 de novembre de 2001, i del qual beu la que es comenta, no és, en primer lloc, el que succeeix en la pesca; això és ja una analogia en si mateixa: el que succeeix en la pesca és que l'autor usa les claus d'un tercer per a accedir als seus comptes. No es fa passar pel tercer davant el terminal, sinó que n'usa les claus sense cap manipulació: les claus s'usen exactament igual que les usaria el seu amo. Manipulació, doncs, no es pot dir que n'hi hagi, com no n'hi ha quan és el titular de les claus qui les usa. En aquestes circumstàncies, quin artifici semblant a una manipulació s'esdevé en aquest cas?

La resposta passa per una anàlisi de les diferències i analogies que presenta la introducció de claus pel seu titular i la introducció de claus per un tercer no titular i sense consentiment. Aquest últim element és, entenem, l'únic capaç de desenvolupar un rol d'interès, i llavors l'interrogant passa a ser el següent: pot ser considerada l'absència de consentiment com un artifici? És obvi que no, però menor és encara la possibilitat d'entendre què és un artifici semblant a una manipulació informàtica, que requereix, per definició, qualsevol tipus d'alteració operada sobre el programari, maquinari, entrada/sortida de l'operació.

Un últim argument prohibeix, *in fine*, la subsumpció de la introducció de claus per un tercer en el concepte d'*artifici semblant a una manipulació informàtica*. La Llei de signatura electrònica determina les condicions que s'han de presentar per a garantir la identitat del titular d'un missatge o la seva integritat. No n'hi ha prou que el missatge de correu electrònic provingui d'un usuari del qual pengen un nom d'usuari (*username*) i una contrasenya. Aquesta sola dada no genera valor probatori sobre la identitat de l'emissor en el tràfic jurídic, ni tampoc sobre la integritat del missatge emès. Si amb la mera introducció d'un nom d'usuari i una contrasenya la llei no permet deduir valor probatori de la identitat de l'emissor del missatge, menys encara pot deduir l'intèrpret que la mera introducció d'aquestes mateixes claus en l'àmbit bancari per un tercer constitueix una manipulació tan important que ha de ser elevada a la categoria d'artifici similar a una manipulació de dades informàtiques.

Conclusió sobre la resolució del Tribunal Suprem davant de la pesca

En definitiva, l'Alt Tribunal no explica les raons per les quals la conducta del verdader pescaire, això és, el que pesca les claus i més tard les utilitza, comet els elements del delicte d'estafa informàtica; la identificació entre utilització de les claus d'un tercer i artifici semblant a una manipulació informàtica supera àmpliament el principi de legalitat, perquè no es basa en les regles de l'experiència humana; i finalment la conducta de qui fa transferències amb els diners obtinguts per tercers mitjançant l'accés inconsentit als comptes de la víctima ja no aporta res a un delicte, l'estafa informàtica, que, encara que s'entengués aplicable estaria clarament consumat.

La imputació participativa del fet requeriria la prova de la participació en la planificació, la qual cosa el Tribunal reconeix que no ha succeït. I l'atribució del fet anterior sobre la base de la coneguda *ignorància deliberada* constitueix una perversió del principi de culpabilitat que ha de ser desterrada del nostre sistema. És el legislador qui ha de prendre la iniciativa en aquest àmbit, i no l'intèrpret sobre la base de la pobresa legislativa.

3.4. Sabotatge informàtic

Els danys informàtics, més coneguts com a *sabotatge informàtic*, van ser objecte de regulació específica pel CP 1995. Aquesta opció va suposar la presa d'una posició legislativa sobre algunes de les qüestions que des de fa algun temps eren objecte de debat doctrinal. En particular, en l'àmbit dels danys informàtics, es discutia sobre la necessitat d'ampliar els tipus penals per a donar cabuda a aquesta específica forma de dany. La necessitat d'un tipus que expressament recollís la sanció penal dels danys informàtics, doncs, motivava el mateix concepte de *dany*, que habitualment s'havia mostrat incapaç –excepció feta de les propostes extensives d'alguns autors– per a ser aplicat als objectes immaterials.

A excepció d'alguns autors (González Rus), la doctrina majoritària estimava que el delicte de danys només era hàbil per a la subsumpció de conductes que es desenvolupessin sobre un objecte material en sentit estricte. Si es dóna per vàlida aquesta afirmació, el problema sorgeix en intentar delimitar els punts de trobada entre l'estructura del delicte de danys clàssic i el delicte de danys informàtics, especialment perquè aquest no es constituïa com a delicte autònom, sinó com un subtipus específic del mateix delicte de danys (De Andrés Domínguez).

El delicte clàssic de danys requereix l'existència d'una acció lesiva sobre l'objecte (que consisteix a inutilitzar, destruir o deteriorar) que, a més, s'ha de plasmar en un dany objectiu en l'objecte. Dany que, fora d'això, haurà de ser avaluable econòmicament. En aquesta avaluació, la quantitat de 400 euros exerceix de frontera entre el delicte i la falta. Però, en tot cas, tret de concepcions funcionalistes de la propietat o el patrimoni, la manera d'avaluar l'objecte atén el seu valor econòmic, el seu valor intrínsec o de mercat. Des d'aquesta perspectiva, el delicte de danys informàtics, d'una banda, no es materialitza en un resultat danyós perceptible pels sentits. A més, l'avaluació econòmica del dany (im)materialment causat presenta problemes importants, ja que, en general, el valor de l'alteració o inutilització, per si mateixa, serà insignificant. Tret, és clar, que s'estigui confonent el dany econòmicament avaluable amb el perjudici realment ocasionat amb l'alteració o dany (De Andrés Domínguez).

El legislador de 1995 va introduir el delicte de danys informàtics com a número segon de l'article 264 CP. Sens dubte el context era prou confús. El tipus bàsic de danys sobre una cosa material es contenia en l'article 263 CP, mentre que el número primer de l'article 264 es referia a danys causats al bestiar mitjançant infecció, contagi, etc. Just després, en el número segon, es descrivien els danys informàtics, cosa que va provocar una àmplia discussió sobre la vinculació

entre els danys materials i els informàtics i, particularment, sobre l'extensió a aquests últims de la frontera de 400 €. Això, al seu torn, portava a la no gens complexa qüestió del tipus de dany que havien de patir les dades.

L'article 264.2 CP considerava explícitament danyoses les conductes de *destrucció*, *alteració* o *inutilització* de dades, programes o documents electrònics aliens, continguts en xarxes, suports o sistemes informàtics (article 264.2 CP). Sobre el particular, s'advertia de les diferències de tractament que pot requerir la interpretació de l'abast de l'alteració o destrucció de dades en funció de si tenen lloc en dades contingudes en una xarxa o, al contrari, en un sistema informàtic o suport aïllat.

La immaterialitat de les dades, tant si configuren programes, com documents electrònics, dificulta la determinació de l'àmbit del que és punible, ja que, en sentit ampli, qualsevol utilització d'un sistema informàtic, segons el seu sentit i la seva funcionalitat, és capaç d'alterar, destruir i fins i tot inutilitzar dades, d'acord, com s'ha dit, amb l'ús normal i lícit a què es destina. L'accés a un programa, document o arxiu, altera o modifica una sèrie de dades en el seu ús convencional, de la mateixa manera que la connexió d'una màquina amb una pàgina web d'Internet requereix sempre modificacions en les dades dels ordinadors, precisament per a possibilitar el "diàleg" entre les màquines i la "connexió" consegüent.

Cal fer notar que, fins i tot si es parteix d'aquesta delimitació conceptual, s'han de fer precisions sobre la resta de la redacció típica, ja que l'amplitud d'algun dels termes emprats –*dades*, per exemple– podria donar lloc a la criminalització de conductes de bagatel·la.

En efecte, la punició de la destrucció, alteració o inutilització de dades, entesa en sentit ampli, donaria lloc a la inclusió en el tipus de danys de qualsevol afectació, per nímia que fos per a l'essència o funcionalitat de la cosa, de l'objecte de tutela. La restricció que ofereix la referència al menyscapte necessari de la cosa obliga a entendre aquestes dades com a immerses en una unitat de sentit, i no considerades aïlladament, de manera que únicament havien de considerar-se rellevants, en el sentit del tipus que s'examina, les conductes que aconseguien, incidint en les dades, destruir materialment o funcionalment la cosa, les dades com a unitat de significació. Si l'esborrament o la inutilització de dades no aconseguia menyscabar la cosa en el sentit apuntat, per manca de rellevància per a la seva essència o funcionalitat, no es pot reputar comès el delicte de danys informàtics.

Amb relació a l'existència de còpies de seguretat, la solució no era unitària en l'antic article 264.2 CP, sota pena d'arribar a conclusions injustes per l'aplicació d'un mateix criteri a supòsits que materialment no ho són. Així, el restabliment de la integritat del text esborrat mitjançant les còpies de seguretat no comporta més dificultats a l'usuari que una ordre rutinària al processador de text en la qual se sol·liciti la substitució del text fet malbé pel complet. Però

quan les dades alterades o destruïdes afectaven, per exemple, la configuració d'un programa que ha de ser reinstal·lat, per més que hi hagués l'original en possessió del titular de la concessió d'ús, s'havia de valorar l'abast del dany no solament en el programa mateix, sinó en tot el que aquell pogués significar per al funcionament del sistema de què es tractés –quant a danys transcendents al mateix programa.

D'acord amb el que s'ha exposat, quan hi havia còpies de seguretat i es podia restablir la cosa amb una mínima activitat per part de la víctima, es podria convenir en la presència d'una temptativa, que seria idònia o no idònia en funció del coneixement que el subjecte actiu tingués d'aquesta circumstància (a favor de la punició de la temptativa en aquests casos, Romeo, González Rus).

3.4.1. La reforma penal operada per la LO 5/2010, de 22 de juny

Tant la Convenció del Consell d'Europa, com la Proposta de decisió marc de la Unió Europea sobre els atacs de què són objecte els sistemes d'informació, han advocat tradicionalment per la creació de tipus penals que permetessin la punició de la mera alteració del funcionament de sistemes informàtics. És a dir, els delictes de danys no solament havien de contenir figures de destrucció de dades com la pèrdua definitiva d'aquestes dades o del seu valor; també havien de contenir figures típiques que permetessin la subsumpció de la mera alteració del funcionament, encara que no hi hagués pèrdua definitiva de dades, programes o sistemes.

En línia amb aquesta política criminal, el legislador espanyol ha reordenat els delictes de danys informàtics, i ha extret de l'article 264 qualsevol referència a danys diferents dels informàtics i ha reservat els seus dos números per a les conductes ja contingudes en l'antic article 264.2 (que ara passa a ser, amb algun canvi, el 264.1 CP) i per a l'alteració del funcionament del sistema (nou article 264.2 CP). La reforma dibuixa el nou article 264 en els termes següents:

> **1.** El qui per qualsevol mitjà, sense autorització i de manera greu, esborri, danyi, deteriori, alteri, suprimeixi, o faci inaccessibles dades, programes informàtics o documents electrònics aliens, quan el resultat produït sigui greu, ha de ser castigat amb la pena de presó de sis mesos a dos anys.
>
> **2.** El qui per qualsevol mitjà, sense estar-hi autoritzat i de manera greu, obstaculitzi o interrompi el funcionament d'un sistema informàtic aliè, introduint, transmetent, danyant, esborrant, deteriorant, alterant, suprimint o fent inaccessibles dades informàtiques, quan el resultat produït sigui greu, ha de ser castigat, amb la pena de presó de sis mesos a tres anys.
>
> **3.** S'han d'imposar les penes superiors en grau a les assenyalades respectivament en els dos apartats anteriors i, en tot cas, la pena de multa del tant al dècuple del perjudici ocasionat, quan en les conductes descrites es presenti alguna de les circumstàncies següents:
>
> [...]
>
> **2a.** Hagi ocasionat danys de gravetat especial o hagi afectat els interessos generals.

El legislador fa un pas en les obligacions de transposició de la manera com ho sol fer en els últims anys: tard, literalment i, sens dubte, malament. Si del que es tracta és de posar fre als supòsits en els quals s'ordena l'esborrament de dades, llavors hauria estat adequat crear un tipus en el qual el que se sanciona sigui l'actuació i no tant el resultat, els efectes del qual, ja que es tracta d'un delicte de naturalesa patrimonial, s'hauran de mesurar en seu de responsabilitat civil derivada del delicte. En efecte, una mateixa ordre d'esborrament pot fer que el resultat sigui innocu (s'esborren les dues primeres pàgines d'un document sense interès) o que el resultat sigui atroç (s'esborren unes quantes instruccions que provoquen una catàstrofe aèria). Per això, fiar el delicte a la capacitat de recuperació de les dades, a l'existència de còpies de seguretat desconegudes per a l'autor que podrien generar hipòtesis de delicte putatiu, etc., aconsellarien posar l'accent no tant en el resultat d'esborrar (que per mitjà de la clàusula de gravetat generarà inseguretat, i sense clàusula de gravetat més encara, perquè esborrar pot ser canviar de lloc o simplement destruir uns quants bytes de bagatel·la) com en l'acció d'esborrament. Per a això, hauria estat potser més útil la creació d'un tipus penal de consumació anticipada que hagués referit el desvalor a l'acció desenvolupada pel subjecte: el que executi ordres d'esborrament, alteració o supressió, deteriorament, o ordres tendents a impossibilitar l'accés a dades o programes.

Si d'aquests fets derivés un dany patrimonial, per impossibilitat de recuperació de les dades, per inversió en recuperació de les dades, etc., tot això seria incorporat a la responsabilitat civil, sense perjudici de les relacions concursals que derivessin al seu torn per altres resultats més greus en si mateixos mereixedors de sanció penal. El bé jurídic es desplaçaria llavors des del patrimoni fins a la integritat del sistema (el contingut patrimonial del qual dependrà del dany econòmic efectivament causat), aquesta vegada sí, en línia amb la política criminal internacional plasmada en l'exposició de motius de la Convenció del Consell d'Europa i en els considerants de la Decisió marc de 2005 sobre atacs als sistemes d'informació.

No ha estat aquesta, tanmateix, l'opció seguida pel legislador. En primer lloc, la reforma aprofundeix en la separació del delicte de danys informàtics respecte a la figura del delicte de danys materials, ja que ara aquests no són una modalitat residual dels danys ordinaris (com succeïa en l'article 264.2 CP), sinó que el precepte en la seva completesa es dedica a la regulació del que s'anomena també *sabotatge informàtic*. Aquesta referència facilita òbviament el trànsit envers interpretacions del delicte basades no tant en el dany a la dada com al seu valor contextual, funcional si es vol, dins del sistema, o a la informació que representa. I, s'hi suma l'actitud eclèctica consagrada en la tipicitat penal, ja que al costat de la referència al dany, esborrament, alteració, etc., el legislador situa la inaccessibilitat de les dades, cosa que podria significar perfectament el manteniment de la seva incolumitat però sense possibilitat d'usar-les en el seu context.

Tanmateix, si es vol donar un àmbit de vigència propi al segon paràgraf i no convertir-lo en una simple redundància del que es disposa en el número primer, caldria convenir que la inaccessibilitat que es proclama en el nou article 264.1 CP ha de significar destrucció definitiva de les dades. En efecte, el paràgraf segon aprofundeix en aquesta direcció en oferir cobertura als denominats *atacs DoS* (*denial of service*) o de denegació de servei, això és, la interrupció del funcionament d'un sistema mitjançant ordres comunes a una màquina però executades simultàniament i de manera massiva. Es tracta de conductes que, en vista de la laxitud amb què els tribunals han entès el concepte de *violència* en el delicte de coaccions, bé es podrien subsumir en aquest delicte (ja que s'impedeix a un altre fer el que la llei no li prohibeix mitjançant *vis in rebus*), però no en els danys si s'entén que l'essència d'aquest delicte és la destrucció de l'objecte material. Llavors, si s'utilitzen els mateixos termes (fer inaccessibles les dades) per a regular situacions diferents (esborrament o interrupció de sistemes) s'hauria de concloure que on la llei distingeix, ha de distingir l'intèrpret, fet que implicaria que, malgrat els canvis aparents, el primer paràgraf de l'article 264 CP conté un delicte de resultat que requereix la destrucció de les dades, és a dir, la seva essència, amb la qual cosa es mantindran els problemes interpretatius clàssics, perfectament plantejats per González Rus respecte a la vella redacció; el segon paràgraf quedaria reservat a la hipòtesi d'atacs al sistema que no causen un dany irreparable, sinó merament temporal, fet que no deixa de ser una anomalia en l'àmbit dels delictes patrimonials.

La referència a la gravetat en tots dos paràgrafs sembla demostrativa de la preocupació del legislador. Tímid en la reforma, sense atrevir-se a sancionar les ordres d'execució d'esborrament amb independència del resultat i exigint en canvi la destrucció de l'essència de la cosa (de la dada, programa o sistema informàtics), sembla acudir al criteri de la gravetat per evitar que els resultats de bagatel·la deslegitimin la tutela tal com està estructurada entorn d'una figura de resultat material. L'equivalència de pena en els paràgrafs primer i segon de l'article 264 es podria justificar només per la referència a la gravetat. Ara bé, no sembla encertat que un concepte indeterminat com "la gravetat" serveixi per a determinar la presència de l'injust i, al mateix temps, que el mateix patró (insistim, el mateix) serveixi per a modular la pena i elevar-la, tal com consagra el número 2n. de l'article 264.3 CP.

4. Continguts il·lícits

La difusió de continguts és un altre dels punts de conflicte que l'eclosió tecnològica ha aguditzat. Tots els problemes que la producció il·lícita de continguts o la producció de continguts il·lícits, la distribució, la comercialització, el consum, etcètera, suscitaven abans de la generalització de l'ús d'Internet, ara es multipliquen per l'efecte amplificador del mitjà.

La resposta legislativa tendeix novament a una pancriminalització de l'ús de les tecnologies per a tallar de soca-rel el creixement exponencial de comportaments que podrien lesionar béns jurídics individuals o col·lectius.

Amb tota probabilitat, són dos els sectors en els quals es deixa sentir més la tensió entre la tendència expansiva de l'ús de les tecnologies i les necessitats de tutela: d'una banda, el món de l'explotació sexual del menor i de la seva imatge; de l'altra, la tutela dels drets de propietat intel·lectual. Les pàgines següents es dedicaran a l'estudi de l'evolució de la política criminal en ambdues matèries.

4.1. Continguts il·lícits associats a l'explotació sexual del menor i de la seva imatge

La constatació de l'increment de la difusió de pornografia infantil a les xarxes telemàtiques s'ha erigit en motor d'una política criminal molt expansiva a la qual Espanya no és aliena, ostatge de la seva pròpia història legislativa recent. L'increment de la difusió telemàtica, en efecte, ha originat un greu problema de discriminació de les conductes més greus que es poden produir en aquest àmbit, amb la finalitat de sancionar penalment les de més lesivitat i deixar extramurs del dret penal la resta. En la base d'aquest increment de la difusió de pornografia a partir de les noves tecnologies, i en particular d'Internet, hi ha, doncs, la causa per la qual tant les institucions internacionals com les de caràcter nacional han elaborat projectes normatius alarmantment expansius sobre aquesta matèria.

4.1.1. Propostes internacionals de repressió de l'explotació sexual del menor

La lògica internacional en matèria de pornografia infantil o explotació sexual del menor en la qual la tecnologia es veu involucrada consisteix en l'elaboració de propostes de criminalització de qualsevol conducta relacionada amb la matèria. Són indiferents tant la presència d'un bé jurídic digne de tutela, com

el major o menor grau de perillositat de la conducta per al bé jurídic prèviament definit, o la confusió fins i tot en un mateix precepte de béns jurídics incapaços de conviure en espais tan reduïts.

En aquest punt, la política criminal internacional és molt similar, independentment del fòrum en el qual es desenvolupi. Així resulten, sens dubte, del contrast entre les propostes del Consell d'Europa i les de la mateixa Unió Europea, pràcticament idèntiques les unes de les altres.

El Consell d'Europa ha desenvolupat dues grans línies d'actuació en matèria d'explotació sexual del menor.

a) El Conveni sobre cibercriminalitat: l'article 9 del text finalment firmat el 2001 conté les línies mestres de la política criminal internacional dominant en la matèria. La proposta de criminalització és amplíssima i s'articula entorn dels elements següents:

- Concepte de *pornografia infantil*: en aquest punt convergeixen gran part dels problemes que planteja l'excessiu intervencionisme penal.
  - **Infantil**: per definició, és infantil tota imatge en actitud sexualment explícita d'un menor de divuit anys. L'establiment d'una minoria d'edat tan elevada promou un model de lliure disponibilitat de la imatge difícilment compatible amb el desenvolupat en la majoria de legislacions penals nacionals de l'àmbit continental, en el qual el menor pot consentir lliurement la relació entre els tretze i els setze anys. Potser quan els majors de setze i menors de divuit mantenen una relació i difonen entre els seus amics les imatges que ells mateixos han gravat s'haurien de convertir en subjectes actius d'un delicte d'explotació sexual d'ells mateixos?

  - **Pornogràfica**: ho serà la imatge sexualment explícita d'un menor, i entenem com a tal la conjunció d'òrgans genitals masculins o femenins, heterosexualment o homosexualment entre ells, i també la masturbació o exposició explícita d'anus o genitals en solitari, o tocaments d'aquestes parts entre menors o per majors d'edat a menors.

  - **Concepte extensiu**: però pornogràfiques als efectes de la punició de determinades conductes sobre aquest material són no solament les imatges sexualment explícites de menors de divuit anys. Pornografia infantil també és considerada aquella en la qual: i) apareixen adults que simulen ser menors (pornografia pseudoinfantil), i ii) apareixen imatges realistes de menors inexistents en la realitat, en actitud sexualment explícita, és a dir, la denominada *pornografia virtual* o *tècnica*.

- **Conductes punibles**: la lluita contra la pornografia infantil exigeix l'abstracció de les conductes amb més capacitat per a comprometre el bé jurídic protegit, prèviament seleccionat pel legislador. El Consell d'Europa

proposarà la incorporació, a les legislacions nacionals, de la producció, oferiment, difusió, comercialització, posada a disposició, procurament i possessió com a expressió de les més greus formes d'actuació en l'àmbit de la pornografia infantil.

b) El Conveni per a la protecció dels menors contra l'explotació i l'abús sexuals, fet a Lanzarote el 25 d'octubre de 2007.

L'expansió d'Internet no solament és quantitativa, sinó també qualitativa. Neixen constantment eines adaptades al Protocol d'Internet que, al mateix temps que generen avantatges, també serveixen per a la realització de fets danyosos no sempre sàviament previstos en la llei penal. La gran acollida de les xarxes socials entre els més joves ha afavorit, en efecte, una nova fórmula d'accés als menors amb la finalitat de mantenir finalment contactes sexuals amb el seu consentiment o sense (viciat o no). Es tracta del fenomen conegut com a *ciberassetjament a menors* (*grooming*), en què, o bé mitjançant l'ús d'una identitat falsa, o bé mitjançant l'ascendència guanyada per l'edat, el menor acaba confiant en el subjecte amb qui acabarà mantenint relacions sexuals violentes, intimidadores o, en el millor dels casos, viciades. És, en qualsevol cas, el vell fenomen de l'abús de superioritat, l'abús de confiança o fins i tot la prevalença, únicament diferenciats per l'ús d'un mecanisme tecnològic en la confecció de l'engany, l'abús o la prevalença.

