EL FRAU I LA DELINQÜÈNCIA INFORMÀTICA: UN PROBLEMA JURÍDIC I ÈTIC

Miquel Barceló

Introducció

Tecnologies amb molt dinamisme com la informàtica generen amb gran rapidesa possibilitats d'ús i abús (vegeu [BAR 87]) que, naturalment, van per davant de la possibilitat de regulació jurídica de les seves conseqüències i responsabilitats.

Per a la tipificació de les noves possibilitats delictuoses que ofereix una tecnologia ubiqua i multiforme com la informàtica, calen esforços conjunts de juristes i informàtics i això porta, de moment, a la formulació de dues menes de discurs que empren llenguatges especialitzats i clarament diferents com passa, en certa forma, amb tots els llenguatges especialitzats.

Els juristes disposen d'un vocabulari tècnic propi que resulta estrany als informàtics, al mateix temps que els informàtics són coneguts pel caràcter tal vegada exageradament críptic del seu vocabulari tècnic que, evidentment, també resulta estrany als juristes. La dificultat d'apropar conceptes formulats amb vocabularis distanciats és un dels problemes implícits en el tractament d'un tema com el del delicte o frau informàtic.

Cal advertir doncs, que aquest text tracta el tema del frau i la delinqüència informàtica des del punt de vista d'un informàtic tot i amb la voluntat de reduir l'especificitat del propi llenguatge tècnic informàtic per a afavorir la comprensió dels lectors amb formació jurídica.

El text fa un repàs a la problemàtica general del frau i la delinqüència informàtica centrada més en el problema en sí que no pas en l'especificitat de la legislació corresponent al tema. D'altra banda, cal advertir que, per a un professional informàtic interessat en els problemes propis de l'impacte social de la tecnologia informàtica, resulta paradoxalment més fàcil estar al dia de les novetats en la legislació nordamericana i anglosaxona (que l'informàtic pot fins i tot trobar en la literatura tècnica de la professió sovint de procedència anglosaxona) que no pas en la realitat de l'encara incipient legislació espanyola sobre el tema.

Cal advertir també aquí sobre la voluntat d'aquest text per exposar i raonar la convicció de que la pròpia característica innovadora del fet informàtic fa i farà que la possible tipificació del delicte vagi sempre per darrera de la realitat de les possibilitats de frau que la informàtica presenta. Per aquesta raó, el problema és, alhora, jurídic i ètic ja que planteja temes d'ètica i deontologia professional que afecten a la totalitat dels informàtics com a grup professional. Com veurem, resulta prou significativa en aquest sentit l'evolució del pensament i dels treballs d'una personalitat como Donn B. Parker, pioner en l'estudi del frau i delicte informàtic ([PAR 76] i [PAR 83]), que ha acabat preocupant-se principalment dels problemes ètics que l'activitat informàtica planteja ([PAR 81] i [PSB 90]).

Delicte i frau

Quan es tria parlar precisament de frau i delinqüència informàtica de forma genèrica és, potser, per la dificultat de parlar concretament del "*delicte informàtic*" com a tal. Sovint s'enten el delicte informàtic, como ho fan per exemple Castillo i Ramallo a [CAR 89], com aquella acció dolosa que provoca un perjudici a persones o entitats i en la que es fan intervenir dispositius o programes informàtics. Però, més senzillament, la consideració d'una activitat com a delictuosa suposa necessariament que el possible delicte hagi estat establert com a tal a l'ordenació del dret positiu d'un determinat país i així ho recullen, per exemple, Vázquez i Barroso a [VAB 93].

De fet, la legislació sobre delictes informàtics és, avui, molt limitada a la majoria dels paï sos i potser encara més a Espanya. Les raons d'aquest fet seran analitzades més endavant a la llum de les pròpies característiques innovadores de la tecnologia informàtica i de les múltiples possibilitats que ofereix per al seu ús ja sia de forma lícita com fraudulenta.

Per això és encara molt comú evitar parlar de "*delicte informàtic*" i referir-se al "*frau informàtic*" o a una genèrica "*delinqüència informàtica*" com es farà en aquest text. Com Castillo i Ramallo a [CAR 89], entenem per frau aquella conducta realitzada mitjançant un sistema informàtic amb la que es vol aconseguir un benefici il.lícit.

Autors com els ja esmentats Vázquez i Barroso a [VAB 93] limiten el frau informàtic als actes fruit de la intencionalitat i realitzats amb voluntat d'obtenir un benefici propi i, de passada, provocar un perjudici aliè. Per això parlen també d'un altre tipus de frau informàtic no intencionat, que Vázquez i Barroso anomenen "*error informàtic*", fruit d'un error humà en la utilització d'un sistema informàtic o com a conseqüència d'un defecte del hardware o del software. En el cas de l'error informàtic, pot no haver-hi benefici directe per part de qui causa el funcionament erroni d'un sistema informàtic, però sí es pot donar un perjudici per altres dels usuaris o pels propietaris del sistema.

Vulnerabilitat de la societat de la informació

Un sistema d'informació és aquell que recull, emmagatzema, processa i distribueix informació. De fet, els sistemes d'informació no són pas una novetat recent i es pot ben dir que n'hi ha hagut sempre i en tot tipus d'activitats humanes. Però és precisament la potencialitat de la seva implementació basada en la tecnologia informàtica i en les comunicacions electròniques el fet que porta a plantejar-se qüestions com la que ara ens ocupa.

A [BAR 92] es presenta el concepte del *factor multiplicador d'una tecnologia* com el nombre de vegades que la tecnologia en estudi és capaç de millorar la funció o l'objectiu que li ha estat encarregada. Els factors multiplicadors de les tecnologies convencionals, tot i la seva gran potencialitat, tenen un ordre de magnitud limitat: 15 en el cas de l'automoció, 150 en el cas de l'aviació, 100 en el cas de l'agricultura (10 aportat per l'invent de l'arada i un altre factor 10 per la utilització de l'adob químic), o fins i tot un factor de l'ordre del miler (1000) en el cas de la revolució industrial.

El fet diferenciador de la tecnologia informàtica dels moderns sistemes d'informació distribuï ts rau en un factor multiplicador molt superior que assoleix, fins i tot, una magnitud de l'ordre del bilió com a resultat de la conjunció sinèrgica de la tecnologia informàtica del procés de dades i de la tecnologia paral.lela de les comunicacions informàtiques. Ambdues presenten, individualment, un factor multiplicador de l'ordre del milió ja que, respectivament, multipliquen la velocitat "manual" del procés i de la comunicació de dades per un factor de l'ordre del milió.

I aquesta potencialitat que implica el gran factor multiplicador de la tecnologia informàtica ha estat desenvolupada en un període temporal francament breu. Quan tot just fa una cinquantena d'anys de la presentació pública del primer ordinador electrònic (l'ENIAC, presentat

el 15 de febrer de 1941), el canvi ha estat significatiu tant en l'augment de potència com en la miniaturització dels sistemes. Forrester a [FOR 85] esmenta un exemple ja clàssic: si l'automoció hagués tingut un desenvolupament semblant, avui podríem adquirir un Rolls Royce per menys de 300 pessetes i, a més, aquest vehicle disposaria d'una potència comparable a la d'un transatlàntic com el "Queen Elizabeth" i fòra capaç de recórrer un milió de quilòmetres (unes 25 voltes al món) només amb un litre de benzina. Tot un somni que, de fet, en l'àmbit de la informàtica, ha estat tecnològicament possible.

Aquestes característiques particulars han portat a parlar d'una nova revolució industrial anomenada "de les tecnologies de la informació" que es fa clarament palesa en l'activitat quotidiana del món modern. Textos com [BAR 87] o [FOR 85] analitzen i detallen algunes de les possibilitats i problemes que presenta aquesta "*revolució de les tecnologies de la informació*".