A l'empara de l'exhibicionisme massiu dels menors a les xarxes socials, es promociona un conveni en el qual es reiteren les obligacions de transposició en matèria de pornografia infantil recollides en el Conveni sobre cibercriminalitat (això sí, corregides, segons es veurà) i s'inclouen avanços nous de la tutela penal. Així, l'article 23 del Conveni estableix l'obligació de tipificar la proposició d'un adult feta mitjançant les tecnologies de la comunicació i la informació per a trobar-se amb un menor a fi d'abusar-ne sexualment.

Novament, es promociona un avançament de la tutela penal, a l'empara aquesta vegada de les xarxes socials (tipus Facebook o Fotolog, etc.). La tutela projectada no es refereix a l'abús amb prevalença, modalitat ja àmpliament coneguda en l'àmbit de les legislacions nacionals del continent, sinó als actes previs de contacte amb el menor per mitjà de les xarxes socials amb aquest únic propòsit, una cosa que d'una altra manera difícilment cauria en l'àmbit de la temptativa, almenys en països com el nostre, fortament lligats a l'objectivització del perill per al bé jurídic a partir d'actes inequívocament típics (en aquest cas, d'abús o agressió sexual).

Per la seva banda, la Unió Europea ha anat plasmant les seves propostes en matèria de pornografia infantil en l'àmbit de les xarxes de telecomunicacions amb dos textos. Primer, en la Decisió marc 2000/375/JAI del Consell, de 29 de maig de 2000, relativa a la lluita contra la pornografia infantil a Internet i,

posteriorment, en la Decisió marc 2004/68/JAI del Consell, de 23 de desembre de 2003, relativa a la lluita contra l'explotació sexual dels nens i la pornografia infantil.

Amb alguna excepció i especificitat que no requereixen massa deteniment, la Decisió marc 2004/68 conté obligacions de tutela pràcticament idèntiques a les descrites en el Conveni del Consell d'Europa sobre cibercrim: es preveu la sanció de la producció, distribució, facilitació, etcètera, de pornografia infantil, que s'entén com no solament aquella en la qual apareixen menors en actitud sexualment explícita, sinó també la pornografia pseudoinfantil i la pornografia virtual o tècnica.

Tant la Decisió marc de la UE com el Conveni de 2007 del Consell d'Europa sobre explotació sexual del menor permeten l'establiment de reserves als estats membres, en supòsits molt específics. En particular, la Decisió marc permetria excloure de responsabilitat la tipificació de la pornografia pseudoinfantil quan, de fet, la imatge reflectís una persona de més de divuit anys. És obvi que aquesta previsió s'ha d'interpretar com un simple dret de reserva, encara que en la redacció de la Decisió marc sembla més una causa de justificació en la qual el supòsit de la prohibició i el supòsit de la justificació serien idèntics.

En efecte, la referència a "poden excloure de responsabilitat criminal" semblaria que tendeix a justificar excepcionalment el fet, en lloc de no desvalorar-lo (que és en el que consistiria una reserva); no obstant això, un grau de contradicció tan elevat entre *prohibició* i *justificació* deslegitima tant la norma que només es pot interpretar com una redacció desafortunada del dret de reserva dels estats a no criminalitzar la pornografia pseudoinfantil.

Així mateix, ambdós textos (Decisió marc de la UE i Conveni de 2007 del Consell d'Europa) recullen la possibilitat d'establir reserva en aquells casos en els quals la imatge del menor en actitud sexualment explícita ha estat obtinguda pel mateix menor i per al seu consum.

> En qualsevol cas, la política criminal internacional en aquesta matèria revela un dèficit sever en la selecció del bé jurídic. Efectivament, sota la bandera de la protecció de la infància, que pocs no estarien disposats a fer-se-la pròpia, s'acumulen desordenadament conductes greument atemptatòries contra la llibertat sexual del menor (com la producció de pornografia infantil, en què es protagonitza l'agressió al menor o l'abús) amb d'altres que no podrien transcendir mai l'àmbit purament moral (el consum de pornografia d'adults que simulen ser menors) i fins i tot amb d'altres en les quals el bé jurídic, tot i existir, no es relaciona en res amb la llibertat sexual del menor, sinó més aviat amb el dret a la pròpia imatge.

Segurament, la llibertat sexual no és la referència més adequada quan es tracta de menors, tenint en compte precisament que és una característica encara en formació entre els petits. Tenint en compte l'anterior, ha estat desenvolupada més encertadament per un sector autoritzat doctrinal (Morales Prats) la indemnitat sexual com a bé jurídic íntimament relacionat amb el lliure desenvolupament de la personalitat i, en conseqüència, l'accés a una llibertat d'elecció futura quant a la manera de desenvolupar-se i realitzar-se sexualment. Però en

qualsevol cas el major o menor encert d'una referència específica al bé jurídic en matèria de sexualitat relacionada amb la infància no pot servir de cobertura per a la regulació sota un mateix epígraf de conductes absolutament dispars en les quals ni tan sols el subjecte passiu (que hauria de ser sempre el menor) coincideix.

El concepte genèric *pornografia infantil* no té prou força per a aglutinar el conjunt de conductes que les propostes internacionals pretenen que els estats nacionals integrin en el seu ordenament jurídic. Pornografia infantil és pornografia en la qual apareixen menors d'edat en actitud sexualment explícita. I la minoria d'edat comprèn una franja ben precisa d'edat que pot ser més o menys àmplia en funció de l'estratègia politicocriminal conjunturalment imperant. Més enllà d'aquesta franja d'edat, la pornografia deixa de ser infantil per a ser convencional; més enllà de les conductes d'ingerència directa en la sexualitat del menor i, per tant, atemptatòries contra la seva indemnitat sexual, es deixa d'afectar el bé jurídic per a entrar en el terreny del que és estrictament moral o, simplement, de béns jurídics diferents.

És obvi que la producció de pornografia entre menors d'edat implica una afectació directa de la indemnitat sexual del menor que afecta o pot afectar severament el desenvolupament normal de la seva personalitat en matèria d'autorealització sexual. El productor de la pornografia és el subjecte que disposa dels mecanismes per a això i fins i tot qui, de vegades, executa els actes d'abús o agressió sexual sobre el menor amb la finalitat de plasmar en algun tipus de suport el resultat de l'abús.

Resulta forçós interrogar-se sobre si amb l'abús o l'agressió mateixos no ha finalitzat ja la lesió del bé jurídic "indemnitat sexual", cosa que faria intranscendent la plasmació o no de l'escena en algun tipus de suport. I al nostre judici la resposta ha de ser negativa. La creació de l'episodi plasmat en un suport reproduïble implica una afectació, cert, de la indemnitat sexual del menor; però, en la mesura que s'executa amb una finalitat ulterior a l'ànim lúbric –l'explotació sexual d'aquest mateix menor a qui concretament s'ha agredit–, la conducta entra de ple en els marges de la indemnitat sexual, ja que aquest és un objecte de tutela altament individualitzable.

No es pot dir el mateix, tanmateix, de les conductes de distribució dels qui no han participat ni en l'execució de la violació del menor ni en la producció de les imatges perpetuables.

És el cas de la distribució amb ànim d'explotació comercial. La indemnitat sexual és aquí difícilment identificable, ja que aquesta incolumitat ja va ser trencada amb la producció i la primera plasmació.

En primer lloc, podria succeir que el menor, la imatge del qual es difon i es distribueix en fòrums públics o s'intercanvia de manera privada, no fos ja menor en el moment de la distribució. Sens dubte, en aquests casos pocs dubtes

hi pot haver de la impossibilitat d'afectar la indemnitat sexual del menor. Però és que tampoc no s'afecta la llibertat sexual de l'adult que és ara aquest menor i, a més a més, podria resultar que, en el moment de distribuir les imatges de la seva agressió sexual, aquest menor hagués mort.

La idea de traficar amb imatges en les quals apareix un menor en actitud sexualment explícita, o bé amb un altre menor (a la qual cosa hauria estat obligat sempre, atesa la impossibilitat que el menor consenti lliurement), o bé amb un adult, és certament repugnant. Però penseu per un moment en la distribució d'imatges reals en les quals apareix l'homicidi d'un home (per exemple, el penjament de Saddam Hussein, àmpliament difós en tots els mitjans de comunicació a escala planetària). I, per no prejutjar la legitimitat/il·legitimitat de l'ajusticiament i tractar de trobar-hi la diferència, penseu en els assassinats de l'antiga Iugoslàvia, la reproducció dels quals és fàcilment localitzable a la Xarxa.

Quan es traça la comparativa, s'evidencia ja un primer problema, segurament de naturalesa cultural: com és possible sancionar la reproducció d'una violació d'un menor i no fer el mateix amb la violació d'un adult? I, aprofundint en l'argument: com és possible sancionar penalment la representació audiovisual de la violació d'un menor i no la de la seva mort, per exemple?

Recentment, han estat penjats al portal Youtube alguns vídeos "humanitaris" en els quals es filmaven l'agonia i la mort de nens sud-americans incapaços de superar un brot de pneumònia aguda a la regió; els autors dels vídeos sol·licitaven donacions per combatre la tragèdia.

Podríem suportar la trucada d'una ONG dedicada a la lluita contra l'explotació sexual, que recaptés fons mitjançant l'emissió de vídeos en els quals es recullen els abusos sexuals del menor?

En segon lloc, encara que el menor fos menor en el moment de la distribució de la imatge, la seva llibertat sexual no es veu més amenaçada amb la difusió de les imatges, ja que la incolumitat sexual del menor va ser truncada amb l'agressió i la seva plasmació en un suport.

De segur, a hores d'ara, s'haurà pogut intuir ja l'opció politicocriminal que inspira aquest text. La difusió de pornografia infantil en sentit estricte (pornografia en la qual apareixen menors reals fins a la franja d'edat que legalment es determini com a tal en actitud sexualment explícita) ha de ser constitutiva de delicte. Però la seva tipificació no s'ha d'abordar en l'àmbit dels delictes contra la llibertat sexual. En aquest àmbit només es podria considerar una modalitat específica d'afavoriment real, ja que l'agressió al bé jurídic relacionat amb la llibertat sexual (la indemnitat o incolumitat) ja va ser verificada definitivament amb l'agressió i la primera plasmació. Com ha assenyalat un sector rellevant de la doctrina, són d'altres els béns jurídics compromesos en l'acció de difondre i comunicar a tercers la imatge del menor agredit. D'una banda, no hi ha cap dubte que tota imatge d'un menor en actes de sexualitat explícita ha estat obtinguda il·lícitament, o bé perquè es participa en l'agressió, o bé perquè es plasma per vegada primera en un suport mentre s'està executant; d'una altra banda, apareix clar com si fos de dia que la imatge del menor, en ser captada il·lícitament, no pot ser objecte de comerç sense afectar greument la intimitat del titular. Així, doncs, els delictes contra la intimitat i la imatge pròpia són el lloc idoni per a la sanció penal de les conductes d'aprofitament de la imatge del menor, i se n'agreuja la responsabilitat en els casos en els quals

l'aprofitament de la imatge, a més, es refereix a la imatge sexual del menor (no cal dir que el mateix hauria de regir per a la seva pròpia mort), d'acord amb una tutela escalonada en funció del tipus d'imatge que concretament s'explota.

Així expressat, fora d'això, també la difusió de la imatge de la mort d'un tercer (que podria ser fins i tot la d'un menor) es podria considerar constitutiva de delicte, de manera que es recupera així l'equilibri de proporcionalitat, ja que, en definitiva, la imatge d'aquell a qui s'executa contra la seva voluntat difícilment haurà estat obtinguda mitjançant el seu consentiment i, per tant, ho haurà estat mitjançant coacció (violència o intimidació).

Si ja la difusió planteja problemes d'acomodació en el si genèric dels delictes contra la llibertat i la indemnitat sexuals, més problemàtica resulta en aquest àmbit la inclusió de la possessió de pornografia infantil. La conducta de qui únicament té per a la seva pròpia satisfacció material pornogràfic en el qual apareixen menors, no hi ha cap dubte que és un factor d'afavoriment, però de la conducta aliena. És un altre qui agredeix, produeix, plasma en un suport i difon.

El consum deslligat del tràfic o intercanvi no és en si mateix agressiu de cap bé jurídic.

Es pot acceptar fins i tot la teoria –molt lligada al consum progressiu de drogues cada vegada més agressives– que el consum de pornografia infantil, quan mostra un desordre de la personalitat, mostra un subjecte amb un pronòstic de perillositat: el pedòfil està en condicions de progressar cap a la pederàstia. I, finalment, és clar que la tolerància respecte al consum de pornografia infantil no és, sens dubte, el model social que hagin de promocionar, ni tan sols tolerar, els poders públics. Però la repressió penal confon el malalt amb el delinqüent. I definitivament la denominada *pornografia tècnica* o *pseudoinfantil*, que engloba tant les hipòtesis en què l'adult simula ser un menor com aquelles en les quals no hi ha cap menor, sinó que es tracta de pures creacions, invencions realistes de personatges no existents en la realitat, no hauria de tenir ancoratge en el sistema de delictes contra la llibertat sexual.

En aquest cas, es tracta d'infraccions contra l'ordre públic, contra una concepció moral àmpliament compartida i només molt minoritàriament subvertida, però moral, al cap i a la fi. No hi ha menors per protegir, ja que es parteix del supòsit de la imitació de menors i la idea d'una referència a la protecció de la infantesa no justifica la utilització dels delictes contra la llibertat sexual: el lliure desenvolupament sexual que s'ha de garantir al menor, lliure d'intromissions alienes, és un bé personalíssim, davant el significat col·lectiu i proteic de la infantesa.

4.1.2. La regulació de la pornografia infantil en el Codi penal

La repressió penal d'aquest fenomen no ha estat, lamentablement, una constant al nostre país. De fet, el CP 1995 va suprimir el delicte de corrupció de menors per les connotacions que la figura delictiva comportava, amb la qual cosa la difusió d'imatges en les quals apareixien menors en actituds sexuals explícites quedaven al marge de la tutela penal. En no haver-hi un delicte específic que donés cobertura a aquestes infraccions, es recorria a la utilització de menors en espectacles exhibicionistes, cosa que podia ser raonable per a la utilització del menor en la captació de la imatge, però sens dubte no per a la seva difusió, on no quedava rastre de vinculació normativa amb el concepte d'*utilització*, per més que algun sector doctrinal s'entossudís a forçar la lletra de la llei contra el seu tenor literal. En el nostre dret intern, per tant, la cobertura penal de la difusió de pornografia infantil es produeix només a partir de la reforma del CP 1995 duta a terme per la LO 11/1999, de 30 d'abril, ara reforçada amb la cobertura que ofereix la reforma operada per la LO 15/2003, de 26 de novembre.

Distribució d'imatges de pornografia infantil

Una mostra clara de l'anomia regnant al nostre país és, sens dubte, l'esdeveniment ocorregut el 1996 en el qual dos estudiants de la Universitat Politècnica de Catalunya distribuïen imatges de pornografia infantil –fotografies preses per tercers– des d'un servidor ubicat a la localitat de Vic, fet que va despertar l'alarma social sobre això en no haver-hi figura legal en què subsumir els fets, per la qual cosa l'assumpte va ser sobresegut en via penal. Responent a l'alarma social despertada i en consonància, d'altra banda, amb les propostes de caràcter internacional, el legislador va introduir l'apartat *b* en l'article 189 CP, segons el qual "ha de ser castigat amb la pena de presó d'un a tres anys: qui produeixi, vengui, distribueixi, exhibeixi o faciliti la producció, venda, difusió o exhibició per qualsevol mitjà de material pornogràfic en l'elaboració del qual hagin estat utilitzats menors d'edat o incapaços, encara que el material tingui l'origen a l'estranger o sigui desconegut. A qui tingui aquest material per a la realització de qualsevol d'aquestes conductes se li ha d'imposar la pena en la seva meitat inferior".

L'article 189.b CP sanciona amb penes de presó d'un a quatre anys qui:

> "[...] produeixi, vengui, distribueixi, exhibeixi o faciliti la producció, venda, difusió o exhibició per qualsevol mitjà de material pornogràfic en l'elaboració del qual hagin estat utilitzats menors d'edat o incapaços, o qui en tingui per a aquestes finalitats, encara que el material tingui l'origen a l'estranger o sigui desconegut".

La pena descendeix fins a un marc d'entre tres mesos i un any en els casos en els quals es tingui el material pornogràfic anteriorment descrit per a l'ús propi.

L'article 189.b CP conté, estructuralment, un delicte de consumació anticipada: no solament la participació delictiva es converteix *ope legis* en autoria (facilitació), sinó que el mer fet d'anticipar l'autoria anticipa alhora la consumació, parificant punitivament la consumació del tràfic amb la mera possibilitat del tràfic. És la mateixa tècnica legislativa seguida en àmbits de tolerància zero, com el tràfic de drogues, en què l'execució d'actes de tràfic (vendre, comprar per vendre...) conviuen penològicament amb la facilitació o l'afavoriment del consum il·legal de drogues tòxiques.

En l'estructura del precepte resideix l'essència de la política criminal abans descrita. Es tracta d'una figura de perill referida a un bé jurídic difús (en sentit purament gramatical, aquí): n'hi ha prou amb la facilitació de la difusió, de la venda o de l'exhibició d'imatges, amb independència que finalment resultin difoses, venudes o exhibides, perquè el precepte es consumi. La consumació anticipada remet, llavors, a una idea de perill per al bé jurídic que, tanmateix i com s'ha vist *ut supra*, no és fàcil aprehendre en el context sistemàtic –la incolumitat i indemnitat sexual– en el qual es basa el precepte.

S'ha d'insistir, per tant, que, en vista del paper catalitzador d'Internet en l'eclosió de xarxes de pederàstia, el dret penal és un recurs necessari, imprescindible, però l'estructura del delicte ofereix un cànon de seguretat jurídica que no pot ni ha de ser sacrificat per molt elevat que es pretengui l'interès. Una tutela penal satisfactòria de l'interès del menor utilitzat ja anteriorment en l'elaboració del material pornogràfic i víctima, per tant, d'un delicte autònom d'agressió sexual passa, com ha explicat Morales Prats, per multiplicar la capacitat dels delictes contra la intimitat i la imatge personal i familiar continguts en els articles 197 i seg., principalment per a aquells casos en els quals la utilització del menor queda ja llunyana i, per tant, també el bé jurídic llibertat sexual, entès com el lliure desenvolupament de la seva sexualitat.

Lectura recomendada

F. Morales Prats (2002). "Pornografía infantil e Internet. Ámbitos de incriminación". A: F. Morales Prats; Ó. Morales García (coord.). *Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet* (pàg. 105 i seg.). Cizur Menor: Aranzadi.

L'article 197 CP ofereix un llarg recorregut per a la repressió penal de l'aprofitament de la imatge del menor: qui produeix la imatge pornogràfica en el moment de l'agressió sexual del menor, amb independència de la seva participació eventual en aquest delicte per mitjà de la intimidació ambiental que exerceix, hi ha de respondre a partir de l'article 197.1 CP (qui per a vulnerar la intimitat d'un altre utilitzi aparells d'enregistrament de la imatge). Qui difon les imatges així obtingudes, hagi o no participat en la seva obtenció, ha de fer el número 3 d'aquest precepte; en ambdós casos, a més, operaria per doble partida el subtipus agreujat de l'article 197.5 CP, atesa la naturalesa sexual de les imatges i la minoria d'edat de la víctima del delicte.

Si en el dret espanyol els problemes que es plantegen, especialment pel que fa a les garanties que hagi d'oferir el procés penal, són ja importants, la punició de la possessió de pornografia infantil els multiplica. I, encara que la matèria és, sens dubte, objecte de sensibilitats especials, no s'han de deixar de subratllar els problemes politicocriminals i tecnicojurídics que es plantegen.

La possessió de material pornogràfic en el qual apareixen menors no tindria, en l'actualitat, cabuda en els delictes contra la intimitat. L'article 189.b CP no és, tanmateix, el lloc més apropiat sistemàticament, ja que cap tipus d'afectació de la indemnitat sexual d'un tercer no es pot predicar del consum privat de les imatges.

En segon lloc, amb relació al concepte de *possessió*, es fa difícil trobar una lògica en la pornografia infantil similar a la dissenyada per la jurisprudència per al tràfic de drogues. Així, quantes imatges s'han de tenir per a fer la conducta? Una sola o múltiples? I una repetida en múltiples ocasions? Es pot parlar de possessió en funció de la qualitat de les imatges, de l'edat dels menors, de la seva naturalesa homosexual o heterosexual, etcètera?

La repressió penal de l'explotació sexual del menor i el seu aprofitament ulterior han de continuar essent un objectiu fonamental dels poders públics, i el dret penal, una eina clarament necessària en la seva administració. Això no significa que es pugui emprar sacrificant els fonaments del sistema, ni que es pugui infratutelar l'interès del menor com a conseqüència d'un ús inapropiat de les regles penals.

4.2. Difusió de continguts i delictes contra la propietat intel·lectual

El cavall de batalla en l'àmbit de la propietat intel·lectual queda referit a la garantia d'explotació de l'obra pel titular dels drets en un context de generalització o, si es vol, utilització quotidiana de suports digitals. L'era de la digitalització, en efecte, repercuteix de manera directa en l'enteniment dels conceptes clàssics i universals de *reproducció*, *comunicació pública* i *distribució*, que, fora d'això, l'article 270 CP fa seus prenent-los directament del Text refós de la llei de propietat intel·lectual (TRLPI).

La fixació d'obres, especialment audiovisuals, en format binari, és a dir, per dígits (zeros i uns), dificulta, si no impedeix, la delimitació entre original i còpia, a més a més de multiplicar la capacitat de reproducció de l'obra sense minvar-ne aparentment la qualitat. En aquest context, l'assignació als diversos interessats de diverses parcel·les d'explotació de l'obra ha requerit un ajust conceptual de certa envergadura, ja que algunes es tenen amb caràcter exclusiu i amb autorització expressa d'explotació per tercers.

A les premisses anteriors s'ha de sumar una qüestió de dimensions estructurals semblants. La mateixa naturalesa d'Internet i la digitalització d'obres qüestionen l'extensió a aquest sector en aquest format, dels drets d'explotació de l'obra pels qui els tenen en la dimensió real. La magnitud del problema és inqüestionable si s'atenen els esdeveniments que afecten el sector audiovisual a Internet. L'emmagatzemament de l'obra en format digital en permet la reproducció mitjançant ordinadors i, en particular, la reducció de la mida que els diferents temes emmagatzemats ocupen en els dos tipus de memòria de la màquina, mitjançant compressió. I, en vista de la capacitat comunicativa del mitjà, no és difícil inferir la repercussió que sobre la còpia privada ha mostrat el model exposat. D'una banda, l'obra musical ha estat comercialitzada en portals d'Internet a preus sensiblement inferiors als que operen al mercat de CD, autorització prèvia d'autors editors i, si escau, entitats de gestió, sota el pretext d'efectuar una comunicació pública de l'obra, de manera que es defuig l'autorització preceptiva dels productors fonogràfics. La situació s'aguditza amb la utilització de programes específicament destinats a l'intercanvi d'arxius

musicals comprimits entre particulars mitjançant la descàrrega directa d'arxius d'ordinador a ordinador, la qual cosa posa en perill, sens dubte, la rendibilitat de l'obra musical i, en conseqüència, l'incentiu a la creativitat.

En aquest context, no es pot desconèixer la clarísima tensió que s'ha viscut a escala global entre l'accés a la cultura com a dret normalment consagrat en els textos constitucionals i el dret dels autors, artistes, etcètera, a explotar l'obra o les seves transformacions. En aquesta tensió, les oscil·lacions són constants.

Inicialment, la indústria va aconseguir el suport governamental per a desenvolupar en els àmbits supranacional, internacional i nacional una tutela jurídica amplíssima del dret d'explotació de les obres. Sens dubte, pocs dubtes hi pot haver de la decantació en favor de la tutela a la llum, per exemple, de la configuració dels règims jurídics europeu i nacional dels programes d'ordinador. O, encara en l'àmbit supranacional, la Convenció del Consell d'Europa proposava en les primeres versions, d'abril de 2000, anteriors al text definitiu obert a la firma, que els estats membres regulessin com a infracció penal tota infracció civil descrita en els tractats i convenis fins llavors vigents (Conveni de Berna, Acta de París, tractats de l'OMPI, etcètera).

Regulació dels delictes contra la propietat intel·lectual

Els delictes contra la propietat intel·lectual, que normalment recorren a l'estructura de la norma penal en blanc, no podien dependre de manera tan absoluta de la infracció civil, ja que amb això es trencaven els principis de subsidiarietat, fragmentarietat i última ràtio, per la qual cosa l'article 10 de la Convenció es va acabar conformant a exigir als estats un nivell suficient i raonable de tutela dels drets d'autor mitjançant els instruments jurídics, inclòs el penal, segons fos necessari en cada estat.

Tanmateix, l'evolució tecnològica i l'aparició de les xarxes de parells, amb programes senzills capaços de permetre l'intercanvi d'arxius audiovisuals entre desenes de milions de persones, desequilibraven greument, *de facto*, la tensió necessària entre la tutela dels drets d'autor i l'accés a la cultura.

Fruit d'aquest desequilibri és l'*statu quo* actual de la situació: mentre que la tutela jurídica que es dispensa als drets de propietat intel·lectual és amplíssima, les fórmules per a accedir sense contraprestació a aquesta mateixa obra proliferen d'una manera gairebé incontrolable, cosa que compromet la viabilitat del sistema tal com el coneixíem. A continuació, es desenvoluparan ambdós aspectes en paral·lel.

4.2.1. La regulació en el Codi penal

a) Tipus bàsic

L'article 270 CP sanciona amb la pena de presó de sis mesos a dos anys o de multa de sis a vint-i-quatre mesos qui, amb ànim de lucre i en perjudici d'un tercer, reprodueixi, plagiï, distribueixi o comuniqui públicament, en tot o en part, una obra literària, artística o científica, o la seva transformació, interpre-

tació o execució artística fixada en qualsevol tipus de suport o comunicada a partir de qualsevol mitjà, sense l'autorització dels titulars dels drets de propietat intel·lectual corresponents o dels seus cessionaris.

L'estructura típica de l'article 270 CP s'ha d'entendre com a norma penal en blanc que obliga l'intèrpret a endinsar-se en les disposicions del Text refós de propietat intel·lectual a fi de poder dotar de significat les conductes típicament rellevants. La legislació extrapenal, en aquest cas, en delimitar exhaustivament el contingut del dret, descriu els límits mínims entre els quals pot discórrer la intervenció penal, que, per tant, no pot anar més enllà en el sistema repressiu davant violacions dels drets de la propietat intel·lectual del que el sistema civil va en la delimitació dels drets tutelats.

El Codi penal planteja una estructura basada en la tutela de l'obra literària, artística i científica, i els drets connexos, és a dir: la seva transformació, interpretació o execució, això sí, fixades per primera vegada en un suport, cosa que inclou la tutela del productor de fonogrames, titular del dret de reproducció exclusiva o contra autorització prèvia. La referència a l'ànim de lucre certifica que la tutela juridicopenal té una dimensió patrimonial. No es protegeix, doncs, el dret moral d'autor, ni tan sols per mitjà de la menció expressa del plagi, si no hi ha una projecció de la conducta cap al dret del titular del dret a l'explotació de l'obra.

Alhora, l'article 270 CP es projecta també sobre els denominats *drets sui generis*. El Text refós de propietat intel·lectual recull una àmplia tutela dels programes d'ordinador i les bases de dades, que s'ha vist corresposta, en efecte, en el Codi penal.

Les bases de dades, que de manera general es podrien definir com a recopilacions de dades o altres elements que adquireixen un sentit en funció de la facilitació del seu maneig i la tutela dels quals es reclama en funció dels enormes recursos humans i tècnics invertits en el procés de creació, són avui objecte de múltiples atacs, dins i fora de la Xarxa, que van propiciar la promulgació, el 1998, de la Llei de bases de dades, absorbida pel TRLPI (àmpliament, sobre el particular, Delgado).

Drets d'autor sobre els programes d'ordinador

Els programes d'ordinador es troben protegits pels drets d'autor, després de les imposicions de la Directiva 91/250/CEE, de 14 de maig de 1991, sobre la protecció jurídica de programes d'ordinador i de l'article 95 TRLPI, que transposa al dret espanyol la Directiva.

Tanmateix, no són considerats com a obra literària, tal com apareixia en el Projecte de 1993 i tal com la Directiva proposava als legisladors nacionals per tal de posar fi als possibles efectes negatius que una dispersió de la tutela conforme a sistemes diversos pogués originar en el mercat comú europeu. L'article 95 TRLPI és, en realitat, una norma especial que regula el que no preveu el règim general, però que hi queda íntegrament sotmès. Essent les excepcions de naturalesa quantitativament superior, sembla que el TRLPI instaura, en realitat, un sistema de protecció dels programes d'ordinador de *ius singulare*; bà-

sicament, perquè el programa d'ordinador no és una creació artística i malgrat que no va encaminat a la comunicació amb un humà, sinó a controlar una màquina.

El TRLPI incorpora en l'article 96 una definició expressa del que s'ha d'entendre per *programa d'ordinador* i estén en el paràgraf segon del mateix precepte i número (art. 96.1 TRLPI) la protecció atorgada al programa, *stricto sensu*, a la documentació tècnica i els manuals d'ús d'un programa. A més, entén englobada en el concepte de *programa d'ordinador* la seva documentació preparatòria. A partir d'aquesta definició i extensió de l'àmbit de protecció del programa d'ordinador com a *ius singulare*, es pot consignar, si més no breument, el contingut dels drets d'explotació que el TRLPI ofereix a l'autor del programa, que bàsicament integra el dret de dur a terme o autoritzar:

- La reproducció total o parcial, fins i tot per a ús personal, per qualsevol mitjà i sota qualsevol forma. Tota forma de càrrega, presentació, execució, transmissió o emmagatzemament d'un programa que necessita una reproducció del mateix programa, ha de ser autoritzada pel titular del dret.

- La traducció, adaptació, arranjament o qualsevol altra transformació d'un programa d'ordinador i la reproducció dels resultats d'aquests actes, sens perjudici dels drets de la persona que transformi el programa d'ordinador.

- Qualsevol forma de distribució pública, inclosa el lloguer del programa d'ordinador original o de les seves còpies. Produïda la cessió del dret d'ús, s'estableix una presumpció *iuris tantum* que la cessió ho serà amb caràcter no exclusiu i intransferible, i s'estén la presumpció fins a les necessitats pròpies de l'usuari.

La protecció al programa d'ordinador és, doncs, amplíssima. La llei parla de llicències d'ús o cessió dels drets d'ús, i atorga la pràctica totalitat dels drets a l'autor. Els programes no es venen, es llicencien per a finalitats específiques, per la qual cosa qualsevol classe d'excés esdevé conducta il·lícita juridicopenalment, tal com hem vist més amunt, en la SAP de Barcelona de 1999.

A més de l'anterior i precisament perquè l'article 270 CP conté una norma penal en blanc, es feia francament difícil sancionar penalment els actes d'aprofitament no lucratiu (és a dir, no orientats a l'obtenció d'un benefici comercial) de l'obra aliena. Fins a la transposició de la Directiva 2001/29/CE, de 22 de maig, relativa a l'harmonització de determinats aspectes dels drets d'autor i drets afins als drets d'autor en la societat de la informació (Directiva de la societat de la informació), el Codi penal es mostrava seriosament incapaç de projectar-se sobre algunes de les conductes més lesives dels interessos econòmics del titular dels drets d'explotació, en particular les descàrregues provinents de les xarxes de parells.

I és que la tutela penal dels drets de propietat intel·lectual s'articula entorn de les conductes bàsiques de reproducció, distribució i comunicació pública, i la insuficiència d'aquests conceptes en gran part dels ordenaments nacionals dels estats membres de la UE per a absorbir el desvalor de les descàrregues d'igual a igual (*peer to peer*) en va motivar la redefinició en la Directiva d'harmonització de drets d'autor.

Reproducció és, a partir de la Directiva, qualsevol forma de còpia total o parcial, directa o indirecta, provisional o definitiva.

Un concepte de *reproducció* com aquest, sens dubte, buida de contingut gran part de la resta de conceptes (*comunicació pública* i *distribució*; en aquest sentit, García Albero). La distribució inclou la posada a disposició de l'original mitjançant la venda o qualsevol altra forma, cosa que posa en dubte la necessitat del suport físic. Finalment, la comunicació pública s'estructura en la Directiva entorn de l'accés simultani d'una pluralitat de persones, amb independència de la manera, el moment o el lloc que triïn per a l'accés.

Els programes d'ordinador i les bases de dades, íntimament lligats a l'evolució tecnològica, van aconseguir, segons s'ha vist, nivells de tutela extraordinaris. L'explotació econòmica de l'obra –sobretot l'audiovisual– es reforça també de manera considerable amb la redefinició dels conceptes bàsics de *reproducció*, *comunicació pública* i *distribució*.

Des del pla objectiu, no hi ha cap dubte ja de la rellevància penal de les conductes que més greument estan erosionant els drets d'explotació de l'obra.

Amb relació a l'ús de tecnologies d'igual a igual per a la descàrrega d'arxius musicals o de vídeo (fonamentalment), atès que la reproducció típica es conforma amb la reproducció parcial, tant la descàrrega com la càrrega en xarxa (*upload*) constituirien reproducció prohibida, ja que mentre que l'obra és a la part de disc dur de l'usuari disponible per a penjar (*upload*), aquesta estarà essent objecte continu de descàrrega. A més, no és necessari que l'obra es descarregui totalment per a entendre'n perfeccionada la reproducció, ja que aquesta pot ser parcial. I el que és més important, com que la reproducció pot ser directa o indirecta, s'habilita un fonament per a la responsabilitat penal del proveïdor de serveis d'Internet (*Internet service provider*, ISP) que posa els servidors a disposició dels programes d'intercanvi per a la recerca d'obres audiovisuals. En aquests casos i encara que el concepte de *reproducció* amb prou feines deixi espai per a l'aplicació d'altres verbs típics, el cert és que qui intercanvia obres protegides per les xarxes de parells també comunica públicament l'obra, ja que l'està posant, mitjançant el sistema de càrrega i descàrrega simultània, a disposició d'una pluralitat de persones.

Conductes de reproducció il·lícita

Altres conductes no menys importants encara que amb diferent impacte econòmic, com el *deep linking* o el *framing*, no es poden sostreure ja a la *vis atractiva* de la nova regulació: l'oferiment en xarxa de pàgines alienes com si fossin pròpies implica una reproducció il·lícita que, si a més és precedida d'un ànim d'explotació comercial, deriva en conducta penalment rellevant. Idèntica sort juridicopenal corre el fenomen "manter" o de venda a la manta (*top manta*): a la reproducció inicial de l'obra d'un tercer s'uneix aquí la distribució d'exemplars físics de la còpia il·legalment obtinguda, de manera que es duu a terme la totalitat dels elements de la infracció penal.

Però la vinculació de l'article 270 CP amb la normativa extrapenal obliga, a més, a una integració del concepte de *lucre*. No n'hi ha prou amb la projecció d'elements només objectius.

La còpia privada constitueix una infracció de la normativa civil quan no es destina a l'ús privat del copista.

La denominada *excepció de còpia privada* s'erigeix així en garantia de remoció dels obstacles per a l'accés a la cultura. Però la còpia privada per a ús privat del copista es pot qualificar així quan no vingui acompanyada d'un ànim d'explotació comercial. En cas que s'interpretés l'ànim de lucre de l'article 270 CP com a simple estalvi per al consumidor del que no ha de pagar per l'obra, el Codi estaria sancionant penalment allò que el TRLPI valora encara positivament en exceptuar del dret exclusiu del titular dels drets d'explotació de l'obra l'autorització d'aquesta còpia (*in extenso*, García Albero). La Fiscalia General de l'Estat ha adoptat aquesta posició a la Circular 1/2006 sobre els delictes contra la propietat intel·lectual.

De l'anterior s'extreu com a conseqüència que la denominada *penjada* (*upload*) de l'obra, és a dir, la posada a disposició del públic sense exemplars físics, realitza formalment el concepte de *reproducció*, però no es pot entendre en manera jurídica penalment rellevant en no presentar-se ànim d'explotació comercial de l'obra, que queda emparada per l'excepció de còpia privada. Tampoc la comunicació pública que aquesta posada a disposició d'un conjunt d'individus significa no duu a terme l'element subjectiu de l'injust present en l'article 270 CP, ja que la comunicació feta no tendeix a l'obtenció d'una contraprestació econòmica. En idèntic sentit, la baixada (*download*) de l'obra implica una reproducció parcial durant la descàrrega i total en finalitzar, però amb un ànim de lucre inexistent.

b) L'elusió de mesures tecnològiques

El Conveni del Consell d'Europa recull en l'article 6 una llista extensa de conductes que els estats membres han d'incorporar a la seva legislació penal interna per a evitar l'elusió de les mesures tecnològiques interposades per a la protecció d'obres. En realitat, l'article 6 del Conveni va més enllà de l'estricta tutela de la propietat intel·lectual i refereix les conductes prohibides a altres àmbits, com les defraudacions o els accessos il·lícits a sistemes d'informació.

La Directiva d'harmonització dels drets d'autor proposa una tutela específica de les mesures tecnològiques en l'àmbit de la propietat intel·lectual que pràcticament configura un bé jurídic mereixedor de tutela diferent de la propietat intel·lectual en si mateixa considerada.

Les mesures tecnològiques i la tutela jurídica que se'ls dispensa són en realitat l'últim (o el primer, segons es miri) dels bastions de la indústria en la batalla per l'equilibri entre el dret a l'explotació de l'obra i l'accés raonable de la població a la cultura. La digitalització de l'obra audiovisual multiplica el risc de còpia, pública o privada (aquí les excepcions no són, precisament, la referència que cal tenir en compte), per la qual cosa s'imposa com a mesura d'autoprotecció l'adopció de cauteles tecnològiques. Però l'experiència demostra que a cada mesura tecnològica d'autoprotecció li succeeix una contramesura tendent a anul·lar-la o fer-la ineficaç, per la qual cosa s'ha imposat en l'àmbit internacional la protecció de les mesures tecnològiques en si mateixes considerades, cosa que anticipa la tutela del bé jurídic o en genera un altre de dimensions diferents.

De les possibles modalitats de protecció tecnològica de l'obra (mitjançant control d'accés, marques d'aigua, gestió de drets –*electronic copyright management system* [ECMS], *electronic right management system* [ERMS], etcètera– i sistemes anticòpia *stricto sensu*), la Directiva no selecciona modalitats específiques, sinó fórmules elusives de mesures tecnològiques, la qual cosa implica que els operadors de la indústria es poden decantar per un ús exclusiu o alternatiu de les mesures, de manera que totes s'han de sotmetre a la tutela de l'ordenament.

Davant la redacció prolixa del Conveni, la Directiva opta per la sanció de:

> i) l'elusió de mesures sabent o amb motius per a creure que amb elles s'està eludint, i ii) les conductes de mera fabricació, distribució, possessió, etcètera, d'elements tecnològics tendents a promocionar l'elusió, circumscrivint aquesta fabricació, distribució, etcètera, a finalitats comercials o hipòtesis d'ús comercial limitat.

Doncs bé, l'article 270.3 CP també castiga amb la mateixa pena que per al cas d'infraccions dels drets de propietat intel·lectual, la fabricació, posada en circulació i tinença de qualsevol mitjà específicament destinat a facilitar la supressió no autoritzada o la neutralització de qualsevol dispositiu tècnic que s'hagi utilitzat per a protegir programes d'ordinador o qualsevol altra obra protegida.

Òbviament, l'article 270 CP avança la barrera de protecció penal, però sorprèn, de tota manera, que s'estengui fins i tot a la fabricació (acte preparatori d'un acte preparatori o, pel cap alt, si s'entén que la càrrega del programa equival a la seva reproducció, d'una temptativa) i a la tinença, quan la majoria d'accessoris destinats a l'obtenció dels codis d'accés a l'engegada d'un programa, o bé tenen diverses possibilitats aplicatives (*kits*), o bé es poden usar per al descobriment de continguts il·lícits, és a dir, en tot cas, no en la vulneració de drets d'autor (tecnologies de doble ús).

Fabricació, tinença o posada en circulació

De la dicció del precepte, en la redacció original del CP 1995, s'havia d'extreure com a conclusió que el que havia d'estar encaminat directament a facilitar la supressió o neutralització dels dispositius no era el mitjà, que podria tenir com a finalitat aquesta i diverses més (neutralitat tecnològica), sinó la fabricació, tinença o posada en circulació. Això era indicatiu no solament que s'havia d'atendre factors objectius que indiquessin

que aquesta era la intenció final del subjecte, sinó de l'existència d'un grau de perill més gran que arrela en la intenció de l'agent, i no en la sola característica del mitjà.

La reforma operada per la LO 15/2003 introdueix un matís a la redacció i deriva la destinació específica no ja a la voluntat de l'agent, sinó al mitjà en si mateix. La modificació tan sols –però, alhora, ni més ni menys– modifica l'objecte de la finalitat específica: si anteriorment el que havia d'estar específicament destinat a alguna cosa era la tinença, fabricació o posada en circulació dels mitjans, ara el que ha d'estar específicament destinat a la supressió no autoritzada és el mitjà en si mateix. I si es té en compte que en la immensa majoria dels casos estarem davant de tecnologies de doble ús, és difícil arribar a subsumir cap conducta en aquest precepte.

c) La tutela penal d'altres serveis d'accés condicional

Les dificultats de l'article 270.3 CP, juntament amb les exigències derivades de la Directiva de serveis d'accés condicional, han obligat el legislador espanyol a modificar l'article 286 CP i a introduir normes penals adreçades a la tutela dels serveis d'accés condicional i, de manera una mica confusa, a la tutela dels equips de telecomunicació.

L'article 286 CP planifica una línia d'intervenció que inclou des de la informació amb incitació de la manera com es pot burlar un sistema d'accés condicional com a estadi més allunyat del bé jurídic (art. 286.3 CP), fins a la utilització, per un usuari final, dels programes o equips que permeten burlar els sistemes d'accés condicional (art. 286.4 CP), passant, a tall d'estadi intermedi, per la facilitació de l'accés intel·ligible als serveis d'accés condicionat, mitjançant les conductes descrites en l'article 286.1.1 i 2 CP.

L'ambició del legislador penal i l'obsessió per no deixar-se res fora dels tipus penals provoquen aquest tipus de preceptes en els quals la participació es torna impossible perquè tot és autoria i la consumació és innecessària perquè la temptativa és el moment final de la conducta. En aquesta voràgine de conductes, el legislador no repara que està tipificant la facilitació de l'accés intel·ligible a un servei d'accés condicionat mitjançant la mera possessió d'un equip o programa no autoritzat.

Les conductes de mera possessió difícilment poden ser facilitadores si el fet desvalorat consisteix només i exclusivament a tenir, la qual cosa demostra que la intenció del legislador no és obtenir una cobertura justa del fenomen de la pirateria de serveis, sinó emprar simbòlicament el dret penal per a aconseguir un efecte intimidador amplificat. D'això és conscient el legislador quan, en el paràgraf tercer, incrimina la revelació o comunicació al públic de la manera com es pot aconseguir la vulneració de la condició incorporada al servei, que així redactat hauria significat una limitació desproporcionada de la llibertat d'informació i comunicació. Per això, s'incorpora una conducta acumulativa ulterior (no alternativa) a l'anterior, que consisteix a incitar els usuaris a aconseguir, conforme a les instruccions revelades, l'accés al servei obviant les condicions imposades pel seu prestador.

5. Responsabilitat penal dels prestadors de serveis d'Internet (ISP)

Abordem a continuació la controvertida qüestió de la responsabilitat dels prestadors de serveis d'Internet en el pla penal.

5.1. Introducció

La incertesa que genera l'expansió d'Internet com a mitjà encara carregat d'un cert grau d'anarquia en la seva gestió es projecta igualment sobre el paper que exerceixen els diferents operadors de la Xarxa. En canvi, el desenvolupament actual de la societat de la informació, basat en la utilització de les TIC, reclama regles de joc precises en l'intercanvi de dades, en general, i en el flux de dades, entès, a més, com a prestació de serveis, activitat econòmica, negoci, etcètera. El marc d'actuació ha de ser precís i els límits en l'actuació dels operadors també, no solament com a garantia dels consumidors quan es tracta d'operacions de caràcter comercial, sinó, més àmpliament, com a garantia de la totalitat de béns jurídics que poden entrar en col·lisió i del funcionament eficaç del sistema mateix de comunicació. El règim de responsabilitat dels diferents operadors de la societat de la informació ha de ser, en conseqüència, diàfan i ha d'evitar així que els problemes derivats de la innovació tecnològica s'acumulin a la incertesa jurídica.

L'especial arquitectura d'Internet determina que les relacions entre els diferents intervinents en la comunicació, la posició de domini o no de cadascun d'ells, la diversa capacitat d'emmagatzemament i la utilització posterior de continguts aliens reclamin regles específiques per determinar el grau de responsabilitat que pot assolir cadascun quan algun dels interessos en joc entra en situació de risc. Per això, la determinació dels límits de la responsabilitat penal al si d'Internet constitueix un tema de gran interès en el binomi dret penal - noves tecnologies.

La circulació en xarxa d'informació que excedeix els límits de les llibertats fonamentals (llibertat d'expressió i informació) per a atacar algunes altres d'igual importància (honor, llibertat sexual, seguretat), ha despertat des d'un primer moment l'alarma social, en la qual, com s'ha assenyalat, els mitjans de comunicació tenen un paper d'una importància extraordinària per l'efecte amplificador tant de la rellevància de certes conductes lesives com del grau de responsabilitat exigible als operadors (Widmer/Bähler, Picotti). De qualsevol manera, continguts sexuals indiscriminats i preocupació del col·lectiu han estat, en primer terme, els ingredients fonamentals per a procedir a l'anàlisi amb detall del repartiment de responsabilitats en l'ordre penal.