Paral.lelament a les potencialitats que ofereix, una tecnologia transformadora com la informàtica, sorgeixen també un creixent nombre de riscos i perills que són, en certa forma, proporcionals a la gran potencialitat de les tecnologies de la informació. Però, precisament el fet d'aquesta evolució tan ràpida del fet informàtic suposa, d'una part, l'existència d'una inevitable separació temporal entre el fet informàtic a regular jurídicament i el naixement de la llei que el regula i, el que és més important i específic, la inevitable temporalitat del dret davant noves tecnologies essencialment canviants com la informàtica.

En els darrers anys és ja freqüent entre els informàtics la reflexió sobre la vulnerabilitat d'una societat sotmesa a les possibilitats de les tecnologies de la informació. Fins i tot institucions com la IFIP (*International Federation for Information Processing* - federació internacional pel procés de la informació, la més gran organització mundial creada al voltant de les tecnologies de la informació) s'han preocupat del tema i, en el seu recent congrés mundial de 1992, es presentà el material de base per a l'estudi sobre *Risc i vulnerabilitat en una societat artificial i basada en la informació* (vegeu [BER 92]), un material de referència (*paper of position*), elaborat pel grup de treball 9.2 (*Working Group* 9.2).

El text de la IFIP posa l'èmfasi en tres exemples que considera típics de la vulnerabilitat creixent d'una organització social que reposa de forma quasi absoluta en les tecnologies de la informació, allò que hom anomena una "*societat de la informació*". Els casos allí esmentats fan referència, per exemple, al col.lapse de la borsa de Wall Street el 19 d'octubre de 1987 que alguns comentaristes fan dependre de la nova agilitat de resposta dels inversors al canvi de cotitzacions, gràcies a programes informàtics que incorporen models acurats del comportament del mercat de valors, ajudats per l'efectivitat dels aparells de comunicació informatitzats que dominaven ja la borsa de Wall Street. També és un cas evident de vulnerabilitat els problemes potencials (i també reals en certs casos de trist record fins i tot a Espanya) als hospitals cada vegada més informatitzats i on l'error o el mal ús dels sistemes de la informàtica mèdica o administrativa de gestió pot portar conseqüències greus amb perill de mort. Berleur, autor del report del WG9.2 de la IFIP, esmenta també el problema, cada vegada més greu, de l'intercanvi electrònic de dades i intangibles i la nova consideració del "document electrònic" que, per exemple, l'ordenament jurídic espanyol sembla acceptar a partir precisament de la llei reguladora del mercat de valors de 28 de juliol de 1988 que ja accepta el "registre en compte" o l'anotació en compte com a cas concret de document electrònic.

Noves necessitats i nous plantejaments

Les noves possibilitats que ofereix la societat de la informació exigeixen unes noves respostes tant a l'àmbit ètic com al jurídic. Allò que per Mason, a [MAS 86], eren quatre temes ètics ineludibles, corresponents a l'era de la informació, es converteixen en el comentari de Morris, a [MOR 92], en els "*quatre drets bàsics que son rellevants en l'era de la informació*".

Aquestes exigències ètiques o també, en la formulació de Morris, dret bàsics són:

A- **Privacitat** (*privacity*, que sovint es tradueix com hem fet aquí amb l'anglicisme ja habitual entre nosaltres, en lloc del terme propi: "intimitat"), - que fa referència a la necessitat de protegir la informació d'un ús no autoritzat.

B- **Exactitud** (*accuracy*), - ja que cal una alta qualitat en la informació per a que els processos de presa de decisions que en ella es recolzen siguin efectius.

C- **Propietat** (*property*), - ja que cal protegir el coneixement (*know how*) que hi ha emmagatzemat als ordinadors tant pel que fa al hardware com el software (dades i programes i, en definitiva, sistemes)

D- **Accés** (*acces*), - ja que cal permetre un accés adequat a la informació, però de forma estrictament controlada.