L'exigència de responsabilitat penal als prestadors de serveis de la societat de la informació, especialment als qui operen en l'àmbit d'Internet, a partir de qualsevol dels mitjans tècnics que ho permeten (cable, telèfon, etcètera), no és, tanmateix, exempta de preocupació política, en general, ni politicocriminal, en particular.

Els operadors, tant els que proveeixen l'accés al servei com els que faciliten la difusió de continguts allotjats als seus servidors, compleixen sens dubte una funció juridicosocial i econòmica de primera magnitud. En el primer sentit, com a facilitadors de la lliure difusió del pensament i les idees, de manera que contribueixen a una distribució més gran del coneixement i l'accés a la informació, en general. En el segon sentit, també és innegable el paper econòmic important que exerceixen els serveis telemàtics en la denominada *nova economia*, per la qual cosa l'esclariment definitiu dels límits en els quals s'ha de desenvolupar l'activitat del prestador del servei és singularment important, quan mostra en positiu les finalitats de política general perseguides amb la utilització de noves tecnologies (àmpliament, Sieber, Zencovich, Formasari i Picotti).

En aquesta tasca, a més, la depuració de responsabilitats s'ha d'enfrontar amb la distinció de la multiplicitat d'operadors de què disposa Internet. Evidentment, no planteja cap problema especial l'autoria de conductes lesives fetes en l'àmbit de la xarxa de xarxes, la responsabilitat de les quals s'entén a títol d'autor pels continguts propis. En canvi, els problemes se succeeixen quan es tracta d'esbrinar la rellevància penal de les accions o omissions d'altres intervinents en la comunicació, com en el cas dels prestadors d'accés a la Xarxa i dels serveis d'allotjament, etcètera.

Responsabilitat penal dels prestadors de serveis d'Internet

Han de respondre el proveïdor d'accés i de servei jurídic penalment pels continguts il·lícits aliens? I en tot cas, ha de respondre el proveïdor d'accés igual que aquell que difon la informació il·lícita o aquell que des de la Xarxa pirateja el programari d'un tercer? I el proveïdor de serveis?

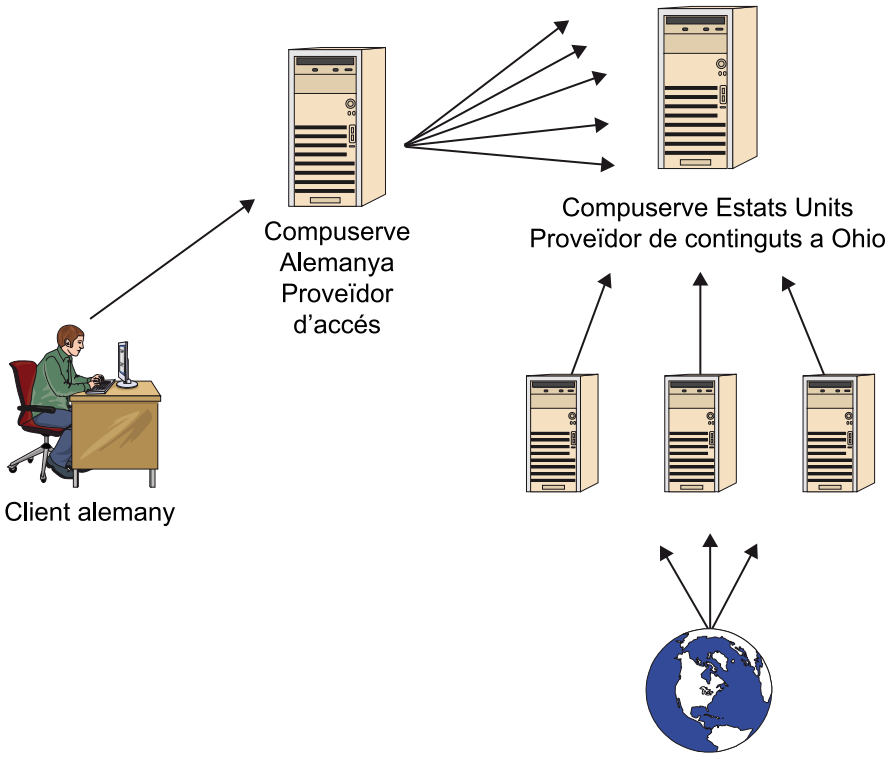
L'adjudicació de responsabilitats per continguts aliens transcendeix la política general, i les dificultats i el cost econòmic inherents a l'adopció de mesures tècniques eficaces i l'assumpció de posicions genèriques de garantia sobre la licitud del tràfic de dades circulant repercuteixen en la configuració dels serveis telemàtics, ja que obligant els operadors a l'assumpció de funcions amb capacitat d'afectació de béns jurídics aliens es presumeix, en primer lloc, una qualificació especial en l'agent que el capacita per a efectuar una censura prèvia de continguts que, en funció de les circumstàncies de pressió social, pot significar una limitació desmesurada de la llibertat d'expressió (àmpliament, Fornasari). Però és que, en segon lloc, es condiciona el mercat dels prestadors de serveis de manera que se'n concreten els requisits de capacitació.

El flux de dades, d'altra banda, es veu sotmès a límits tècnics la possible realitat dels quals pot ser poc menys que utòpica, ja que el control de la informació depèn en darrer terme de la instal·lació de sistemes de rastreig de la informació que es pot considerar il·lícita o lesiva d'interessos aliens, quan no, simplement, irreal.

Pena de dos anys de presó al proveïdor de servei per difusió de pornografia infantil

No falten, sens dubte, casos en els quals s'ha plantejat la responsabilitat penal del proveïdor de servei. El maig de 1998, el Tribunal Superior de Munic condemnava un proveïdor alemany a la pena de dos anys de presó per difusió de pornografia (delicte segons els casos, a Alemanya) a títol d'autor, malgrat que el subjecte en qüestió no era l'autor material de les notícies sobre pedofília difoses –gràcies al seu servidor– en el grup de notícies (alt.pedophilia.sex). L'administrador del servei era responsable de l'empresa Compuserve Deutschland, filial al 100% de la matriu Compuserve America, el servidor general de la qual era a la Universitat d'Ohio.

L'administrador del sistema disposava, doncs, de l'exclusiva d'accés als continguts que la matriu difonia des dels Estats Units, però no es trobava tècnicament capacitat per a tancar l'accés només a un o diversos dels continguts oferts per la matriu, com ho demostra el fet que, al primer requeriment de la policia per a la suspensió de pedophilia.sex, l'autor va suspendre d'immediat aquest grup de notícies i, alhora, uns tres-cents grups més que s'hi trobaven lligats (en profunditat, Sieber). El supòsit es pot descriure gràficament com segueix:



5.2. Règim jurídic penal aplicable als ISP per continguts aliens

Els interrogants apuntats anteriorment, juntament amb la proliferació de supòsits en els quals la resposta del prestador de serveis quedava sota sospita, van determinar, en el pla internacional, la promulgació de la Directiva 2000/31/CE del comerç electrònic. El text de la Unió Europea recull les regles sota les

quals es pot fer respondre al prestador de serveis per danys causats per tercers. Es tracta d'una estructura basada en la regla de l'exempció de responsabilitat, sobre la qual es construiran posteriorment un conjunt d'excepcions.

La Directiva del comerç electrònic va ser traslladada al nostre ordenament jurídic mitjançant la coneguda Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i el comerç electrònic (LSSICE).

La LSSICE trasllada literalment el règim general d'irresponsabilitat de l'ISP i les seves exempcions, amb alguna peculiaritat amb relació al coneixement que ha de tenir aquell respecte a l'il·lícit fet pel tercer, però no conté previsions penals. A falta de normes penals específiques sobre això, la delimitació de la responsabilitat penal dels proveïdors d'Internet (*access-service providers*) s'ha assajat des de l'aplicació de les categories i instituts generals de la disciplina i prenent com a referent les normes específiques que regulen la responsabilitat general i específicament juridicopenal en altres àmbits de la comunicació, com la premsa, ràdio, televisió, cable o satèl·lit.

Les vies que poden arribar a oferir instruments dogmàtics satisfactoris per a l'anàlisi de possibles responsabilitats en l'actuació del proveïdor de serveis que allotja en el seu servidor continguts il·lícits, es redueixen pràcticament a l'ús de la clàusula de comissió per omissió de l'article 11 CP i, atesos els límits de legalitat a què l'aplicació de la comissió per omissió se sotmet, a la participació criminal en el delicte. Són precisament els requisits inherents a l'article 11 CP els que van motivar en un primer moment la cerca d'analogies entre l'actuació dels prestadors d'accés i serveis d'Internet i la desenvolupada pels professionals dels mitjans de comunicació "tradicionals", per aquest motiu més àmpliament regulats. Vegem separadament ambdues fórmules.

5.2.1. Les possibilitats d'aplicació de l'article 30 CP

En el context tecnològic en el qual l'activitat dels actors d'Internet es desenvolupa i amb caràcter previ a la promulgació de la Directiva del comerç electrònic, alguns països del nostre entorn han tractat d'estendre el règim jurídic de la premsa escrita o, fins i tot, el d'un altre tipus de mitjans de comunicació (emprant aquí el terme convencionalment), a l'activitat desenvolupada a Internet, experiment àmpliament rebutjat per la doctrina (Zencovich, Riccio, entre d'altres) i la jurisprudència i que tampoc no és acollit en la Directiva.

Cas Cubby Inc. contra Compuserve

És interessant el cas Cubby Inc. contra Compuserve, recollit per Magni/Spolidoro. Davant una presumpta difamació efectuada per un tercer a partir d'un grup de notícies allotjat en un servidor, el tribunal va entendre que l'equivalència de l'ordinador central (*host*) no es trobava tant en la figura de l'editor, encarregat de la supervisió de totes i cadascuna de les informacions publicades, com en la d'un venedor de llibres, a qui seria absurd reclamar un deure de control dels continguts que ven.

Una aposta similar al nostre país dóna un resultat igualment rebutjable, per raons en abstracte semblants, i només diferents amb relació a la terminologia emprada en la normativa sectorial de telecomunicacions (d'una altra opinió, Gómez Tomillo). La Llei 14/1966, de 18 de març, de premsa i impremta, àmpliament derogada després de l'entrada en vigor de la Constitució, regula, bàsicament, tal com es desprèn del que es disposa al llarg del capítol II, l'activitat de difusió a partir d'impresos, que s'entén com "la reproducció gràfica destinada, o que es pugui destinar, a ser difosa". L'amplitud d'aquesta definició és després delimitada per la classificació dels impresos en publicacions unitàries i periòdiques; les primeres comprenen "els llibres, fullets, fulls solts, cartells i altres impresos anàlegs", mentre que les segones estarien integrades per "seminaris i aquelles altres que, en general, apareixen en qualssevol períodes de temps determinat".

La premsa escrita, doncs, difereix de la comunicació establerta a Internet ja en la definició mateixa del seu objecte, que es limita a la versió impresa de les comunicacions difoses en el mitjà i que, a més, ha de respondre, segons es desprèn de l'article 9 de l'esmentada Llei de premsa, a uns requisits formals en funció de la periodicitat de la publicació, novament circumscrita a la versió en paper. D'això es poden extreure ja algunes conseqüències, no per òbvies, innecessàries: d'una banda, de les possibles analogies entre el sistema d'Internet i la premsa, no es pot diferir *in totum* el règim de responsabilitat (i, específicament, el penal) previst per a aquesta sobre aquella; de l'altra, la comunicació via Internet, segons el model analitzat, no respon en sentit estricte a la idea de difusió, no almenys en alguns dels serveis a partir dels quals poden ser dutes a terme determinades accions de caràcter delictiu, per la qual cosa la projecció del règim de la premsa escrita a l'anomia regnant a Internet deixaria òrfena de tutela un ampli ventall de conductes –de gran importància– dutes a terme a la Xarxa.

Allà on la difusió és la funció principal exercida o que és capaç d'exercir el servei concret de què es tracti, la submissió d'Internet a la legislació de premsa, almenys juridicopenalment –i, per relació, tampoc civilment– no és satisfactòria, fins i tot encara que es pretengui l'equiparació no ja des del concepte de *difusió* o les analogies entre Internet i la premsa, sinó des de la idea de *mitjà mecànic de difusió*.

En efecte, el règim dissenyat en el capítol X de la Llei remet la depuració de responsabilitats penals al que disposa l'article 15 CP 1973, que es correspon, en el que és fonamental, amb l'article 30 CP 1995. És difícil trobar les similituds entre premsa i Internet si es té en compte que el supòsit per a l'aplicació d'aquest precepte és la realització de delictes o faltes "utilitzant mitjans o suports de difusió mecànics". Davant l'opinió generalment acceptada que l'ús de l'expressió *mitjà de difusió mecànic* permet la incorporació de qualsevol sistema diferent de la pura comunicació oral intersubjectiva no auxiliada de cap

suport, inclosa tota innovació tècnica que permeti la difusió, fins i tot més enllà de la premsa escrita, ràdio i televisió (Quintero), es poden efectuar algunes precisions (amb amplitud, Montero):

En primer lloc, alguns serveis de la societat de la informació, com la transmissió punt a punt, encara que multifreqüent, són exclosos legalment des del seu règim jurídic sectorial del concepte de *difusió*, la qual cosa fa innecessària la conceptualització del mitjà tècnic com a mecànic, ja que, en tot cas, no ho serà de difusió, encara que la informació, en sentit ampli, sigui difosa per aquest mitjà.

En segon lloc, el concepte de *mitjà mecànic* és referit des de la interpretació gramatical a estructures complexes energèticament alimentades, a un conjunt d'estructures interdependents que funcionen per si mateixes. Internet, en canvi, permet el tràfic d'informació d'una manera específica; precisament, la consignada en el gràfic. És un mitjà tècnic, no mecànic. Des d'un punt de vista hermenèutic basat en la història de l'article 30 CP és evident que va ser creat per a garantir la depuració de responsabilitat en els nous mitjans de difusió de notícies basats en la mecànica –comprometent al mínim la llibertat d'expressió (Vives)–, no en la tècnica, com ara la premsa, que requereix un sistema mecànic complex de creació de planxes, injecció de tinta, assecatge, etcètera, per a la difusió posterior de la informació. Per aquest motiu, la sistemàtica del precepte fa referència a les maneres de gestió conegudes de la premsa escrita, ni tan sols adaptable a la realitat de la ràdio i televisió, i molt menys a la realitat d'Internet.

En aquest punt, es pot efectuar una precisió sobre el que disposa l'article 823 bis de la Llei d'enjudiciament criminal (LECrim), d'acord amb el qual el procediment especial per a l'enjudiciament dels delictes comesos mitjançant la impremta també ha de ser aplicable a l'enjudiciament dels delictes comesos per mitjans sonors o fotogràfics, difosos per escrit, ràdio, televisió, cinematògraf o altres similars, i estén a tots ells les regles de responsabilitat excloent i subsidiària de l'article 30 CP. Aquest precepte, tal com veurem a continuació, no es pot estendre al règim d'Internet. La clàusula de comparació analògica "o altres similars" obliga a fonamentar l'equivalència, no solament del mitjà, sinó del rol exercit pels diversos actors. Però Internet escapa no solament de la lògica de la premsa, sinó fins i tot de la d'altres mitjans sonors o de ràdio o televisió. En efecte:

- L'activitat d'un diari és limitada, quant a la informació que conté, si és que es vol ser fidel al concepte de *publicació periòdica*, ocupa un espai físic, de manera que la informació de la qual es pot fer responsable al director ha de ser limitada necessàriament, prou per a fer-li exercir el rol de director, sobretot quan la nomenclatura de l'article 30 CP no pot ser formalment entesa, sinó referida a l'acompliment de rols específics.

- Contràriament, la informació capaç de ser difosa a Internet, perquè és il·limitada, impedeix l'acompliment d'un rol pròpiament parangonable al de director d'una publicació, excepte en els casos en els quals l'activitat desenvolupada a partir d'aquest mitjà coincideix exactament amb el sistema de publicacions periòdiques. Però la subsumpció en el concepte de *mitjà mecànic de difusió* per aquest motiu, ignorant els apuntats anteriorment, incorreria en confusió *pars pro toto*, ja que la publicació periòdica no és característica essencial de la Xarxa. I és que el règim excepcional de responsabilitat de l'article 30 CP no s'ajusta a la dinàmica d'Internet, en què hi ha operadors difícilment enquadrables en aquest precepte, aliens, per tant, a les regles de subsidiarietat i exclusió que s'hi promocionen, i viceversa, subjectes sotmesos a l'abast de l'article 30 CP i que són desconeguts en el ciberespai.

Exemples d'operadors aliens al règim de responsabilitat de l'article 30 CP

Entre els primers es podria assenyalar els usuaris que, sense ser autors de les imatges que allotgen a les seves pàgines web amb la tècnica del *linking*, coneixen el contingut il·lícit que s'amaga en els enllaços de remissió, sense que se'ls pugui considerar directors de la publicació (la pàgina web, pròpiament, no ho és) o del programa (relatiu al moment i al rol exercit per un espai específic), la qual cosa tampoc no és vàlida per al servei web d'Internet. Entre els segons, es poden avançar els extraordinaris problemes d'identificació entre els operaris d'Internet de directors d'empreses enregistradores, emissores o impressores, necessitats per definició inexistents en aquell mitjà.

- La possible identificació entre els prestadors de serveis i algunes de les categories clàssiques de la difusió mitjançant la premsa escrita o altres suports *mecànics* s'esvaeix davant de principis d'exclusió de responsabilitat establerts en la Directiva del comerç electrònic, antagònics als que tradicionalment fonamenten la responsabilitat al si de la premsa escrita. S'ha de partir en tot cas, tal com estableix la Directiva en l'article 15, de l'absència de deures de vigilància i supervisió de les dades allotjades al servidor, totalment raonable quan la capacitat lògica d'un servidor de mitjà abast permet, amb la tecnologia actual, l'hostatge de milers de pàgines sota qualsevol dels protocols convencionals –que es multiplica, a causa de la tècnica del *linking*, des de pàgines allotjades en altres servidors, la qual cosa, sens dubte, pràcticament n'impossibilita el control real o eficaç.

  Ultra això, la cerca activa de continguts il·lícits o la supervisió general de les dades allotjades a l'ordinador central trobaria dificultats eticosocials serioses, ja que, davant de les diverses maneres de filtratge de continguts que es poden efectuar en un sistema de xarxa, significarien un control de l'activitat de tercers i una valoració sobre el seu caràcter lícit o il·lícit; el risc és, en aquest punt, evident.

  Si es té en compte el paral·lelisme d'Internet amb els sistemes de difusió de premsa i televisió, l'activitat d'inspecció del proveïdor hauria significat obertament l'establiment d'un sistema de censura difícilment compatible amb l'entorn. Com que la responsabilitat del director d'un mitjà de comunicació escrit es pot esglaonar pels continguts de tercers editats a la seva plataforma, la depuració de responsabilitat del proveïdor no admet la comparació: així, l'activitat que més fàcilment es podria assimilar a l'exercida, per exemple, pel director de l'empresa editora, és a dir, la del

prestador del servei d'emmagatzematge de dades queda exempta de responsabilitat sempre que aquest desconegui la il·licitud de l'activitat o actuï amb promptitud una vegada advertit d'això, i en qualsevol cas se l'eximeix de la necessitat de supervisió de continguts. O, de manera idèntica, en la mesura que la Directiva eximeix d'una obligació general de supervisió i/o cerca activa de continguts el prestador de serveis quan aquests consisteixin en l'arxivament de dades, està situant en esferes diferents operadors que analògicament serien assimilables, com el director de la publicació i el proveïdor del servei d'emmagatzemament.

- Finalment, el requisit de la capacitat tècnica per a la suspensió del servei a què es refereix la LSSICE per imperatiu de la Directiva, a més dels problemes de determinació que presenta davant de les diverses maneres de filtratge de continguts que es poden efectuar en un sistema de xarxa, pressuposa un control de l'activitat de tercers i una valoració sobre el seu caràcter lícit o il·lícit. La supressió o el filtratge de continguts es poden efectuar al si d'un diari escrit, atesa la limitació de continguts, mentre que a Internet (Seminara) poden implicar riscos seriosos per a la llibertat.

5.2.2. Responsabilitat per comissió activa a títol d'autoria o participació

Partint del que s'ha establert anteriorment, la (co)responsabilitat dels intermediaris de la societat de la informació pot ser depurada mitjançant les respectives figures de la part especial, imputades a títol de comissió, la qual cosa és possible en els casos en els quals el proveïdor desenvolupi un vertader fer positiu, més enllà de la simple facilitació d'un servei, és a dir, prenent part directa en l'execució del fet mitjançant la creació de continguts propis o la selecció dels aliens que hi seran difosos; això succeirà en els serveis de difusió per web (*webcasting*) o, d'una manera una mica menys evident, amb les llistes de distribució, en els casos en els quals el proveïdor desenvolupi el doble rol de proveïdor i difusor de continguts; és a dir, en els casos en què l'intermediari no solament presta el servei de difusió, sinó que assumeix la producció pròpia dels continguts.

Es tracta, en definitiva, d'intervencions positives en la delimitació dels continguts que formaran part del paquet d'informació del servei de multidifusió i/o polidistribució mitjançant llistes. Certament, l'acció desenvolupada pel proveïdor serà, en la majoria dels casos, producte de la infracció del deure de cura en la tasca de selecció de continguts, cosa que limita la punició per mitjà de la clàusula de comissió imprudent, però també l'abast d'eventuals tipus imprudents, atesa l'absència del deure de control de continguts (Morales García).

La imputació del fet al proveïdor del servei a títol de participació tampoc no està exempta de problemes. Sens dubte, si el prestador no té coneixement del contingut o, tot i tenir-lo, manca de mitjans tècnics per a la seva supressió

(especialment en els casos de provisió d'accés, en els quals, com en l'assumpte Compuserve, s'afirmava la impossibilitat d'aconseguir vetar únicament l'accés a un únic contingut), difícilment es pot convenir en una responsabilitat com a còmplice o partícip necessari, ja que el fet principal depèn íntegrament d'un tercer, sense que la seva aportació, en ajustar-se a l'exercici d'una funció determinada, pugui ser reprotxada. Diferent és el cas en el qual el proveïdor del servei decideix no retirar la informació o bloquejar l'accés a la informació, tot i poder-ho fer sense dificultat. En aquesta hipòtesi, els interrogants s'obren en un doble àmbit.

D'una banda, amb relació al possible esgotament del delicte, de manera que la participació de l'intermediari es limitaria a enervar o esmorteir els efectes del fet antijurídic. Davant l'opinió que el fet principal es trobarà en general consumat, atesa la classe d'accions típicament rellevants que es presentaran a la subsumpció del fet (difusió, comunicació, reproducció), són possibles dos fronts argumentals que afavoririen la incriminació del prestador com a cooperador necessari o còmplice. D'una banda, si el proveïdor coneix el contingut abans de permetre-hi l'accés, la seva aportació al fet pot ser qualificada de *cooperació necessària*, atesa la doctrina dels béns escassos o, fins i tot, la del domini del fet.

En aquest sentit, és interessant l'exemple recollit en les seves respectives obres per Picotti i Widmer/Bähler. En aquell cas, el Tribunal Federal Suís va confirmar la condemna per participació necessària activa del proveïdor d'un servei telefònic de contingut eròtic, prèviament advertit per l'Administració de Justícia suïssa perquè impedís l'accés als menors a aquest servei, encara que per a això n'hagués de suspendre l'activitat.

D'una altra banda, si, al contrari, no va tenir aquesta possibilitat, però adquireix coneixement posteriorment a la seva difusió, s'han de diferenciar diverses hipòtesis:

- Si el delicte és permanent quant a la seva consumació, el proveïdor hi pot respondre a títol de participació, sempre que el fet permeti la intervenció de tercers en qualsevol moment, previ a l'esgotament del delicte.

- Si el fet és de consumació instantània, el proveïdor no ha de respondre dels fets produïts anteriorment al seu coneixement.

- En canvi, el manteniment del contingut il·lícit (penseu en un delicte contra la propietat intel·lectual, per exemple, per reproducció del codi font d'un programari o comunicació pública d'aquest) permet la interrupció de la unitat de fet –on aquesta sigui present–, de manera que els actes posteriors, en tant que entra en joc un factor d'essencialitat en el manteniment de l'acció il·lícita, fossin constitutius d'un delicte nou pel qual l'ISP ha de respondre a títol d'autor.

De la reflexió anterior neix el segon problema, en el qual s'ha centrat actualment el debat jurídic penal europeu. Admesa la possibilitat de participar en el fet aliè mitjançant el manteniment de la prestació, cal determinar la manera

activa o omissiva en què es manifesta. Anteriorment a l'entrada en vigor de la LSSICE, la legislació extrapenal no assolia deures d'actuar de l'intermediari, per la qual cosa la imputació a títol omissiu era complexa, atesa la clàusula d'incriminació del delicte omissiu del dret espanyol (succeeix el mateix en l'italià i l'alemany). Per això, només quan es presentaven aquests supòsits era factible el recurs al dret penal per als casos en els quals el prestador de servei es limita a no impossibilitar la connexió al contingut o a no retirar-lo, quan en té coneixement.

Des d'aquestes premisses, un sector doctrinal va entendre que el manteniment del servei quan l'intermediari coneix la il·licitud dels continguts allotjats al servidor constitueix una contribució objectiva al fet aliè en la qual no són possibles excepcions a les regles generals de participació activa. O, el que és el mateix, no fa falta recórrer a l'omissió. L'automatització del servei no seria llavors un obstacle per a la verificació d'una conducta de cooperació necessària activa, en la qual, de tota manera, es presenten accions positives adreçades al manteniment, fins i tot automatitzat, d'aquest servei i que actuen a tall de concausa o *conditio sine qua non* del resultat típic. Davant això s'ha oposat la desconnexió, en termes d'imputació objectiva, entre la conducta de l'intermediari i el resultat típic derivat en tot cas de la conducta de l'autor, risc, en conseqüència, només jurídicament imputable des d'estructures d'omissió.

5.2.3. Responsabilitat a títol de comissió per omissió

L'actuació del proveïdor, tanmateix, no sempre pot ser reconduïda a l'àmbit de l'actuació positiva, almenys des del punt de vista de la rellevància penal de la seva acció (amb estructura causal). Això succeirà amb claredat especial en la pura facilitació d'accés a la Xarxa, en l'allotjament de pàgines alienes, i també en la gestió de grups de notícies no moderats i del correu electrònic i, de manera diferent, segons s'analitzarà més endavant, en els grups moderats per l'intermediari, la informació cursada mitjançant llistes de distribució i la difusió per web.

En la prestació dels serveis exposats en primer lloc, els judicis d'imputació del resultat respecte a l'acció de l'autor de la informació o les dades i de l'intermediari se situen en plans diversos mancats de connexió jurídica, novament llevat d'infracció de la prohibició de tornada, imputant *ad infinitum* a partir d'estructures causals o d'equivalència de les condicions. Així, doncs, en si mateix considerat, el fet de proveir la infraestructura tècnica o l'allotjament de continguts manca de rellevància jurídica, reafirmada pels criteris exposats en la Directiva del comerç electrònic, de manera que la cerca de criteris d'imputació únicament podria discórrer al si de l'omissió de deures de control específics, sobre la prohibició dels quals la LSSICE, d'acord amb la Directiva del comerç electrònic, és clara. La qüestió és una mica diversa en el segon grup de

supòsits, ja que hi convergeixen formes actives (supervisió i control, per exemple) i el seu anvers (absència de control o supervisió quan prèviament s'han pres decisions positives respecte, per exemple, als continguts seleccionats).

En aquest cas, el concepte d'*omissió* del qual es parteixi, el criteri d'equivalència amb la *causació activa del resultat* que es manegi, i el sentit i l'abast de les posicions de garantia descrites en l'article 11 CP, són fonamentals per a la fixació de les bases sobre les quals fonamentar la possible coresponsabilitat de l'intermediari en cadascuna de les modalitats delictives que inclou Internet. Aquesta via requereix, doncs, la possibilitat que el fet concret pugui ser dut a terme, en funció de l'estructura típica de referència, de manera omissiva, per a la qual cosa la figura delictiva concreta ha de participar d'una estructura de resultat (és a dir, on el tipus penal prohibeixi la causació d'un resultat).

Per a aquells casos en els quals l'estructura del delicte no impedeix la realització del fet en comissió per omissió i, en qualsevol cas, per a les conductes de participació via d'omissió i pressuposats el coneixement de l'activitat il·lícita desenvolupada per mitjà del servei tècnic prestat i el seu manteniment dolós, resta encara per aclarir la presència de deures jurídics d'actuar, afirmats els quals es pot efectuar el judici d'equivalència entre la causació activa del resultat i la seva no-evitació. S'han de diferenciar novament els diversos serveis desenvolupats pels intermediaris al si de la societat de la informació i, particularment, d'Internet:

- Amb relació a la simple transmissió de dades, la Directiva del comerç electrònic tan sols reflectia situacions en les quals no es podria ventilar de cap manera la responsabilitat del proveïdor, i també d'altres tantes de no incloses per aquesta prohibició. En aquest cas, no es pot inferir, al contrari, l'existència d'obligacions legals d'actuar, per la qual cosa la clàusula de l'article 11 CP s'endevina en aquest cas d'aplicació impossible a supòsits en els quals el simple transmissor no eviti, per exemple, la circulació per les seves xarxes d'informació lesiva de drets de propietat intel·lectual, la qual cosa, d'acord amb la filosofia que inspira la Directiva, sembla encertat. Fora d'això, els supòsits recollits en l'article 14.1 LSSICE no es refereixen pròpiament a la pura transmissió de dades alienes, sinó que contenen supòsits d'actuació a títol propi, especialment en clara referència a la selecció o modificació de les dades pel mateix intermediari; per aquesta raó, la responsabilitat es ventila, si escau, per la via de l'autoria activa.

- Qüestió diferent és la que s'esdevé en els supòsits d'allotjament de dades, potser els més problemàtics. Al mateix temps que la LSSICE eximeix l'intermediari de l'obligació de supervisió, imposa deures específics d'actuar una vegada comunicada a l'administrador del servei la presència de continguts il·lícits a l'ordinador central, o en aquells casos en els quals l'administrador els conegui per vies diverses a la comunicació de l'autoritat administrativa o judicial. Concretament, l'article 16.1.b LSSICE és el que se n'ocupa, amb la qual cosa, en descriure les vies de coneixement i les

accions que ha de prendre el prestador, s'estan incloent en el dret intern obligacions legals que posteriorment han de servir a la fonamentació de posicions de garantia, és a dir, que han de permetre acreditar la concurrència de deures jurídics d'actuar que, perquè s'ometen, són estructuralment equivalents a la causació activa del resultat material.

És a aquests deures als quals s'ha d'acudir per a fonamentar l'equivalència estructural entre acció i omissió, i no als supòsits de control d'una font de perill derivada de la realització d'activitats de risc, ja que això no es pot afirmar com a norma a Internet. L'acompliment d'una activitat en un context de perill pot comportar una obligació de control o de manteniment del perill en els termes autoritzats; tanmateix, no és correcte parlar d'Internet com a font de perill (Sieber i Picotti).

- Relacionats amb la depuració de responsabilitat penal del proveïdor d'accés o servei, hi ha els supòsits en els quals el titular d'una pàgina inclou en el contingut enllaços a pàgines amb continguts il·lícits, com, per exemple, pornografia infantil o continguts obertament injuriosos (Jofer).

El problema al nostre país torna a ser similar al que s'esdevé amb els proveïdors d'accés o de servei. Es tracta de delimitar si els continguts il·lícits (pornografia infantil, injúries, delictes contra la salut pública –per exemple, per distribució de fàrmacs–, etcètera) són d'alguna manera imputables a l'autor de l'enllaç o, al contrari, si la seva conducta queda impune. Evidentment, si la determinació de responsabilitat és complexa amb el proveïdor de serveis, fins i tot ho serà més en el cas de l'autor d'un enllaç. La solució variarà en funció de les diferents accions lesives.

En el cas de la comunicació pública, la reproducció, etcètera, d'obres sotmeses a drets de propietat intel·lectual, l'atribució de responsabilitat és dubtosa: des de la LSSICE, perquè no queda clar que l'usuari particular encaixi en el concepte de *prestador d'un servei de la societat de la informació*, per la qual cosa, en cas negatiu, no li podrien ser aplicables els articles relatius a la responsabilitat ni, en conseqüència, podrien fonamentar una posició de garantia legal o contractual.

En el cas de la difusió de pornografia infantil, n'hi hauria prou amb el coneixement del contingut del que s'ha difós per a poder entendre aquesta conducta enquadrada en el concepte de *facilitació de la difusió*, especialment en vista de la facilitat amb la qual tècnicament podria desprendre els enllaços expressament generats en pàgines de pornografia infantil, cosa que, en canvi, no seria exigible al prestador d'accés, encara que tingués coneixement que per la xarxa l'accés de la qual gestiona s'estan enviats continguts il·lícits.

En definitiva, és possible la realització del fet per part del prestador de serveis en comissió per omissió sempre que, coneixent la il·licitud (il·licitud, és clar, juridicopenalment rellevant, és a dir, infracció contra la propietat intel·lectual, etcètera) de les dades que allotja, que manté en la seva memòria cau o que

dirigeix per mitjà de motors de cerca o la incorporació d'enllaços en pàgines pròpies, tot i així decideixi mantenir la vigència dels continguts, bé no impossibilitant-hi l'accés, bé no suprimint-los del servidor.

5.2.4. Fonament jurídic penal de les situacions d'irresponsabilitat

La LSSICE, en els articles 16 i 17, estableix els requisits per a entendre concurrent el coneixement efectiu de la situació il·lícita. En particular, reclama a aquest efecte l'existència d'una resolució que declari la il·licitud o d'un requeriment de l'autoritat competent. Així mateix, es pot adquirir coneixement efectiu de la situació il·lícita en els casos en els quals l'ISP la conegui per mitjà de mecanismes establerts mitjançant els corresponents convenis que així ho reconeguin. Això condueix al fet que, en els casos d'absència de coneixement efectiu, l'ISP no pot ser responsable del contingut il·lícit. I això planteja, immediatament, una doble lectura: o bé estem parlant d'una previsió oberta, en la qual s'expressen les formes en què, en tot cas, s'entén la presència de coneixement efectiu sense descartar-ne d'altres, o bé són aquestes i cap més, les maneres com l'ISP pren legalment coneixement de la il·licitud.

En el primer cas, la prova del coneixement del contingut il·lícit per l'ISP conduiria a la imputació del delicte d'acord amb les regles anteriorment dibuixades. Això deixa obert, en canvi, el problema del frau eventual, de manera que el coneixement de la probabilitat que, amb la conducta exercida, s'estigui contribuint eficaçment a la producció d'un resultat danyós, també seria possible entre les formes de coneixement efectiu. Aquesta situació no sembla compatible amb els plantejaments originals de la Directiva, que en l'article 15 establia que el coneixement de fets o circumstàncies pels quals es pogués inferir la il·licitud del contingut podria donar lloc, com a molt, a una acció per danys i a perjudicis, per la qual cosa, si assumís la possibilitat de vies alternatives de coneixement de la il·licitud, entraria per la finestra allò que prèviament havia estat expulsat per la porta. I, encara que de manera menys directa, sembla que és aquesta la via seguida per la LSSICE en parlar de *coneixement efectiu*.

Sense prejutjar en aquesta primera opció quines són les vies d'accés al coneixement de la il·licitud, el cert és que el coneixement sembla que haurà de ser efectiu, és a dir, referit al contingut en si mateix, i no a judicis de probabilitat, com succeeix amb el frau eventual. Des d'aquesta opció, s'ha proposat excloure la responsabilitat de l'ISP quan tingui un coneixement de la perillositat eventual de la conducta que duu a terme amb relació a un determinat bé jurídic penalment protegit, acudint a les causes de justificació, en particular a partir de la circumstància setena de l'article 20 CP (Guardiola). En aquesta hipòtesi, s'entén que, en els casos en els quals es coneix realment però no efectivament, el frau es duu a terme en la seva integritat, però per qüestions politicocriminals

s'exceptua la sanció per al fet. Raons que, lògicament, s'haurien de buscar al si de la LSSICE i en el millor desenvolupament de la funció econòmica i social que duen a terme els ISP.

> Al nostre judici, tanmateix, el que succeeix és que no sorgirà el deure jurídic d'actuar de l'agent, ja que la LSSICE només l'obliga en aquestes hipòtesis. És a dir, l'obligació legal d'actuar de l'article 11 CP només sorgeix en aquells casos en els quals l'ISP actuï amb un coneixement que excedeixi la mera probabilitat. I la Directiva, encara més generosa amb les exempcions de responsabilitat, impedia la imposició d'obligacions de supervisió al prestador. De manera que, només en els casos en què el subjecte actiu prengui coneixement (el que li exigeix la LSSICE, és a dir, l'efectiu) de la il·licitud del fet (encara que aquest pugui provenir de més vies que les establertes en els articles 16 i 17 LSSICE), neix l'obligació legal d'actuar.
>
> Tingueu en compte que les hipòtesis de responsabilitat del prestador de serveis en els termes aquí discutits es refereixen sempre a continguts de tercers, per la qual cosa la seva conducta sempre és d'omissió de deures d'actuació (no fer-hi impossible l'accés, no retirar-los de la Xarxa, no adoptar mesures de comunicació a tercers, etcètera), ja que només l'omissió d'aquests deures després de la presa de coneixement està realment connectada en termes de risc amb la lesió al bé jurídic. En definitiva, l'estructura de la norma no varia i les exigències del frau de cada tipus penal són les mateixes; però en hipòtesi de frau eventual, no és possible fer néixer la posició de garantia en el prestador, ja que el seu deure d'actuar comença amb l'efectivitat del coneixement, i no abans.

El segon, en canvi, implica l'afirmació que la falta de coneixement efectiu en els termes dissenyats en els articles 16 i 17 LSSICE desemboca en la irresponsabilitat de l'ISP, encara que existeixi, de fet, coneixement real del contingut il·lícit o sense necessitat d'esbrinar si hi va haver o no coneixement real al marge de les vies exposades en la LSSICE.

Aquesta opció, que genera un amplíssim ventall d'impunitat ja que confon, en realitat, les raons de prova amb les raons substantives, és tanmateix en la base d'algunes resolucions judicials que van considerar innecessari aprofundir durant la instrucció penal en el coneixement real de la il·licitud una vegada descartat el coneixement per les vies descrites en la LSSICE.

> Així, en efecte, la Interlocutòria de 7 de març de 2003 dictada pel Jutjat d'Instrucció núm. 9 de Barcelona, en l'assumpte ajoderse.com, la resolució va decretar el sobreseïment lliure perquè no va quedar prou acreditat el coneixement efectiu de l'ISP d'acord amb les vies exclusives previstes en els articles 17 i 18 LSSICE i basant-se en un informe de la Brigada d'Investigació Tecnològica de la Policia Nacional en el qual s'indicava que no constava que el subjecte actiu hagués estat notificat de la il·legalitat del contingut o comminat a fer-hi impossible l'accés.

6. Retenció de dades de les comunicacions

El control de dades de tràfic de les comunicacions ha estat objecte d'atenció per la comunitat internacional durant els últims deu anys. La política criminal internacional i nacional ha patit oscil·lacions importants fins a desembocar en la Directiva 2006/24/CE, de 15 de març, sobre conservació de dades generades o tractades amb relació a la prestació de serveis de comunicacions electròniques d'accés públic o de xarxes públiques de comunicacions, i la Llei 25/2007, de 18 d'octubre, de transposició d'aquesta Directiva.

Les dades de tràfic de les comunicacions, com ho són les del contingut, tenen una transcendència especial per al curs de determinades investigacions criminals. Com que des de les dades de tràfic és possible la construcció de perfils d'identitat, qualsevol accés de tercers a aquestes dades ha de ser objecte d'una regulació escrupolosa. Però no s'ha de perdre de vista que una concepció excessivament bucòlica de les dades com a temple inaccessible del dret a la intimitat seria il·lusòria. De fet, seria tan ingenu com tractar de combatre a hores d'ara el valor de les empremtes dactilars en el curs d'investigacions policials o judicials. Convé, doncs, conèixer les oscil·lacions avançades anteriorment, a fi d'efectuar una valoració raonada crítica de la regulació vigent.

6.1. La retenció de dades en la Convenció del Consell d'Europa sobre cibercrim

La Convenció planteja un règim jurídic de preservació de les dades de les comunicacions més que raonable, que, tanmateix, no va ser així de raonable des de l'origen. En efecte, la primera versió de la Convenció, feta pública el 27 d'abril de 1999, preveia l'obligació de preservació de totes les dades de les comunicacions per un període no inferior a un any. En definitiva, els ISP, és a dir, els prestadors de serveis de la societat de la informació, quedaven obligats a registrar l'activitat dels usuaris i a emmagatzemar les dades resultants, amb el risc consegüent per a la intimitat i les dades personals dels usuaris, i el funcionament normal de les xarxes telemàtiques. Tanmateix, i igual que succeiria amb altres propostes de la Convenció relatives al règim de protecció de dades i, en particular, a la cessió de les dades obtingudes en el curs d'una investigació criminal a tercers estats part del Conveni, aquesta obligació resultaria finalment exclosa del text definitiu del tractat, principalment per falta d'acord entre la Unió Europea i el Consell d'Europa.

LA UE, amb la Recomanació 3/1999 sobre la conservació de les dades de tràfic pels proveïdors d'Internet, va expressar ja abans de la primera versió de la Convenció, feta pública pel Consell d'Europa, la seva oposició a mesures d'intervenció sobre el tràfic de dades. La Recomanació, elaborada pel grup de l'article 29 sobre la protecció de dades personals, va expressar la seva preo-

cupació respecte a l'arxivament de dades als diversos països membres de la UE. Conscient de la necessitat de controlar les dades que circulen per un servidor per tal de poder efectuar les tasques de facturació oportunes d'acord amb les dades demanades, el grup va tractar de conciliar, a més, les necessitats d'investigació criminal en temps real i la indemnitat dels béns jurídics subjacents.

De fet, el grup va considerar en la Recomanació que el fet que un tercer pogués arribar a tenir la informació derivada del tràfic de dades per mitjà d'un servidor implicaria una violació de dret fonamental, en general constitutiva de delicte, llevat que la mesura d'intercepció de la comunicació o el seu contingut complissin les exigències jurídiques típiques de l'afectació de drets fonamentals recollides en les diverses convencions sobre els drets de l'home, això és, proporcionalitat de la mesura, només adoptable en els casos en què no hi hagi altres mecanismes alternatius per al desenvolupament de la investigació, i un fonament clar per a la seva adopció, en el qual s'haurien de reflectir la durada, la finalitat, els mitjans tècnics que s'empraran i els límits de la intercepció.

Amb aquests antecedents, la Convenció va establir que la preservació de les dades de tràfic per al seu ús posterior al si d'una investigació de naturalesa penal havia de seguir un filtre de proporcionalitat d'acord amb la regulació interna de cada estat.

D'acord amb l'article 15 de la Convenció, la mesura de preservació de dades de tràfic continua reclamant un judici de proporcionalitat aplicable judicialment. Els estats han de poder aplicar mesures de retenció quan una investigació concreta i específica així ho requereixi. En aquests casos i només en aquests, s'ha de justificar que la preservació de les dades pot determinar l'acreditació definitiva de la comissió d'un fet constitutiu d'infracció penal. No es tracta, fixeuvos, d'una preservació operada per exigència legal, sinó d'una potestat legal sotmesa al filtre judicial de la proporcionalitat.

De fet, la mateixa Convenció ofereix als països signants l'oportunitat de decidir si volen aplicar la possibilitat de preservar dades de tràfic només en els casos dels delictes regulats en la part substantiva de la Convenció, a qualsevol figura que es pugui acomodar en el concepte de *delinqüència informàtica* o a qualsevol delicte que, tenint una pena greu, pugui ser susceptible de ser acreditat mitjançant una prova derivada de les dades preservades (art. 14 de la Convenció).

La Convenció es refereix sempre a preservació de dades, la qual cosa significa la conservació de les existents ja emmagatzemades, i no la de dades que es puguin generar en un futur. És obvi que les necessitats d'investigació penal i prevenció del crim organitzat i el terrorisme requereixen l'accés a dades de les comunicacions que serveixen de manera exponencial també a l'acció delictiva, com de manera exponencial serveixen també en l'escometiment d'accions lí-

cites. Així, doncs, de vegades, aquestes dades poden ser objecte de modificació o alteració si no s'actua ràpidament sobre elles una vegada es té coneixement que accedir-hi pot ser la fórmula d'acreditació del fet delictiu.

Íntimament unit a això i al judici de proporcionalitat que obliga a efectuar la norma, hi ha un altre element no menys important en la decisió de preservació: les condicions i garanties de la salvaguarda. Si el simple emmagatzemament genera un risc per a la intimitat que no ha de permetre actuacions de tall generalista, la seva adopció sobre la base de l'acreditació d'una necessitat certa i real s'ha de basar, a més, en condicions de preservació certes i segures. L'emmagatzemament de les dades preservades no es pot efectuar de manera que el seu accés sigui més fàcil per a tercers o augmenti el risc concret i real per a la intimitat del titular de les dades. En aquest sentit, la Convenció proposa dues grans mesures: el control jurisdiccional de la manera com les dades són objecte d'emmagatzemament i la imposició de deures de cura especials en la gestió i sigil en la comunicació.

Les dades preservades conforme a la proposta de la Convenció es poden emmagatzemar durant un període de noranta dies, renovables segons les circumstàncies concurrents. Es tracta d'un període raonable i suficient, coincident amb el judici elaborat pel grup de l'article 29 al seu dia per a justificar els períodes màxims d'emmagatzemament a efectes de facturació. Termini raonable, a més, perquè sobre aquestes dades, amb la supervisió judicial adequada, es pugui actuar amb criteris de raonabilitat en la investigació d'un delicte determinat i concret. Tingueu en compte, en efecte, que no n'hi ha prou amb la conservació de les dades, sinó que s'ha d'habilitar les autoritats de cada estat membre perquè adoptin mesures que garanteixin, d'una banda, la integritat i confidencialitat de les dades (garantia respecte a l'usuari) i, de l'altra, la seva utilitat per a la investigació (garantia en favor de l'Estat). Són, en definitiva, les diverses situacions, esglaonades per ordre d'agressivitat sobre les dades, que poden derivar com a imprescindibles en la investigació d'un delicte una vegada aquesta circumstància n'ha provocat la preservació. Sobre aquestes dades, cal imposar deures, a la manera com ho duu a terme l'article 16 de la Convenció:

- de **conservació**;

- de **protecció de les dades conservades davant atacs eventuals de tercers**, la qual cosa constitueix un dels riscos més importants i més freqüentment denunciats per a la intimitat;

- de **secret**, ja que l'obligat a la conservació no s'hauria de sentir legitimat en cap cas per a, després de la utilització de les dades en la investigació, la comunicació d'aquestes dades sobre la base d'una ruptura prèvia del secret fixada en el moment de la comunicació a les autoritats competents.