Per autors com Morris, aquestes exigències jurídiques, convertides per ell en "drets", són el marc de referència d'una crida ineludible a la necessitat d'un component ètic en la conducta professional dels especialistes en sistemes d'informació. De fet, els especialistes són els qui disposen de més poder per malmenar els sistemes informàtics i atemptar contra aquests nous drets bàsics de l'era de la informació. Encara que, convé recordar-ho, no són els únics.

En aquest sentit, altres autors com Del Peso (vegeu [DPE 89], tot i reconeixent el fet de que "*l'activitat informàtica és molt vulnerable*", i defensant explícitament el paper i la funció dels professionals de l'auditoria informàtica, sintetitzava ja cinq grups de figures, més o menys diferenciades, pròpies de la delinqüència informàtica:

1- **Frau informàtic:** ús indegut o manipulació fraudulenta d'elements informàtics de qualsevol tipus que permeten un benefici il.lícit

2- **Hacking** o "terrorisme lògic": que inclou els casos de vandalisme, terrorisme, destrucció, etc. que provoquen perjudicis i són motivats per venjances, xantatges, sabotatge o, fins i tot, per una molt *sui generis* "curiositat intel.lectual" que caracteritzava els primers *hackers* o manipuladors no autoritzats de sistemes informàtics.

3- **Accions físiques** contra la integritat dels sistemes informàtics

4- **Atemptats contra el dret a la intimitat** (privacitat) de les persones, realitzats gràcies a l'existència de bases de dades informatitzades i les possibilitats que presenta la mateixa informàtica per vulnerar els sovint escassos sistemes de seguretat operatius.

5- **Atemptats a la propietat intel.lectual informàtica**, que, de forma exageradament simplificada, hom anomena col.loquialment "pirateria del software", oblidant també la possibilitat (que ja ha estat realitat) d'una equivalent "pirateria" del hardware que, de fet, correspon a un cas típic d'espionatge industrial.

Resulta fàcil posar en relació les cinq figures delictuoses de Del Peso amb els drets que recull Morris abans esmentats, però allò que aquí interessa és constatar que algunes d'aquestes accions il.lícites poden estar ja recollides en l'ordenament legal, tot i que sovint s'hagi fet amb independència de la tipicitat exclusiva del fet informàtic. Es tracta, en aquest cas, d'una regulació per analogia que, com veurem, sembla insuficient per a cobrir totes les particularitats del fet informàtic.

Per exemple, les accions il.lícites incloses per Del Peso en el tercer grup (accions físiques contra la integritat dels sistemes informàtics), que semblen limitar-se al hardware, equivalen a les que es poden cometre contra la integritat de qualsevol tipus de maquinaria i cal pensar que ja estan convenientment recollides al Codi Penal. Aquest és un cas on la regulació per analogia ha de resultar suficient.

Igualment, les accions il.lícites incloses en el cinquè grup (atemptats a la propietat intel.lectual informàtica) incideixen en un aspecte concret de la protecció intel.lectual que ja es

contempla explícitament com a cas particular a la llei espanyola de Propietat Intel.lectual d'11 de novembre de 1987. Hi ha, en aquest cas, una regulació per analogia, però també una referència explícita a la particularitat del fet informàtic.

Però també cal tenir en compte que, per l'especificitat de la informàtica, hi ha aspectes de les accions il.lícites abans esmentades que no estan clarament recollides en els codis jurídics, i que difícilment ho estaran precisament per la multiplicitat, dinamisme i variabilitat de la tecnologia informàtica.

De fet, com a complement de les accions il.lícites del tercer grup, hi ha també la possibilitat de les "accions lògiques" que afecten al software (dades i programes), que Del Peso separa de les corresponents al hardware i, en el fons, utilitza per cobrir totes les altres vessants de figures il.lícites. De fet, tipologies com les de Del Peso intenten ordenar un conjunt molt heterogeni de possibilitats de frau i delinqüència ofertes per la informàtica.