Una vegada fixades les garanties per al titular de les dades emmagatzemades i conservades per a la seva utilització al si d'una investigació criminal, no és menys important llavors fixar les garanties d'utilització per part de l'estat: cal, efectivament, que les dades conservades puguin ser posades immediatament a disposició de les autoritats competents amb les degudes garanties perquè la mesura excepcional adoptada sigui eficaç des del primer moment. Per aquesta raó, els articles 17, 18 i 19 de la Convenció construeixen els mecanismes jurídics necessaris per a habilitar les autoritats de cada estat part perquè les dades puguin ser divulgades als investigadors pel prestador del servei, comunicades amb caràcter immediat o puguin ser decomissades, copiades, inaccessibles per a tercers, etcètera.

Després de la preservació de dades, és a dir, el seu emmagatzemament judicialment ordenat per al cas concret i practicat en condicions de seguretat que minimitzin el risc per a la intimitat i per temps limitat, aquestes dades haurien de poder ser objecte de comunicació o divulgació a l'autoritat judicial que en va autoritzar l'ordre de preservació.

Més enllà de la preservació, tanmateix, hi ha el registre en temps real de dades de tràfic i de contingut. Si sobre la pura preservació de dades de tràfic, i en particular sobre la comunicació o divulgació, pesa ja la idea que es tracta de dades de la comunicació mateixa, subjectes al règim d'autorització judicial, amb més motiu encara s'hi haurà de recórrer per a recollir dades de contingut, cosa que s'entén com a comunicació, però també com a pura preservació. En qualsevol cas, la Convenció fa l'últim pas regulador i recorda la importància que per a la investigació de delictes greus podria arribar a tenir la intercepció en temps real de dades de contingut. Sobre les dades s'han d'adoptar mesures que permetin, amb cauteles idèntiques de secret i garantia d'indemnitat, recollir o gravar, mitjançant l'aplicació de mitjans tècnics existents a l'estat part (o obligar el prestador a fer-ho), les dades de contingut que circulin per la xarxa pública de telecomunicacions.

6.2. Retenció de dades a la Unió Europea

Vegem en primer lloc quin era el règim previst en la Directiva 2002/58/CE, sobre privacitat en les comunicacions electròniques, i analitzarem després el règim de retenció de dades que va establir la Directiva 2006/24/CE, i la transposició a l'ordenament espanyol.

6.2.1. La Directiva 2002/58/CE

Malgrat l'amenaça d'alguns països, entossudits a introduir en el seu ordenament intern, malgrat les obligacions internacionals subscrites, la possibilitat d'emmagatzemar i retenir dades de les comunicacions per si de cas fossin relacionats amb la comissió d'un fet constitutiu de delicte, el 2002 la Unió Europea

encara era fidel als seus principis. La Directiva 2002/58/CE, de 12 de juliol, del Parlament Europeu i el Consell relativa al tractament de les dades personals i a la protecció de la intimitat en el sector de les comunicacions electròniques, excloïa la possibilitat d'arxivament de dades de caràcter personal.

Ho feia en termes molt similars a com s'havia pronunciat la Directiva de 1997 de protecció de les dades personals de les persones físiques. Però, en aquesta ocasió, els seus considerants eren francament contundents:

> "Aquestes dades només s'han de poder emmagatzemar en la mesura que resultin necessàries per a la prestació del servei, per a finalitats de facturació i per als pagaments d'interconnexió i durant un temps limitat."

I si l'exposició de motius –és a dir, els considerants– de la Directiva és clara, no ho és menys l'articulat, i particularment els articles 5, 6 i 9. S'hi tornen a abocar totes les consideracions relatives a la necessitat d'una valoració prèvia a l'adopció de qualsevol mesura de restricció del dret a la intimitat, de manera que es promou la confidencialitat de les dades i la seva afectació al dret a la intimitat sobre qualsevol altra necessitat. Els estats garanteixen la confidencialitat de les dades de tràfic i contingut de les comunicacions; les dades de tràfic, a més, només poden ser emmagatzemades a efectes de facturació al client i entre operadores.

No obstant això, la Directiva porta la penitència en el seu propi pecat. Va voler ser especialment clara i amable en la delimitació dels supòsits en els quals l'equilibri podria ser alterat, perquè ha de poder ser alterat per a salvaguardar interessos que, de vegades, han de poder ser preponderants (vida, llibertat, integritat, seguretat nacional, etcètera). Tanmateix, l'article 15.1 de la Directiva, encarregat de delimitar l'abast de les excepcions a la preservació de dades, es va excedir i des d'una ponderació legal que es decanta pel dret a la intimitat i permet que sobre la base del principi de proporcionalitat pugui ser invertit l'equilibri, permet obrir una porta a tot el contrari; és a dir, una porta que, sempre que s'afirmi la preservació d'un altre bé com a supòsit de la retallada de la intimitat, aquesta pugui ser retallada.

En definitiva, l'article 15.1 de la Directiva, amb una redacció desafortunada, fa el salt des de la proporcionalitat real, ajustada al cas concret, a una proporcionalitat legislativament determinada abans que ni tan sols es plantegi el conflicte:

> "[...] els *estats membres* poden adoptar, entre d'altres, mesures legislatives en virtut de les quals les dades es conservin durant un termini limitat justificat pels motius establerts en aquest apartat (scil. *la prevenció, investigació, descobriment i persecució de delictes*)."

Al nostre judici, la Directiva no habilita amb la frase subratllada la creació de normes que, amb caràcter general i al marge de necessitats reals de prevenció de la comissió d'un delicte concret i determinat o de la seva investigació, permetin la preservació i l'emmagatzemament per un temps limitat de dades de tràfic. Sinó que només habilita a allò que la Convenció del Consell d'Europa

establia sobre cibercrim anys enrere: és possible la preservació i l'arxivament de dades de tràfic per qüestions diverses a la pura facturació o gestió de la comunicació mateixa. És possible i només es pot regular per llei la manera com es pot acordar aquest emmagatzemament, però res d'això significa que legalment s'hagin d'habilitar, ni es pugui fer, obligacions generals d'arxivament de dades en tot cas, temps i circumstància per si això pogués eventualment ser interessant per a l'esbrinament del delicte.

6.2.2. Proposta de decisió marc d'emmagatzemament i retenció de dades de tràfic i la Directiva 2006/24/CE

L'any 2004, França, Suècia, Irlanda i el Regne Unit van tractar d'impulsar una proposta de decisió marc en matèria de retenció que permetés l'arxivament de dades de tràfic. Aquesta decisió marc situaria el debat en l'àmbit del tercer pilar, és a dir, en l'espai europeu de seguretat i justícia. El Parlament Europeu rebutjava llavors la proposta i aquesta reacció de rebuig és la que permetia obrir la via del primer pilar, al·ludint a l'espai europeu de comerç, per a regular qüestions directament basades en la lluita contra el terrorisme i, en general, la prevenció del delicte.

Dos anys després, veia la llum la Directiva 2006/24/CE del Parlament Europeu i del Consell, de 15 de març, sobre la conservació de dades generades o tractades amb relació a la prestació de serveis de comunicacions electròniques d'accés públic o de xarxes públiques de comunicacions i per la qual es modificava la Directiva 2002/58/CE. Es va adoptar així una decisió determinada a partir d'un element d'harmonització de la legislació dels diferents estats membres, sobre la base, essencialment, de la comprovació que diversos estats de la UE ja havien adoptat en el seu dret intern mesures semblants a les que proposava la Directiva, la qual cosa llavors imposaria la necessitat de racionalització de la legislació de l'espai comú.

L'aprovació de la Directiva ha estat precedida d'un procés crític formidable. Si el 1999 era la mateixa Unió Europea qui exercia amb èxit de contrapès a les mesures d'emmagatzemament proposades per la Convenció del Consell d'Europa sobre cibercrim, la gènesi d'aquesta Directiva ha estat objecte de crítiques ferotges provinents d'institucions de la mateixa Unió que a la fi s'han mostrat incapaces de frenar el lliberticidi. El grup de l'article 29, el supervisor europeu de protecció de dades, el Comitè Econòmic i Social, etcètera, van expressar tots ells la seva preocupació màxima per la possibilitat que una norma com la Directiva 2006/24 es pogués arribar a aprovar.

La Directiva parteix de la constatació d'un canvi social gairebé absolut derivat dels atemptats de Madrid i Londres, el 2004 i el 2005, respectivament. De fet, els considerants 8 i 10 es refereixen específicament a reunions del Consell Europeu que van tenir lloc immediatament després dels atemptats terroristes referits i en les quals sempre s'acabava encoratjant la Comissió i el Parlament

perquè adoptés mesures legislatives que permetessin avançar en la ràpida obtenció de dades de les comunicacions a efectes de la prevenció i repressió del delicte.

La Directiva fa taula rasa amb totes les dades que puguin tenir incidència directa o indirecta en el tràfic ordinari de les comunicacions electròniques, telemàtiques o de telefonia.

Els ISP han de retenir i emmagatzemar, per un període de fins a dos anys i mai inferior a sis mesos, totes les dades que permetin:

- Rastrejar i identificar l'origen d'una comunicació.
- Identificar la destinació d'una comunicació.
- Identificar la data, hora i durada d'una comunicació.
- Identificar el tipus de comunicació.
- Identificar l'equip de comunicació dels usuaris o el que es considera que és l'equip de comunicació.
- Identificar la localització de l'equip de comunicació mòbil.

Totes les connexions fetes mitjançant telefonia mòbil, per Internet –connexió a pàgines web, descàrregues, temps de connexió, persones amb qui s'entaula conversa o relació, tipus de llocs visitats, freqüència, connexió–, en definitiva, totes les connexions que conformen el comportament social majoritari, han de ser retingudes per un temps no inferior a sis mesos.

A partir de la consideració anterior sorgeix la gran antítesi interpretativa: la Directiva és només una manera de raonament formal, buit de contingut material en l'argument. Es tracta d'una norma que, efectivament, intenta trobar cobertura en d'altres i simplificar un discurs, el de la ponderació de béns en joc, ja de per si prou complex, i mira de semblar amable, justa i necessària. Però una anàlisi contraposada dels punts de partida i els arguments expressats en els considerants no resisteix la comparació.

En efecte:

- A diferència del que marca la Convenció del Consell d'Europa sobre cibercrim, que manté la proporcionalitat com a via per a la ponderació de béns en conflicte judicialment, la Directiva deriva la ponderació a l'àmbit legislatiu. Basant-se en una lectura impossible de l'article 15.1 de la Directiva de protecció de dades, que buidaria de contingut tractats i convenis seculars, la Directiva pretén efectuar la ponderació de béns en els seus considerants: com que la conservació de dades s'ha acreditat com una eina

d'investigació necessària i eficaç, cal conservar-les totes, emmagatzemades, durant almenys sis mesos, al marge de la necessitat real en el temps d'aquestes dades.

La proporció ha operat, doncs, *iuris et de iure*. S'ha determinat que la mesura és en tot cas necessària, encara que no ho sigui en el cas concret. El trànsit des d'una norma que habilita l'emmagatzemament en condicions excepcionals i absolutament justificades en el cas concret, a una norma que habilita l'emmagatzemament com a regla general no justificada ni necessitada legalment de justificació en el cas concret, és un trànsit cap a l'abisme jurídic. És una interpretació aberrant del principi de ponderació de béns, però sobretot és l'abrogació legal del dret a la intimitat en favor dels poders públics, garants en principi de tot el contrari.

- De fet, el supervisor europeu i la Directiva parteixen de perspectives molt diferents. El primer entén que el Conveni del Consell d'Europa de 1950 imposa en l'article 8 el respecte a la intimitat dels ciutadans (com a norma dirigida als poders públics). Només excepcionalment es podria limitar el dret, d'acord amb una jurisprudència del Tribunal Europeu de Drets Humans més que consolidada (casos: Amann, 2000; Malon, 1984; i Dudgeon, 1985). La Directiva parteix del contrari: la investigació del delicte ha esdevingut fonamental des dels atemptats terroristes de Nova York, Madrid i Londres. Qualsevol primacia del dret a la intimitat sobre el poder informàtic de l'estat i l'anàlisi de la informació pel seu aparell, ha de vèncer la lògica d'una norma que imposa precisament l'anul·lació del dret en favor del poder de l'estat.

- Però, a més, la Directiva és especialment perillosa. Davant la perspectiva del supervisor, en la qual la restricció del dret hauria de garantir les condicions de seguretat i, tal com succeïa amb la Convenció del Consell d'Europa sobre cibercrim, de confidencialitat i integritat de la informació, la Directiva confia als estats la gènesi i el desenvolupament de normes que tinguin aquesta necessitat, però en situar-se al primer pilar deixa fora de l'àmbit de la Directiva mateixa qualsevol obligació a ella i la seva transposició vinculada. De manera que la retenció serà obligada quan finalitzi el període d'implementació i es transposi al dret intern. Les garanties d'integritat, preservació, confidencialitat, etcètera no formen, almenys no necessàriament, part de la norma que, encara que partint d'un excés, ha de regular la retenció i l'arxivament de dades. En conclusió: arxivament de dades sense garanties de confidencialitat i integritat i seguretat.

- El dèficit de proporcionalitat, finalment, és màxim en la Directiva, en mancar de qualsevol referència al tipus de delictes en la investigació dels quals es poden analitzar les dades retingudes. Es poden utilitzar per a la prevenció de la comissió de delictes. De qualssevol delictes. En definitiva, el nombre de finalitats per a les quals es podrien utilitzar les dades és infinit.

6.3. La Llei 25/2007, de 18 d'octubre, de transposició de la Directiva

La Directiva 2006/24/CE anticipa el judici de proporcionalitat i, a més, permet la retenció de dades de tràfic en hipòtesi de mera prevenció del delicte –abans, doncs, de la seva comissió–, d'acord amb judicis de pronòstic.

La Llei 15/2007, de 18 d'octubre, de transposició de la Directiva, ha aconseguit tornar l'equilibri a la ponderació legal d'interessos. L'article 1.1 de la norma, en efecte, esdevé essencial:

> "Aquesta Llei té per objecte la regulació de l'obligació dels operadors de conservar les dades generades o tractades en el marc de la prestació de serveis de comunicacions electròniques o de xarxes públiques de comunicació, i també el deure de cessió d'aquestes dades als agents facultats sempre que els siguin requerides per la corresponent autorització judicial amb finalitats de detecció, investigació i enjudiciament de delictes greus previstos en el Codi penal o en les lleis penals especials."

La Llei, gràcies a la redacció reproduïda, resol els dubtes de constitucionalitat que hauria plantejat una transposició íntegra de la Directiva. Les dades emmagatzemades només es poden fer servir en la investigació i prevenció del delicte amb autorització judicial prèvia i només en el cas de delictes greus, és a dir, aquells la pena dels quals sigui superior a cinc anys, la qual cosa significa que en la ponderació d'interessos la intimitat preval i només cal exposar-la en casos greus i amb control judicial. A més, la Llei vincula la protecció de les dades emmagatzemades amb la regulació recent continguda en el Reglament de mesures de seguretat aprovat pel Reial decret 1720/2007, de 21 de desembre, que modula les exigències tècniques de salvaguarda en funció de la importància de les dades recollides.

La transposició en els termes apuntats oxigena el principi de proporcionalitat i torna la retenció de dades de les comunicacions a l'àmbit del que és raonable. No significa això, tanmateix, que la planificació de la retenció de dades de les comunicacions sigui una lletania de virtuts tecnicojurídiques.

En primer lloc, confiar la modulació del termini d'emmagatzemament a un desenvolupament reglamentari eventual constitueix un excés de la Llei de transposició: no sembla raonable que sigui un reglament qui estableixi la naturalesa jurídica de determinades dades per a, a continuació, establir-ne el període de retenció màxim i mínim; hauria estat desitjable que fos la mateixa Llei qui advertís una jerarquia inicial en el tipus de dades emmagatzemades per després desplegar-lo reglamentàriament.

En segon lloc i des del punt de vista pràctic, la Llei pot haver limitat excessivament l'àmbit d'aplicació de la retenció. Si l'emmagatzemament massiu de dades implica una posada en perill de la intimitat, atès el risc elevat que aquestes dades acabin essent accessibles per tercers no autoritzats, no sembla raonable que aquestes dades no puguin ser accessibles en la lluita contra la criminalitat

informàtica: són delictes greus (art. 13.1 CP, amb relació a l'article 33.2 CP) aquells que comporten una pena greu, i són penes greus aquelles en les quals la pena de presó és superior a cinc anys.

Un marc penal així no es troba ni en l'estafa bàsica (pesca electrònica, targetes de crèdit), ni en els delictes de difusió de continguts il·lícits (pornografia infantil, propietat intel·lectual), ni en els delictes contra la intimitat, o d'extorsió 243 CP, llevat que es recorri als subtipus agreujats (art. 197.6 CP, 250 CP, etcètera). I una lectura literal de la Llei, en la qual el judici de proporcionalitat parteix de penes greus, és a dir, superiors a cinc anys, obligaria l'òrgan d'instrucció a denegar totes les sol·licituds de dades de tràfic emmagatzemades que fossin cursades en l'àmbit d'investigacions concernents a delictes tecnològics. Una gran paradoxa, sens dubte: la tecnologia, exclosa de l'àmbit d'investigació dels delictes tecnològics. I com veurem a continuació, determinades dades de tràfic, com la IP d'origen, resulten determinants per a l'inici mateix de les indagacions que tendeixen a l'esbrinament del delicte i el delinqüent.

En tercer lloc i també des d'una dimensió pràctica, la relació detallada de dades que poden ser objecte d'emmagatzemament i cessió a les autoritats per a la investigació del delicte genera certs inconvenients. L'obtenció de la IP d'un usuari requereix una autorització judicial. Això significa que les forces i els cossos de seguretat necessiten una autorització judicial per a esbrinar l'origen d'una comunicació. Certament, la IP assignada a una màquina en el procés de comunicació pot ser suficient per a identificar un individu i, en aquesta mesura, és una dada que no es pot qualificar de neutre. Però el seu valor per a l'inici d'una investigació és tan elevat que s'haurien d'haver sabut discernir els casos en els quals la sol·licitud de la IP d'origen ha de requerir una autorització judicial d'aquells altres en els quals no cal.

Si es té en compte, a més, que el jutge no hauria d'admetre peticions de facilitació d'aquest tipus de dades per a hipòtesis d'investigació de delictes associats als processos de transferència de dades (perquè no superen la pena prevista de cinc anys de presó referits en l'article 1.1 Llei 25/2007), no sembla que es pugui concloure que la regulació és òptima quant a la manera concreta d'ordenar les dades objecte d'emmagatzemament.

Finalment, l'absència d'una regulació tan prolixa com dotada de contingut material entorn de les garanties d'emmagatzemament incrementa notablement el risc per a la intimitat i deixa la ponderació legal en una desiderata poc fonamentada.

7. Lloc de comissió del delicte i competència jurisdiccional

Epígraf redactat íntegrament per María Rosa Fernández Palma

El caràcter global i transfronterer de la Xarxa planteja, també en l'àmbit penal, problemes de determinació de la llei aplicable i la jurisdicció competent, que examinarem en aquest últim apartat.

7.1. Introducció

El criteri general d'atribució de competència jurisdiccional penal a un estat determinat apareix representat pel principi de territorialitat, que delimita l'abast de la competència dels tribunals espanyols a fets delictius comesos en l'àmbit espacial de les seves fronteres. Així, l'article 23.1 de la Llei orgànica del poder judicial (LOPJ) adverteix el següent:

> "En l'Ordre penal correspon a la jurisdicció espanyola el coneixement de les causes per delictes i faltes comesos en territori espanyol o comesos a bord de vaixells o aeronaus espanyols, sense perjudici del previst en els tractats internacionals en els quals Espanya sigui part."

Fora d'aquest, la *vis atractiva* dels tribunals espanyols afecta, a més, els nacionals espanyols per fets comesos més enllà de l'espai territorial, sempre que es presentin els elements previstos en l'article 23.2 LOPJ (principi personal). I, finalment, la jurisdicció espanyola s'estén, per mor dels principis real o de comunitat d'interessos i de justícia universal, a l'elenc de matèries expressament previstes, amb independència del lloc de comissió i la nacionalitat del subjecte actiu (art. 23.3 i 4 LOPJ).

La resistència tradicional dels estats a cedir parcel·les de sobirania té un dels seus fonaments en el principi de territorialitat penal, que en el seu vessant positiu permet als jutges i tribunals d'un estat enjudiciar qualsevol fet delictiu que tingui lloc dins del seu àmbit territorial –sigui qui sigui el seu autor– i negativament comporta que aquells únicament tinguin competència dins d'aquest mateix context espacial –amb les excepcions abans avançades. No és difícil entendre el fonament del criteri –deixant-ne de banda l'ancoratge polític– si es pensa que normalment el lloc de comissió coincideix amb el de resultat i que, lluny de les fronteres pròpies, els fets amb rellevància penal difícilment poden causar perjudicis –això dit, sense obviar les excepcions clàssiques a la regla, representades per altres principis actuals, com el de comunitat d'interessos o justícia universal.

Internet i el tipus de relacions que aquesta afavoreix, tanmateix, han desestabilitzat, si es pot afirmar així, l'aparentment serè panorama descrit, la qual cosa possibilita que les conductes que es desenvolupen en qualsevol lloc del món –i per persones no nacionals d'aquest estat– puguin causar efectes lesius o posar en perill béns jurídics també en qualsevol punt de la geografia en el qual hi hagi una màquina amb accés a la xarxa d'Internet.

Comentari sobre el contrasentit de sobirania territorial en l'entorn d'Internet

No podem deixar d'apuntar el contrasentit que representa que els estats pretenguin aferrar la seva sobirania mitjançant l'assegurament de la seva territorialitat penal, quan materialment el mateix funcionament d'Internet els pot restar, d'acord amb el contingut d'aquest criteri, materialment, amplíssimes parcel·les de sobirania, en condicionar la persecució d'il·lícits penals a fets únicament esdevinguts a les fronteres territorials.

La clau en matèria de competència jurisdiccional penal –si ens centrem en el principi general al·ludit–, l'ofereix la determinació del lloc de comissió del delicte.

El sistema de funcionament propi d'Internet condiciona la naturalesa de delictes a distància de moltes de les infraccions que es perpetren a la Xarxa, la qual cosa dificulta la fixació del *forum delicti comissi*, no solament perquè el lloc d'execució o comissió en sentit estricte no sol coincidir amb el lloc de producció del resultat, sinó perquè, en els delictes de mera activitat, moltes vegades no es pot perseguir la infracció als territoris on pugui estar tenint algun tipus d'efecte.

Les limitacions del principi de territorialitat, que en molts casos podrien ser salvades mitjançant l'aproximació dels ordenaments penals dels diferents estats, s'han intentat obviar mitjançant una interpretació flexible dels criteris de determinació del lloc de comissió del delicte, que, com més avall es constatarà, poden conduir a l'enteniment de la competència territorial conforme a criteris d'atribució de competència universal, de manera que desvirtua la coherència del sistema o la fonamentació de les excepcions a la regla general.

Amb tot, s'ha de deixar constància, d'una banda, que les insuficiències del principi de territorialitat no constitueixen una novetat, sinó que són un tema ja conegut i tractat per la doctrina penal en ocasió de l'estudi dels anomenats *delictes a distància* o *en trànsit*, que s'ha vist agreujat en nombre i complexitat per les particularitats de comunicació que ofereix Internet i el possible ús dels seus avantatges per a la comissió d'il·lícits penals. I, d'una altra banda, de les dificultats interpretatives del mateix terme *lloc de comissió*, com més avall es tindrà ocasió d'exposar.

7.2. El principi de territorialitat. Teories per a la determinació del lloc de comissió del delicte

Tal com hem avançat més amunt, l'article 23 LOPJ consagra l'anomenat *principi de territorialitat* proclamant la competència de la jurisdicció espanyola per al coneixement de les infraccions penals comeses dins del territori nacional.

El concepte nuclear de la definició, el constitueix la determinació del lloc de comissió del delicte, qüestio de senzillesa aparent però que, tanmateix, no té un contingut unànimement consensuat. En efecte, el lloc de comissió es pot identificar amb el lloc d'execució de l'acció típica o d'omissió de la conducta (teoria de l'acció). Però també amb el de producció del resultat (teoria del resultat). O amb ambdós, si és que aquells no coincideixen espacialment i la infracció té naturalesa de delicte de resultat (teoria de la ubiqüitat).

Són notòries les llacunes de punibilitat que es poden suscitar amb un enteniment restringit del lloc de comissió conforme a la teoria de l'acció o la teoria del resultat, alternativament; per això, la doctrina i la jurisprudència es mostren partidàries majoritàriament de la teoria de la ubiqüitat, que permet atribuir competència als òrgans jurisdiccionals tant del lloc de l'acció o omissió, com del lloc del resultat, si és que aquests apareixen espacialment deslligats, com és essència en els anomenats *delictes a distància*.

Sentència de l'Audiència Nacional de 2 de febrer de 2007

La Sentència de l'Audiència Nacional de 2 de febrer de 2007 recorda que "el problema apareix en els delictes a distància, en els quals l'acció i el seu resultat es produeixen en llocs diferents. La llei espanyola vigent manté un silenci absolut sobre quin és el lloc de comissió del delicte, per la qual cosa, en principi, s'ha d'acudir a les opcions interpretatives tradicionals que són, per a la teoria de l'activitat que el delicte sigui comès allà on l'autor ha dut a terme la seva acció, i per a la teoria del resultat el lloc on es produeix. Com que tant l'una com l'altra teoria condueixen a llacunes de punibilitat i produeixen situacions d'impunitat intolerables, la doctrina es basa majoritàriament en la teoria de la ubiqüitat, d'acord amb la qual es pot considerar comès el fet, tant al lloc on s'ha dut a terme l'acció, com en aquell en el qual s'ha produït el resultat.

La teoria de la ubiqüitat és perfectament assumible en el nostre ordenament vigent, en no manifestar-se expressament l'article 23.1 de la LOPJ sobre el lloc de comissió, la qual cosa permet qualsevol interpretació, i el fet que la LOPJ vigent prescindeixi de qualsevol precisió, no solament permet sinó que afavoreix una interpretació àmplia del concepte de *comissió del delicte*, de manera que aquesta comporta tant la realització d'una activitat, com la producció d'un resultat, la qual cosa en la teoria del delicte es coneix com a *desvalor d'acció* i *desvalor de resultat*, i així el delicte no es comet exclusivament en el moment de l'acció ni en el moment de la producció del resultat, sinó en ambdós, cosa que coincideix amb la tesi de la ubiqüitat.

Tot l'anterior resulta aplicable al supòsit extradicional, en el qual els fets es diuen comeses en cinc llocs a l'estranger i a Mallorca, però l'actuació a Mallorca només es refereix a una actuació inicial per a la promoció, via Internet, de l'activitat criminal, que no és excloent sinó concurrent amb altres llocs estrangers. D'altra banda, l'organització de la logística de les comandes fraudulentes va ser efectuada per dos coautors més en tres determinades ciutats alemanyes on s'embalaven i preparaven les trameses, i des d'on també amb el concurs de dos coautors més, en el pla criminal prèviament traçat pel reclamat, es distribuïen a l'estranger a partir de l'empresa UPS".

Nota sobre l'absència de competència dels tribunals espanyols sobre l'assumpte

Fixeu-vos que, malgrat que la conducta es desenvolupa parcialment en territori espanyol (s'ofereix el producte en una pàgina web, la qual cosa es pot considerar com a part de l'engany típic de l'estafa), el tribunal descarta la competència dels tribunals espanyols per falta de connexió prou important dels fets (proporcionalitat) amb el nostre territori.

Amb tot, cal destacar, en primer lloc, la dificultat per a fixar el lloc d'execució de l'acció típica quan s'empra Internet com a suport o vehicle per a la comissió, ja que sovint no coincideixen el lloc des del qual físicament s'introdueixen els continguts il·lícits o s'ordena la destrucció de dades, per exemple, i la seu del servidor en el qual s'allotgen. Davant d'aquest ampli elenc de possibles llocs de comissió, la doctrina més recent sembla haver abandonat la idea de fixar el lloc de comissió per referència al lloc d'allotjament de les dades o la pàgina web –això és, normalment, el de la seu del prestador de serveis–, pel més físic del lloc des d'on es produeix la transferència de dades des d'un ordinador de manera que són fets públics en una pàgina web o el del lloc des d'on es dóna l'ordre que permet un accés il·legal (Sánchez/Blanco).

Tot i així, la determinació del lloc d'execució mitjançant el criteri exposat es podria veure greument dificultada pel mode d'atac en cadena que se sol utilitzar en aquest tipus de delinqüència, en el qual intervenen diverses màquines amb funcions diferents que sovint permeten esborrar les empremtes de l'origen de l'activitat.

Així va succeir, entre d'altres, en el denominat *cas Hispahack*, en el qual l'atac informàtic dissenyat es va desenvolupar mitjançant l'accés successiu a altres màquines amb la finalitat d'esborrar les empremtes de l'origen de la ingerència. El lloc d'ubicació de les màquines tapadora és, a més, aleatori, la qual cosa donaria lloc, aparentment, a l'entrada en joc de la jurisdicció de múltiples estats.

Segurament aquesta dada, entre d'altres, ha contribuït a propiciar tesis particularment extensives del concepte de *lloc de resultat* que permeten estendre el fòrum de competència no solament als llocs en els quals es verifica el resultat típic, sinó també a aquells en els quals simplement es deixen sentir els seus efectes, encara que el delicte resulti, en sentit estricte, de mera activitat (per exemple, el lloc des d'on es permeti l'accés a un contingut il·lícit). Aquesta visió, que aparentment contribuiria a l'ideal d'una seguretat més gran, pot comportar situacions no desitjables i, el més rellevant, a la pràctica condueix a identificar els fonaments del principi de territorialitat amb els propis que justifiquen les excepcions a aquesta regla, sense que necessàriament la matèria així ho aconselli. En efecte, des del primer punt de vista, s'ha de subratllar que l'ordre axiològic d'una cultura determinada conforma l'abast del seu ordenament penal, la qual cosa podria propiciar que fets no desvalorats al lloc de la seva execució es poguessin criminalitzar per la seva disponibilitat en un altre espai estatal que sí els atribueix rellevància penal (àmpliament, Sánchez/Blanco).

Amb relació al segon aspecte, aquest enteniment ampli de *resultat* desvirtua el principi de competència territorial, del contingut del qual únicament es conservaria el *nomen*, ja que, a la pràctica i en vista de la mateixa naturalesa d'Internet, els tribunals de qualsevol estat des del qual resultessin accessibles els continguts es reputarien competents per al coneixement dels fets, de manera que s'universalitzaria la competència per a, en principi, qualsevol conducta, sense la referència necessària a la matèria que caracteritza les excepcions representades pels principis real i de justícia universal. Les dificultats exposades justifiquen, però, un enteniment restringit del concepte de *resultat* –i, per tant, del seu lloc de producció–, tenint en compte que un bon percentatge de les llacunes de punibilitat que pogués propiciar serien contrarestades eficaçment mitjançant un assaig seriós d'unificació internacional de legislació en matèria de delicte informàtic.

Interlocutòria de 5 de maig de 2003 sobre la competència jurisdiccional partint de la teoria de la ubiqüitat

La Interlocutòria de 5 de maig de 2003 dictada pel Jutjat Penal núm. 18 de Barcelona va declarar tant la competència jurisdiccional dels tribunals espanyols com la territorial dels de Barcelona, a partir de la coneguda com a *teoria de la ubiqüitat*, i va afirmar –després d'efectuar un repàs dels corrents doctrinals més rellevants– que "aquest criteri que sembla el més satisfactori ha estat acceptat pel TS 2n. en la Interlocutòria de 20 de maig de 1992, en dir que tant l'acció com el resultat són elements del tipus.

Per tant, el lloc de comissió és en principi aquell en el qual ambdós elements hagin tingut lloc. Tanmateix, quan l'acció i el resultat no tinguin lloc dins de la mateixa jurisdicció, és aplicable el principi de la ubiqüitat, segons el qual tant el lloc de l'acció com el lloc del resultat han de ser rellevants a efectes de l'article 14.2 LECrim". En el cas concret, es tractava d'una presumpta infracció de propietat intel·lectual, en posar a disposició del públic, des d'un servidor ubicat als Estats Units, determinats programes que permetrien el "craqueig de programes d'ordinador i obres audiovisuals protegides. Les pàgines web d'allotjament van ser creades inicialment a Espanya, per ciutadans espanyols, i la posterior introducció, gestió i administració dels continguts il·lícits era duta a terme pels mateixos integrants de la companyia Vesatec des d'Espanya, i no és sinó posteriorment quan els imputats decideixen desplaçar-se fora del territori nacional per continuar amb el desenvolupament de les conductes imputades, concretament per mitjà d'un servidor gratuït de nom *Isla Tortuga* amb seu als Estats Units".

A més, la resolució tracta com a dades rellevants que permeten l'afirmació de competència que "els imputats són espanyols, de manera que és igualment territori nacional on s'han trobat, físicament, les proves del presumpte delicte que hagin preparat; són, igualment, espanyols els principals clients dels imputats, la qual cosa significa realment que els presumptes delictes perpetrats per aquests despleguen els seus efectes en territori espanyol; igualment, és a Espanya on es produeix el descobriment del delicte, lloc en el qual, com acabem de dir, desplega els seus efectes i perjudicis".

S'ha d'advertir que el principi personal (art. 23.2 LOPJ), pràcticament en desús en els últims temps, ha aconseguit una certa revitalització gràcies a les infraccions comeses a Internet i els obstacles que presenta la determinació del lloc de comissió del delicte, per les raons apuntades.

Sentència de l'Audiència Provincial de Barcelona de 8 de gener de 2008

Com a mostra, la SAP de Barcelona, secció vuitena, de 8 de gener de 2008, afirma que "ni l'al·legació ni la pretensió d'incompetència dels nostres tribunals es pot acollir, atesa la redacció de l'article 23.2 de la LOPJ, que reconeix la competència dels tribunals espanyols encara que el delicte hagi estat comès a l'estranger, sempre que els seus responsables siguin espanyols i es donin uns supòsits que, en aquest cas, no s'han demostrat absents, concretament la tipicitat del fet al país de comissió, la querella del fiscal i que el delinqüent no hagi estat jutjat ja al país de comissió del delicte".

Finalment, s'ha de posar de manifest que els delictes relatius a la prostitució i els de corrupció de menors formen part del conjunt d'infraccions que conformen el principi de justícia universal (art. 23.4.*e* LOPJ). Les dificultats exposades, juntament amb l'existència de consens internacional per a la reprensió d'aquestes conductes, han permès ampliar l'àmbit d'aquest principi, a fi d'afavorir la lluita contra la pornografia infantil i altres formes de corrupció de menors.

Bibliografia

Álvarez Vizcaya, M. (2001). "Consideraciones político criminales sobre la delincuencia informática: el papel del Derecho penal en la Red". A: J. J. López Ortega (dir.). *Internet y Derecho penal. Cuadernos de Derecho Judicial, CGPJ* (núm. X).

Andrés Blasco, J. de (1999). "Internet". *Cuadernos del Senado* ("Serie Minor", núm. 1).

Andrés Domínguez, A. C. (1999, 2 de febrer). "El delito de daños informáticos". *La Ley* (núm. 4725).

Bacigalupo Zapater, E. (1983). "Estafa y abuso de crédito". *La Ley* (núm. 3, pàg. 998-1004).

Bacigalupo Zapater, E. (1988). "Utilización abusiva de cajeros automáticos por terceros no autorizados". *Poder Judicial* (núm. 9 especial).

Bacigalupo Zapater, E. (2001). "La protección penal de los derechos industriales". *Revista Electrónica de Ciencia Penal y Criminología (RECPC)* (núm. 3). En línia: <http://criminet.ugr.es/recpc/recpc_03-07>.

Bacigalupo Zapater, E. (2002). "Documentos electrónicos y delitos de falsedad documental". *RECPC* (núm. 4, pàg. 1-17). En línia: <http://criminet.ugr.es/recpc/recpc_04-12.pdf>.

Bajo Fernández, M. (2004). *Los delitos de estafa en el Código penal*. Madrid: Centro de Estudios Ramón Areces.

Bajo Fernández, M. (2005). "El artículo 248". A: M. Cobo del Rosal (dir.). *Comentarios al Código penal*. Vol. VIII: *Delitos contra el patrimonio y contra el orden socioeconómico*. Madrid: EDERSA.

Bajo Fernández, M. (dir.) (1998). *Compendio de Derecho penal (parte especial)* (vol. II). Madrid: Centro de Estudios Ramón Areces.

Bercovitz Rodríguez-Cano, R.; Marín López, J. J. (2007). "El límite de copia privada y las redes de intercambio *peer to peer*". A: F. Caminal Badia (dir.). *Protección de la obra audiovisual. Cuadernos de Derecho Judicial, CGPJ* (núm. 3).

Blanco Cordero, I.; Sánchez García de Paz, I. (2002). "Problemas de Derecho penal internacional en la persecución de delitos cometidos a través de Internet". *Actualidad Penal* (núm. 7).

Bolea Bardón, C.; Robles Planas, R. (2001). "La utilización de tarjetas ajenas en cajeros automáticos: ¿robo, hurto o estafa?". *La Ley* (núm. 4).

Bravo García, J. L. (2002). "Falsificación de moneda y tarjetas de pago: el art. 387 del Código penal". A: J. M. Maza Martín (dir.). *Tarjetas bancarias y Derecho penal. Cuadernos de Derecho Judicial, CGPJ* (núm. 6).

Busch, C. (1995). *La protección penal de los derechos de autor en España y Alemania*. Barcelona: Cedecs.

Capeller, W. (2000). "Not such a Neat Net. Some comments on virtual criminality". *Social & Legal Studies* (núm. 10, vol. 2, pàg. 229-242).

Castells, M. (1997). *La era de la información: Economía, sociedad y cultura*. Vol. I: *La sociedad red* (traducció de Carmen Martínez Gimeno). Madrid: Alianza.

Castilla Cubillas, M. (2007). *La tarjeta de crédito*. Madrid/Barcelona: Marcial Pons.

Cavanillas Múgica, S. i altres (2007). *Responsabilidades de los proveedores de información en Internet*. Granada: Comares.

Collin, B. C. (1996). "The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge". A: *11th Annual International Symposium on Criminal Justice Issues*. En línia: <http://www.afgen.com/terrorism1.html>.

Conde-Pumpido Ferreiro, C. (1997). *Estafas*. València: Tirant lo Blanch.

Corcoy Bidasolo, M. (1992). "Protección penal del sabotaje informático. Especial consideración de los delitos de daños". A: S. Mir Puig (coord.). *Delincuencia informática*. Barcelona: PPU.

Cotino Hueso, L. (2007). *Libertad en Internet: La Red y las libertades de expresión e información.* València: Tirant lo Blanch.

Cramer, P. (1997). "§ 263a n. m. 1". A: A. Schöncke; H. Schröder. *Strafgesetzbuch Kommentar* (25a. ed.). Munic.

Cremades, J.; Fernández Ordóñez, M. A.; Illescas, R. (coord.) (2002). *Régimen jurídico de Internet.* Madrid: La Ley.

Cuesta Aguado, P. M. de la (2002). "Derecho penal económico y nuevas tecnologías". A: L. R. Ruiz Rodríguez (ed. lit.). *Sistema penal de protección del mercado y de los consumidores: actas del II Seminario Internacional de Derecho Penal Económico, Jerez, desembre de 2000* (pàg. 187-212). València: Tirant lo Blanch.

Choclán Montalvo, J. A. (1997). "Estafa por computación y criminalidad económica vinculada a la informática". *Actualidad Penal* (núm. 2).

Choclán Montalvo, J. A. (2001). "Fraude informático y estafa por computación". A: J. J. López Ortega (dir.). *Internet y Derecho penal. Cuadernos de Derecho Judicial, CGPJ* (núm. X).

Choclán Montalvo, J. A. (2002). "Infracciones patrimoniales en los procesos de transferencia de datos". A: Ó. Morales (dir.). *Delincuencia informática: Problemas de responsabilidad. Cuadernos de Derecho Judicial, CGPJ* (núm. 9).

Choclán Montalvo, J. A. (2006). "Infracciones patrimoniales en los procesos de transferencia de datos". A: C. M. Romeo Casabona (coord.). *El cibercrimen: Nuevos retos jurídico-penales, nuevas respuestas político-criminales*. Granada: Comares.

Diego Díaz-Santos, M. R. (2001). *Derecho penal, sociedad y nuevas tecnologías*. Madrid: Colex.

Díez Ripollés, J. L. (2005). "De la sociedad del riesgo a la seguridad ciudadana: un debate desenfocado". A: *Homenaje al profesor doctor D. Gonzalo Rodríguez Mourullo*. Cizur Menor: Thomson-Civitas.

Faraldo Cabana, P. (2007). "Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática". *Eguzkilore. Cuaderno del Instituto Vasco de Criminología* (núm. 21).

Faraldo Cabana, P. (2009). *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico*. València: Tirant lo Blanch / ICAB.

Fernández Entralgo, J. (2002). "Falsificación y utilización fraudulenta de tarjetas electrónicas". A: J. M. Maza Martín (dir.). *Tarjetas bancarias y Derecho penal. Cuadernos de Derecho Judicial, CGPJ* (núm. 9, pàg. 13-66).

Fernández Esteban, M. L. (1998). *Nuevas tecnologías, Internet y derechos fundamentales*. Madrid: McGraw-Hill.

Fernández Esteban, M. L. (2000). *Intimidad en la empresa y secreto de las comunicaciones*. Cizur Menor: Aranzadi Civil.

Fernández García, E. M. (1999). "Fraudes y otros delitos patrimoniales relacionados con la informática e Internet". *Estudios jurídicos. Ministerio Fiscal* (núm. 4).

Fernández García, E. M.; López Moreno, J. (1997). "La utilización indebida de tarjetas de crédito en el Código penal de 1995". *Revista del Poder Judicial* (núm. 46).

Fernández Palma, M. R.; Morales García, O. (2000). "El delito de daños informáticos y el caso Hispahack". *La Llei* (núm. 283).

Fernández Pinós, J. E. (2002). "Cuestiones procesales relativas a la investigación y persecución de conductas delictivas en Internet". A: F. Morales Prats; Ó. Morales García (coord.). *Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet.* Cizur Menor: Aranzadi.

Fernández Teruelo, J. G. (2007, gener). "Respuesta penal frente a fraudes cometidos en Internet: estafa, estafa informática y los nudos de la Red". *Revista de Derecho Penal y Criminología* (núm. 19).

Fornasari, G. (2004). "Il ruolo della esigibilità nella definizione della responsabilità penale del provider". A: L. Picotti (coord.). *Il diritto penale dell'informatica nell'epoca di Internet* (pàg. 423-432). Pàdua: Cedam.

Galán Muñoz, A. (2004). "El nuevo delito del art. 248.3 CP: ¿un adelantamiento desmedido de las barreras de protección penal del patrimonio?". *La Ley* (núm. 3).

Galán Muñoz, A. (2005). *El fraude y la estafa mediante sistemas informáticos: Análisis del art. 248.2 CP*. València: Tirant lo Blanch.

Galán Muñoz, A. (2006). "Expansión e intensificación del Derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática". *Revista de Derecho y Proceso Penal* (núm. 15).

García Noguera, I. (2007). "La STJCE de 13 de septiembre de 2005: ¿una puerta abierta para la competencia penal de las comunidades europeas? Posibles repercusiones para el tratamiento de la delincuencia relacionada con las tecnologías de la comunicación y la información". *Revista de Derecho y Proceso Penal* (núm. 17).

García Rivas, N. (1995). "Los delitos contra la propiedad intelectual en el Código penal de 1995". A: A. Pacheco Guevara (dir.). *Propiedad intelectual: aspectos civiles y penales. Cuadernos de Derecho Judicial, CGPJ* (núm. 34).

García Rivas, N. (2005). "Estructura jurisprudencial del delito de estafa (una revisión crítica de sus elementos objetivos)". A: J. Boix Reig (dir.). *Estafas y falsedades (análisis jurisprudencial)*. Madrid: Iustel.

Gimbernat Ordeig, E. (1995). "Los delitos contra la propiedad intelectual". A: J. A. Martín Pallín (dir.). *Delitos contra la propiedad: Aspectos problemáticos. Cuadernos de Derecho Judicial, CGPJ* (núm. 15).

Gómez Benítez, J. M.; Quintero Olivares, G. (1988). *Protección penal de los derechos de autor y conexos*. Madrid: Civitas.

Gómez Tomillo, M. (2006). *Responsabilidad penal y civil por delitos cometidos a través de Internet: Especial consideración del caso de proveedores de contenidos, servicios, acceso y enlaces* (2a. ed.). Cizur Menor: Aranzadi.

González Rus, J. J. (1999). "Protección penal de sistemas, elementos, datos, documentos y programas informáticos". *RECPC* (núm. 1). En línia: <http://criminet.ugr.es/recpc/recpc_01-14.html>.

González Rus, J. J. (2003). "Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (art. 264.2 del Código penal)". A: J. L. Díez Ripollés, J. L. i altres (ed.). *La ciencia del Derecho penal ante el nuevo siglo. Libro homenaje al profesor doctor D. José Cerezo Mir*. Madrid: Tecnos.

González Rus, J. J. (1986). "Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos". A: *Revista de la Facultad de Derecho de la Universidad Complutense* (núm. 12, monogràfic).