Algunes de les figures il.lícites abans esmentades requereixen un tractament específic. Així les del grup quart (atemptats contra el dret a la intimitat o privacitat) han generat en el nostre país el naixement de la llei orgànica de regulació del tractament automatitzat de les dades de caràcter personal (LOARTAD) tot i que, en aquest cas concret, els professionals informàtics més sensibles (associacions professionals com ATI o grups com la Comissió de LLibertats i Informàtica, CLI) critiquen la manca de control de les dades en poder de l'Administració i la parcialitat de l'agència de protecció de dades creada a la LOARTAD que resulta, de fet, massa depenent del poder executiu, amb tota seguretat un dels més necessitats de control en aquest aspecte. Tot i que aquest no és el tema central d'aquest treball, resulta convenient esmentar aquí l'interesant estudi comparatiu sobre el tractament del tema de la protecció de la privacitat a Europa que realitza Marcelo a [MAR 91].

També, pel que fa referència a les accions il.lícites del grup cinquè (atemptats a la propietat intel.lectual informàtica), cal pensar que hi ha prou problemes pendents ja que, per exemple, per altres raons que no resulta adient exposar aquí, la llei espanyola de patents de 20 de març de 1986, en el seu article quart, rebutja la possibilitat de patentar el software seguint, en aquest punt, un acord general europeu. Posteriorment, el Consell de la Comunitat Europea ha elaborat una directriu que defensa explicitament els drets d'autor dels creadors del software (14 de maig de 1991).

No hem esmentat fins ara les accions il.lícites que Del Peso inclou en el primer i segon grup (frau informàtic i *hacking*) que seran tractades amb prou detall més endavant, com a tema central d'aquest treball.

Internacionalització dels problemes del dret informàtic

Cal ara referir-se també a la internacionalització dels problemes jurídics creats per la informàtica. Les xarxes d'ordinador i el seu abast internacional permeten la difusió de programes, dades i, en definitiva, sistemes per damunt de les fronteres estatals. Per això resulta de gran utilitat atenir-se als resultats del dret comparat en l'àmbit internacional, en concret pel que fa referència al fet informàtic. En aquest sentit cal destacar els treballs de Sieber ([SIE 86] i [SIE 90] per exemple) o estudis puntuals sobre lleis concretes com el que fa Wasik, a [WAS 92], sobre la *Computer Misuse Act* que es convertí en llei al Regne Unit l'agost de 1990.

El treball de Sieber recull com a tret principal el fet de que els sistemes informàtics deixen de tractar amb objectes amb corporeï tat física, per a ésser el suport de nous objectes sense realitat física com és la informació i la seva distribució. Hem esmentat, abans, l'exemple del "document informàtic" ja acceptat fins i tot en l'ordenament jurídic espanyol (registre en compte acceptat per la llei reguladora del mercat de valors), però, per lluitar amb eficiència contra el frau i

la delinqüència informàtica, caldrà ampliar aquesta idea i reconèixer tota una munió d'aquest tipus d'objectes no corporis.

Precisament per això, Sieber suggereix que el canvi de paradigma que representa el pas d'objectes corporis a incorporis justifica la necessitat de lleis específiques pròpies del fet informàtic. En aquest sentit Sieber, com a resultat del seu treball de dret comparat, és de l'opinió que "*el règim legal per a la informació no es pot derivar per analogia de les reglamentacions per als objectes corporis, cal que sigui fonamentat de forma separada*". Sieber es concentra en l'especificitat de la informació i de les tecnologies que li estan associades per renunciar a una altra de les possibilitats de tractar legalment el fet informàtic: la utilització per analogia de lleis ja existents sobre el robatori, la protecció de la propietat, el vandalisme, etc.

De fet, els estudis sobre legislació comparada marquen clarament aquestes dues tendències en el tractament legal del fet informàtic: lleis específiques o aplicació analògica de lleis ja existents. En realitat, les dues opcions no semblen excloure's i es donen conjuntament en l'ordenament legal de diversos països. Malgrat tot, és fàcil estar d'acord amb Sieber. Tot i que la incorporeïtat dels objectes informàtics i les diferents característiques de la informació són només una raó entre moltes, cal pensar en la necessitat de lleis específiques per tractar de forma adient el frau i la delinqüència informàtica.