González Rus, J. J. (1988). "Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos". *Poder Judicial* (núm. 9, especial).

González Rus, J. J. (1997). "Protección penal de sistemas, elementos, datos, informaciones, documentos y programas informáticos". *Estudios Jurídicos. Ministerio Fiscal* (núm. 3).

González Rus, J. J. (1999). "Bien jurídico protegido en los delitos contra la propiedad intelectual". En: J. Cerezo Mir i altres (ed.). *El nuevo Código penal: presupuestos y fundamentos. Libro homenaje al Profesor Doctor D. Ángel Torío López*. Granada: Comares.

González Rus, J. J. (2005). "Daños a través de Internet y denegación de servicios". A: *Homenaje al profesor doctor D. Gonzalo Rodríguez Mourullo*. Cizur Menor: Thomson-Civitas.

Gracia Martín, L. (2003). *Prolegómenos para la lucha por la modernización y expansión del Derecho penal y para la crítica del discurso de resistencia*. València: Tirant lo Blanch.

Guardiola García, J. (2003, novembre). "La responsabilidad de los prestadores de servicios de la Sociedad de la Información a la luz de la Ley 34/2002 y de la Directiva 2000/31/CE". *Revista de Derecho de la Universitat de València* (núm. 2). En línia: <http://www.uv.es/revistadret/num2/jguardiola.htm>.

Guerrero Picó, M. del C. (2006). *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal*. Madrid: Civitas.

Guimarães, M. R. (2007). "El pago mediante tarjetas de crédito en el comercio electrónico. Algunos problemas relativos a su naturaleza jurídica, marco contractual y régimen aplicable, desde una perspectiva comparada en los derechos portugués, español y comunitario". A: R. M. Mata y Martín (dir.). *Los medios electrónicos de pago: Problemas jurídicos*. Granada: Comares.

Gutiérrez Francés, M. L. (1996). "Delincuencia económica e informática en el nuevo Código penal". A: M. A. Gallardo Ortiz (dir.). *Ámbito jurídico de las tecnologías de la información. Cuadernos de Derecho Judicial, CGPJ* (núm. 11).

Jofer, R. (1999). *Strafvervolgung im Internet.* Frankfurt: Peter Lang.

Lenckner, T. (1981). *Computerkriminalität und Vermögensdelikte*. Heidelberg/Karlsruhe: C. F. Müller.

Lezertua, M. (2001). "El proyecto de convenio sobre el cybercrimen del Consejo de Europa". A: J. J. López Ortega (dir.). *Internet y Derecho penal. Cuadernos de Derecho Judicial, CGPJ* (núm. 10).

López Barja de Quiroga, J. (1997). "El moderno Derecho penal para una sociedad de riesgos". *Revista del Poder Judicial* (núm. 48).

López Barja de Quiroga, J. (2001). "Problemas actuales de los delitos de estafa, fraude de subvenciones, apropiación indebida y administración desleal". *Manuales de Formación Continuada, CGPJ* (núm. 14, pàg. 429-491, monogràfic sobre dret penal econòmic).

López Moreno, J.; Fernández García, E. M. (2001). "La world wide web como vehículo de delincuencia: supuestos frecuentes". A: J. J. López Ortega (dir.). *Internet y Derecho penal. Cuadernos de Derecho Judicial, CGPJ* (núm. X).

López Ortega, J. J. (2001). "Libertad de expresión y responsabilidad por los contenidos en Internet". A: J. J. López Ortega (dir.). *Internet y Derecho penal. Cuadernos de Derecho Judicial, CGPJ* (núm. X).

López Ortega, J. J. (2006, 4 de maig). "Dimensión jurídico-penal del correo electrónico". *Diario La Ley* (núm. 6475). [Base de dades de *La Ley*].

López Ortega, J. J. (dir.) (2001). *Internet y Derecho penal. Cuadernos de Derecho Judicial, CGPJ* (núm. X).

López-Tarruella Martínez, A. (2009). "Criterio de focalización y forum delicti commissi en las infracciones de propiedad industrial e intelectual en Internet". *Revista de Propiedad Intelectual* (núm. 31).

Magni, S.; Spolidoro, M. S. (1997). "La responsabilità degli operatori in Internet: Profili interni e internazionali". *Il Diritto dell'Informazione e dell'Informatica* (núm. 1).

Mapelli Caffarena, B. (2003). "Consideraciones en torno a los delitos contra la propiedad industrial". A: J. L. Díez Ripollés i altres (ed.). *La ciencia del Derecho penal ante el nuevo siglo. Libro homenaje al profesor doctor D. José Cerezo Mir*. Madrid: Tecnos.

Marchena Gómez, M. (2001, juliol). "El sabotaje informático: entre los delitos de daños y desórdenes públicos". *Actualidad Informática Aranzadi* (núm. 40).

Marín de Espinosa Ceballos, E. B. (2005). "La protección penal de la propiedad intelectual: análisis de las modificaciones introducidas por la Ley Orgánica 15/2003, de 25 de noviembre". *Revista de la Facultad de Derecho de la Universidad de Granada* (núm. 8).

Martín Morales, R. (1995). *El régimen constitucional del secreto de las comunicaciones*.

Martínez González, M. (2007). "Mecanismos de seguridad en el pago electrónico". A: R. M. Mata y Martín (dir.); A. M. Javato Martín (coord.). *Los medios electrónicos de pago: problemas jurídicos*. Granada: Comares.

Martínez-Buján Pérez, C. (2005). *Derecho penal económico y de la empresa: Parte especial* (2a. ed.). València: Tirant lo Blanch.

Mata Barranco, N. de la. (1988). "Utilización abusiva de cajeros automáticos: apropiación de dinero mediante la tarjeta sustraída a su titular". *Poder Judicial* (núm. 9, especial, pàg. 151-174).

Mata Barranco, N. de la. (1989). "Utilización abusiva de cajeros automáticos". *Poder Judicial* (núm. 9).

Mata Martín, R. M. (1995). *El delito de robo con fuerza en las cosas*. València: Tirant lo Blanch.

Mata Martín, R. M. (2001). *Delincuencia informática y Derecho penal*. Madrid: Edisofer.

Mata Martín, R. M. (2005). "Protección penal de la propiedad intelectual y servicios de radiodifusión e interactivos: excesos y equívocos. Su continuación en la reforma de 25-11-03". A: J. C. Carbonell Mateu i altres (coord.). *Estudios penales en homenaje al profesor Cobo del Rosal* (pàg. 619-634). Madrid: Dykinson.

Mata Martín, R. M. (2006). "Perspectivas sobre la protección penal del software". A: C. M. Romeo Casabona (coord.). *El cibercrimen: Nuevos retos jurídico-penales, nuevas respuestas político-criminales* (pàg. 97-152). Granada: Comares.

Mata Martín, R. M. (2006). "Protección penal de la propiedad intelectual y servicios de radiodifusión e interactivos: excesos y equívocos". A: F. Galindo (coord.). *Gobierno, derecho y tecnología: las actividades de los poderes públicos* (pàg. 295-312). Cizur Menor: Thomson-Civitas.

Mata Martín, R. M. (2007). "Medios electrónicos de pago y delitos de estafa". A: R. M. Mata Martín (dir.). *Los medios electrónicos de pago: Problemas jurídicos* (pàg. 319-365). Granada: Comares.

Mata Martín, R. M. (2007). "Protección penal de los derechos del autor en Internet". *Estudios de derecho judicial, CGPJ* (núm. 138, pàg. 61-117, monogràfic sobre les darreres reformes penals).

Mata Martín, R. M. (2007). *Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago: El uso fraudulento de tarjetas y otros instrumentos de pago*. Cizur Menor: Thomson-Aranzadi.

Mata Martín, R. M. (dir.) (2007). *Los medios electrónicos de pago: Problemas jurídicos*. Granada: Comares.

Maza Martín, J. M. (2003). "La necesaria reforma del Código penal en materia de delincuencia Informática". *Estudios Jurídicos, Ministerio Fiscal* (núm. 2, pàg. 285-318).

Maza Martín, J. M. (2002). "La reforma necesaria del Código penal en materia de tarjetas bancarias". A: J. M. Maza Martín (dir.). *Tarjetas bancarias y Derecho penal. Cuadernos de Derecho Judicial, CGPJ* (núm. 6, pàg. 215-257).

Maza Martín, J. M. (dir.) (2002). "Tarjetas bancarias y Derecho penal". *Cuadernos de Derecho Judicial, CGPJ* (núm. 6).

Miró Llinares, F. (2003). *La protección penal de la propiedad intelectual en la sociedad de la información*. Madrid: Dykinson.

Montero, E. (2000). "La responsabilité des prestataires intermédiaires de l'Internet". *Revue Ubiquite* (núm. 5).

Morales García, Ó. (2001). "Criterios de atribución de responsabilidad jurídico penal a los prestadores de servicios e intermediarios de la sociedad de la información". *Revista de Derecho y Proceso Penal*.

Morales García, Ó. (2001). "Malversación, estafa informática y falsedad en documento electrónico. Algunas reflexiones sobre la STS de 30 de octubre de 1998". A: G. Quintero Olivares (dir.). *El nuevo Derecho penal español: Estudios penales en memoria del profesor José Manuel Valle Muñiz*. Pamplona: Aranzadi.

Morales García, Ó. (2003). "La tutela penal de las comunicaciones laborales. A propósito de la estructura típica del artículo 197 del Código penal". A: A. Jurado; M. Jeffery; J. Thibault (coords.). *Tecnología informática y privacidad de los trabajadores*. Cizur Menor: Aranzadi.

Morales García, Ó. (2004). "Política criminal en el contexto tecnológico". A: Ó. Morales García (dir.). *Criminalidad informática: Problemas de responsabilidad. Cuadernos de Derecho Ju-*

dicial, CGPJ (núm. 9). [Publicat també amb el títol "Politica criminale nel contesto tennologico". A: L. Picotti. *Il diritto penale dell'informatica nell'epoca di Internet*. Pàdua: Cedam.]

Morales García, Ó. (2009). "El control informático de la libertad". A: L. R. Ruiz Rodríguez (dir.). *Respuestas internacionales a los retos de la seguridad*. València: Tirant lo Blanch.

Morales Prats, F. (1984). *La tutela penal de la intimidad: privacy e informática*. Barcelona: Destino.

Morales Prats, F. (1996). "Comentario a los artículos 197 y sig.". A: G. Quintero Olivares (dir.); J. M. Valle Muñiz (coord.). *Comentarios al nuevo Código penal*. Pamplona: Aranzadi.

Morales Prats, F. (2002). "El Derecho penal ante la pornografía infantil en Internet". A: F. Morales Prats; Ó. Morales García (coord.). *Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet*. Cizur Menor: Aranzadi.

Morales Prats, F. (2005). "Internet. Derecho penal y derechos fundamentales". A: Murillo Villar (coord.). *Estudios jurídicos sobre la sociedad de la información y nuevas tecnologías: Con motivo del XX aniversario de la facultad de derecho*. Burgos: Universidad de Burgos.

Morales Prats, F.; Morales García, Ó. (coord.) (2002). *Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet*. Cizur Menor: Aranzadi.

Morillas Cueva, L. (2005). "El artículo 255". A: M. Cobo del Rosal (dir.). *Comentarios al Código penal. Tomo VIII. Delitos contra el patrimonio y contra el orden socioeconómico: Artículos 234 a 272* (pàg. 511-549). Madrid: EDERSA.

Morillas Cueva, L. (2008). "Nuevas tendencias del Derecho penal. Una reflexión dirigida a la cibercriminalidad". *Cuadernos de Política Criminal* (núm. 94, pàg. 5-32).

Morris, S. (2004). *The future of netcrime now: Part 1 - Threats and challenges*. Londres: Home Office.

Muñoz Conde, F. (1995). "Falsedad y estafa mediante abuso de crédito e instrumentos crediticios". A: F. Muñoz Conde (dir.). *Falsedad y defraudaciones. Cuadernos de Derecho Judicial, CGPJ* (núm. 11, pàg. 133-165).

Muñoz Conde, F. (2005). "Las reformas de la parte especial del Derecho penal español en el 2003: de la "tolerancia cero" al "Derecho penal del enemigo". *Revista General de Derecho Penal* (núm. 3).

Muñoz Cuesta, F. J. (2009). "Estafa informática: introducción de datos falsos en operaciones mercantiles vía Internet que motivan transferencias de dinero no consentidas". *Revista Aranzadi Doctrinal* (núm. 37).

Muñoz de Morales Romero, M. (2007). "La aplicación del principio de interpretación conforme a las decisiones-marco: ¿hacia el efecto directo?: especial referencia al caso Pupino". A: L. Arroyo Zapatero; A. Nieto Martín (dir.). *El Derecho penal de la Unión Europea: Situación actual y perspectivas de futuro*. Conca: Ediciones de la Universidad de Castilla-La Mancha.

Muñoz Paredes, J. M. (2005). *Nuevas tecnologías en el funcionamiento de las juntas generales y de los consejos de administración*. Madrid: Civitas.

Müssig, B. (2002). "Desmaterialización del bien jurídico y de la política criminal. Sobre las perspectivas y los fundamentos de una teoría del bien jurídico crítica hacia el sistema". *RDPC* (núm. 9).

Nieto Martín, A. (2007). "Posibilidades y límites de la armonización del Derecho penal nacional tras Comisión v. Consejo (comentario a la STJCE, asunto C-176/03, de 13-9-2005)". A: L. Arroyo Zapatero; A. Nieto Martín (dir.). *El Derecho penal de la Unión Europea: Situación actual y perspectivas de futuro*. Conca: Ediciones de la Universidad de Castilla-La Mancha.

Núñez Castaño, E. (1998). *La estafa de crédito*. València: Tirant lo Blanch.

Orts Berenguer, E. (1998). "Propiedad intelectual, nuevas tecnologías y Derecho penal". A: E. Fernández Masiá i altres. *Los derechos de propiedad intelectual en la nueva sociedad de la información (perspectivas de derecho civil, procesal, penal e internacional privado)*. Granada: Comares.

Orts Berenguer, E.; Roig Torres, M. (2001). *Delitos informáticos y delitos comunes cometidos a través de la informática*. València: Tirant lo Blanch.

Palma Herrera, J. M. (2005). "Las redes P2P de intercambio de archivos desde la perspectiva del Derecho penal". A: J. C. Carbonell Mateu i altres (coord.). *Estudios penales en homenaje al profesor Cobo del Rosal*. Madrid: Dykinson.

Paredes Castañón, J. M. (2001). *La protección penal de las patentes e innovaciones tecnológicas*. Madrid: McGraw-Hill.

Peguera Poch, M. (2007). *La exclusión de responsabilidad de los intermediarios en Internet*. Granada: Comares.

Pérez Manzano, M. (1998). "Las defraudaciones (I). Las estafas". A: M. Bajo Fernández (coord.). *Compendio de Derecho penal: Parte especial* (vol. II). Madrid: Centro de Estudios Ramón Areces.

Picotti, L. (2002). "Aspectos supranacionales de la responsabilidad penal de los prestadores de acceso y Servicio en Internet" (traducció de l'italià d'Óscar Morales García). A: F. Morales Prats; Ó. Morales García (coord.). *Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet*. Cizur Menor: Aranzadi.

Queralt Jiménez, J. J. (2005). "Tres ejemplos de reciente política legislativa. Del olvido del Derecho penal liberal al amasijo de letras". A: J. C. Carbonell Mateu i altres (coord.). *Estudios penales en homenaje al profesor Cobo del Rosal* (pàg. 749-762). Madrid: Dykinson.

Queralt Jiménez, J. J. (2008). *Derecho penal español: Parte especial* (5a. ed.). Barcelona: Atelier.

Quintero Olivares, G. (1999). *Manual de Derecho penal: Parte general* (amb la col·laboració de F. Morales Prats i J. M. Prats Canut). Cizur Menor: Aranzadi.

Quintero Olivares, G. (2001). "Internet y propiedad intelectual". A: J. J. López Ortega (dir.). *Internet y Derecho penal. Cuadernos de Derecho Judicial* (núm. X).

Ribas, J. (1999). "Editorial Aranzadi gana el primer juicio en España por la comercialización ilegal de sus bases de datos en Internet". *AJA* (núm. 401).

Rodríguez Mourullo, G.; Alonso Gallo, J.; Lascuraín Sánchez, J. A. (2002). "Derecho penal e Internet". A: J. Cremades; M. A. Fernández-Ordóñez; R. Illescas (coord.). *Régimen jurídico de Internet*. Madrid: La Ley.

Romeo Casabona, C. M. (1988). "La protección penal del software en el derecho español". *Actualidad Penal* (núm. 2).

Romeo Casabona, C. M. (1991). "Los delitos de daños en el ámbito informático". *CPC* (núm. 43).

Romeo Casabona, C. M. (1987). "La utilización abusiva de tarjetas de crédito". *Revista de Derecho Bancario y Bursátil* (núm. 26).

Romeo Casabona, C. M. (1988). "Delitos cometidos con la utilización de tarjetas de crédito, en especial en cajeros automáticos". *Poder Judicial* (núm. 9, especial).

Romeo Casabona, C. M. (1988). *Poder informático y seguridad jurídica*. Madrid: Fundesco.

Romeo Casabona, C. M. (1993). "Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías". *Poder Judicial* (núm. 31, pàg. 163-204).

Romeo Casabona, C. M. (2004). *Los delitos de descubrimiento y revelación de secretos*. València: Tirant lo Blanch.

Romeo Casabona, C. M. (2006). "De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal". A: C. M. Romeo Casabona (coord.). *El cibercrimen: Nuevos retos jurídico-penales, nuevas respuestas político-criminales*. Granada: Comares.

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

Rovira del Canto, E. (2003). "Hacia una expansión doctrinal y fáctica del fraude informático". *Revista Aranzadi de Derecho y Nuevas Tecnologías* (núm. 3, pàg. 109-143).

Rovira del Canto, E. (2001). "Tratamiento penal sustantivo de la falsificación informática". A: J. J. López Ortega (dir.). *Internet y Derecho penal. Cuadernos de Derecho Judicial, CGPJ* (núm. 10, pàg. 457-508).

Rovira del Canto, E. (2002). *Delincuencia informática y fraudes informáticos*. Granada: Comares.

Ruiz Rodríguez, L. R. (2006). "Uso ilícito y falsificación de tarjetas bancarias". *IDP. Revista de Internet, Derecho y Política* (núm. 3).

Sánchez García de Paz, M. I. (1999). *El moderno Derecho penal y la anticipación de la tutela penal*. Valladolid: Universidad de Valladolid.

Sanz Morán, J. A. (1993). *Elementos subjetivos de justificación*. Barcelona: Bosch.

Segura García, M. J. (1995). *Derecho penal y propiedad industrial*. Madrid: Civitas.

Segura García, M. J. (2005). *Los delitos contra la propiedad industrial en el Código penal de 1995*. València: Tirant lo Blanch.

Seminara, S. (1997). "La pirateria su Internet e il Diritto Penale". *Rivista Trimestrale di Diritto Penale dell'Economia* (núm. 1-2).

Serrano Gómez, E. (2000). *La propiedad intelectual y las nuevas tecnologías*. Madrid: Civitas.

Sieber, U. (1980). *Computerkriminalität und Strafrecht* (2a. ed.). Colònia/Berlín/Bonn/Munic: Carl Heymanns.

Sieber, U. (1986). *The International Handbook on Computer Crime*. Nova York: John Wiley & Sons, Inc.

Sieber, U. (1996). "Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen (II)". *Juristenzeiutung (JZ)* (núm. 9). En línia: <http://www.jura.uni-wuerzburg.de/lst/sieber>.

Sieber, U. (1998). "The 'compuserve' judgment of the local court Munich dated May 28, 1998". *Multimedia und Recht* (núm. 8, pàg. 429 seg.).

Sieber, U. (1999). "Die Rechtliche Verantwortlichkeit im Internet. Grundlagen, Ziele und Auslegung von Paragraph 5 TDG und paragraph 5 MDStV". *Multimedia und Recht* (núm. 2). En línia: <http://www.jura.uni.wuerzburg.d/lst/sieber/mmr/5mmrbei_dt.HTM>.

Sieber, U. (1999). "Strafrecht und strafprozeßrecht". A: U. Sieber; T. Hoeren. *Handbuch Multimedia-Recht. Rechtsfragen des elektronischen Geschäftsverkehrs Loseblatt-Ausgabe*. Munic: C. H. Beck.

Sieber, U. (2008). "Legal Aspects of Computer-Related Crime in the Information Society -concrime Study-, prepared for the European Comission" [document en línia]. Versió 1.0, 1 de gener de 1998: <http://ec.europa.eu/archives/ISPO/legal/en/comcrime/sieber.html>.

Silva Sánchez, J. M. (2006). *La expansión del Derecho penal: Aspectos de la política criminal en las sociedades postindustriales* (2a. ed.). Montevideo / Buenos Aires: BdeF.

Suárez González, C. J. (2003). "Derecho penal y riesgos tecnológicos". A: L. Arroyo Zapatero i altres (coord.). *Crítica y justificación del Derecho penal en el cambio de siglo*. Conca: Ediciones de la Universidad de Castilla-La Mancha.

Tabarelli de Fatis, S. (2002). "La controvertida regulación jurídico penal de la difamación a través de Internet". A: F. Morales Prats; Ó. Morales García (coord.). *Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet*. Cizur Menor: Aranzadi.

Tasende Calvo, J. (2003, 9-15 de juny). "Los delitos contra la propiedad intelectual. Tipicidad y doctrina legal". *Actualidad Penal* (núm. 24). [Base de dades de *La Ley*.]

Tasende Calvo, J. (dir.) (2004). *Delitos contra el patrimonio: Delitos de apoderamiento. Cuadernos de Derecho Judicial, CGPJ* (núm. 13).

Valmaña Ochaita, S. (2004). "La tarjeta de crédito como llave falsa en el delito de robo con fuerza en las cosas". *La Ley Penal* (núm. 7).

Valle Muñiz, J. M. (1987). *El delito de estafa: Delimitación jurídico penal con el fraude civil*. Barcelona: Bosch.

Valle Muñiz, J. M. (1994). *El elemento subjetivo de justificación y la graduación del injusto penal*. Barcelona: PPU.

Valle Muñiz, J. M. (1996). "Comentario al artículo 248 CP". A: G. Quintero Olivares (dir.); J. M. Valle Muñiz (coord.). *Comentarios al nuevo Código penal*. Pamplona: Aranzadi.

Villacampa Estiarte, C. (1999). *La falsedad documental: análisis jurídico-penal*. Barcelona: Cedecs.

Vives Antón, T. S. (1996). "Comentario al artículo 30 CP". A: T. S. Vives Antón (coord.). *Comentarios al Código penal de 1995 (I)*. València: Tirant lo Blanch.

Widmer, U.; Bähler, K. (1996). "Strafrechtliche und aktienrechtliche Haftung von Internet Providern". *Computer und Recht* (núm. 3).

Xalabarder Plantada, R. (2002). "Infracciones de propiedad intelectual y la Digital Millenium Copyright Act". A: F. Morales Prats; Ó. Morales García (coord.). *Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet*. Cizur Menor: Aranzadi.

Zencovich, Z. "La pretesa estensione alla telematica del regime della stampa" [document en línia]. <http://www.beta.it/edit/zencovich.html>.