El que sí cal constatar és que, tal com hem vingut suggerint repetides vegades fins ara, la potencialitat de les tecnologies de la informació, el caràcter "revolucionari" del seu impacte en les organitzacions socials, el dinamisme propi de la informàtica i la multiplicitat de formes que pot prendre el frau i la delinqüència informàtica, fan pràcticament impossible esperar d'un ordenament jurídic la resposta completa a totes les modalitats de frau i delicte informàtics. Per això, com passa a d'altres professions de gran incidència social, cal comptar també, pel bé de la societat, en un complet codi ètic i deontològic que governi l'actuació dels professionals informàtics i, de fet, eviti gran part dels perills de frau que ofereixen les noves tecnologies de la informació.

Tipologia del frau informàtic

Quan es fa esment del frau informàtic, resulta ja habitual prendre com a referència els treballs de Donn B. Parker, consultor senior del SRI (Stanford Research Institute). Parker estudia el tema del frau i la delinqüència informàtica des dels anys setanta, atenent a les que ell anomena "quatre dimensions" del problema que sintetitza en:

- el modus operandi,
- la tipologia dels autors dels fraus informàtics,
- els problemes ètics associats, i
- els precedents legals ja existents i la legislació encara pendent sobre aquest afer.

El tractament de les dues primeres "dimensions" del problema va ser desenvolupat per Parker en el primer dels seus llibres clàssics sobre el delicte informàtic, [PAR 76]. El text de 1983, [PAR 83], utilitza una perspectiva històrica per continuar l'anàlisi ja fet i encetar el tractament de les dues darreres "dimensions". El caire de pioner d'aquest treball li ha donat una gran difusió i justifica, tal vegada, que se'n faci sovint referència fins i tot sense citar l'origen. També explica l'existència de treballs que pretenen complementar l'estudi de Parker, per fer aparèixer noves aportacions sobre el mètode de detecció del frau o les evidències que poden suggerir la seva presència com es fa, per exemple, en el quadre recollit a [HIS 81].

D'aquesta tipologia tan difosa del modus operandi del frau informàtic, cal remarcar el seu caire conjuntural i la necessitat evident de posar-la contínuament al dia per recollir les noves tècniques que el dinamisme de la tecnologia informàtica fa sorgir amb els nous sistemes. Malgrat tot i seguint una tradició ja inevitable, esmentarem aquí (com es fa a tants d'altres llocs) els mètodes que Parker recollia fins a 1983 com a més característics i que són:

- **introducció de dades falses** (*data diddling*) que ve a ésser la manipulació fraudulenta de les transaccions d'entrada a un sistema informàtic per a introduir-hi moviments falsos o eliminar l'entrada d'operacions reals que haurien d'haver estat introduï des.
- **cavall de Troia** (*Trojan horse*) que fa incloure en un programa normal un conjunt d'instruccions no autoritzades que actuï , en certs casos, de forma diferent en allò que havia estat previst, evidentment, en benefici de l'autor o per a sabotejar l'usuari.
- **tècnica del salami** (*salami technique*), de nom prou atractiu, i que consisteix en petites manipulacions que, sumades, fan un gran frau. És habitual citar en aquest punt el no demostrat i quasi mític cas de la desviació fraudulenta del resultat d'arrodonir per defecte els cèntims en transferències bancàries o nòmines, un sistema que, evidentment, pot resultar atractiu a Nord-Amèrica però no tant al nostre país.
- **ús no autoritzat de programes especials** (*superzapping*) que consisteix en utilitzar de forma no autoritzada qualsevol programa d'utilitat (de vegades fins i tot suposadament "provisional") que permeti d'alterar dades i resultats o obtenir informació. El nom en anglès deriva d'un vell i molt conegut programa de servei de certs sistemes IBM anomenat, precisament, "superzap".
- **portes falses** (*trap doors*) que consisteix en fer servir "forats" i defectes en la seguretat dels sistemes i "entrades especials" que es posen, sovint amb caire de provisionalitat, en els programes per fer més àgil el seu procés de prova i depuració i que, a l'hora de la instal.lació de la versió definitiva, no es treuen.
- **bombes lògiques** (*logic bombs*) que permeten fer un tipus diferit de sabotatge amb unes rutines ocultes (la bomba lògica) que, per exemple, a cada execució d'un programa fa anar un comptador que, en arribar a un cert valor, executa una operació destructiva. És un procediment que, regulat per un comptador o per una data clau, s'ha convertit en el més habitual en la majoria de virus informàtics.
- **atacs asíncrons** (*asynchronous attacs*) que aprofita possibilitats del sistema operatiu dels ordinadors per introduir, per exemple en certs punts de recuperació del sistema, la possibilitat d'un rellançament en condicions diferents de les autoritzades. Cal esmentar que, pensada a mitjans dels anys setanta, aquesta és una modalitat que era, llavors, de difícil realització tècnica. Avui caldria incloure en aquest apartat casos com el fet d'escriure un programa que reprodueix la pantalla d'entrada a un sistema i que, quan l'usuari autoritzat entra la seva paraula de pas, emmagatzema aquesta informació en un fitxer a disposició del perpetrador del frau, que obté així la possibilitat d'un accés que li estava prohibit.
- **recollida d'informació residual** (*scavenging*) que consisteix en aprofitar tot tipus de deixalles (llistats i manuals tirats a la paperera i no destruï ts, cintes, estat final de la memòria en finalitzar l'execució d'un programa, etc) per obtenir informació reservada i sensible.
- **divulgació no autoritzada de dades reservades** (*data leakage*) o divulgació no autoritzada d'informació secreta, obtenint dades reservades per espionatge o adquisició fraudulenta a partir de conjunts d'informació pensats amb d'altra finalitat, per exemple, a partir del cens electoral, d'informes mèdics i hospitalaris, etc.
- **entrada a cavall** (*piggybacking and impersonation*) que, anomenada també "enginyeria social", consisteix, per exemple, en fer-se passar per altre i, així, aconseguir informació reservada.
- **"punxar" linies** (*wiretapping*) que consisteix en intervenir les línies de comunicació informàtiques per accedir o manipular les dades que hi circulen.

- **simulació i modelatge de delictes** (*simulation and modeling*) que utilitza un ordinador per planificar i controlar un delicte mitjançant tècniques de simulació, que permetin veure què passaria en realitzar realment el delicte.

Fins aquí la llista, ja clàssica, d'una tipologia del modus operandi del frau informàtic prou divulgada i coneguda. El que cal, quan passen ja deu anys de la seva formulació definitiva a [PAR 83], és recordar precisament el seu caràcter conjuntural i sotmès al pas del temps. D'altres estudis sobre els comportaments del manipuladors no autoritzats del sistemes informàtics (*hackers*) van incorporant noves "tècniques" que de vegades són noves i també, tot simplement, variacions sobre alguns dels tipus centrals i canònics ja esmentats pel mateix Parker.

Així, llibres especialitzats en el comportament dels *hackers* com són [STO 89], [RAY 91], [HAM 91] o [CLM 92], o versions quasi "periodístiques" d'estudis sobre el frau informàtic como [SNE 90], fan esment a noves modalitats de frau i delinqüència informàtica. Esmentem-ne, com a exemple, només uns quants:

- **exploració** (*scanning*) que consisteix en fer una exploració seqüèncial per trobar els números de telèfon o les paraules de pas que permeten l'accés a ordinadors o sistemes informàtics reservats.
- **mirar per l'espatlla** (*shoulder surfing*) que consisteix, tal i com indica el seu nom, en mirar per sobre l'espatlla d'un operador autoritzat per, en seguir el moviment dels seus dits sobre el teclat, esbrinar quina és la seva clau de pas al sistema i, així, robar-ne el seu coneixement.
- **buscar a les escombraries** (*dumpster diving*), nova variant de la "recollida d'informació residual" establerta per Parker i que consisteix en cercar a les escombraries els documents no destruï ts i amb informació sensible.
- **mistificació** (*spoofing*) que és una nova denominació del que abans hem anomenat "enginyeria social" i, que permet obtenir informació amb engany i simulació de personalitat.
- **etc.**

Com és fàcil de veure, el nombre de mètodes és variat i creixent amb el temps i l'ingeni (que no en falta) dels interessats en cometre fraus i delictes informàtics. Per això la simple referència a la dotzena de mètodes esmentats per Parker serà sempre una tipologia limitada com, de fet, ho serà qualsevol altre tipologia donat el dinamisme de la informàtica i dels *hackers*.

Hackers, del romanticisme al delicte

Si bé la tipologia de modus operandi del frau i la delinqüència informàtica de Parker han estat prou difosos, ho han estat molt menys les altres "dimensions" que, segons aquest indiscutible especialista en el tema, acompanyen el fenomen. Una de molt important és aquella que fa referència a les característiques dels autors dels fraus informàtics, els *hackers*. De fet, l'objectiu central del segon llibre de Parker sobre el delicte informàtic, [PAR 83], és concentrar-se "*en l'essència del problema: la gent que es dedica al delicte, i no pas en els instruments que fan servir*" tal i com diu el mateix Parker al prefaci de [PAR 83].

Possiblement tot va començar amb els *phreakers*, els manipuladors no autoritzats de les línies telefòniques nordamericanes dels anys seixanta. La voluntat d'utilitzar fraudulentament les línies telefòniques de la companyia telefònica Bell (la principal als Estat Units de Nord-Amèrica), per obtenir gratuï tament la possibilitat de fer trucades telefòniques de llarga distància, va estimular l'activitat d'un conjunt de joves que anomenaren la seva activitat com a *phreaking*. Els *phreakers* prenien el seu nom d'una conjunció de *freak* (sonat), *phone* (telèfon) i *free* (gratuï t i, també, lliure). Com es pot veure, ells mateixos recollien en el seu nom el caràcter marginal de la seva activitat que, inicialment, podia respondre fins i tot a uns certs objectius possiblement

romàntics d'alliberament de certes servituds de la tecnologia. No és aquest el lloc per detallar les activitats dels *phreakers* i convé remetre al lector interessat al primer capítol de l'amè i interessant llibre de Clough i Mungo [CLM 92].

De fet, els sistemes telefònics utilitzen ordinadors i els mateixos *phreakers* van anar convertint-se també en manipuladors no autoritzats de sistemes informàtics. Però, en els mateixos anys seixanta i setanta, cal constatar l'aparició d'un altre tipus de manipulador no autoritzat: el *hacker*.

L'atractiu innegable de la tasca de fer programes de tota mena fa sorgir un tipus d'especialista informàtic, jove, decidit i mogut segurament per una nova "curiositat intel.lectual" que passa a denominar-se *hacker*. De fet, sembla que *hacker* ve a etiquetar, originalment, a qui "fa mobles a cops de destral" tal i com s'indica al diccionari de Raymond, [RAY 91], que, a més, defineix el *hacker*, en primera accepció, com a "*una persona que gaudeix explorant els detalls dels sistemes programables i com estendre les seves capacitats, i oposat als usuaris que prefereixen aprendre només el mínim necessari*". Aquesta és una visió positiva i romàntica del *hacker* que, malauradament, ha evolucionat cap a un sentit negatiu com a resultat de les terribles conseqüències de les activitats dels *hackers*.

La traducció del terme *hacker* no ha estat mai feta a casa nostra, i s'utilitza directament el terme anglès. Cal dir, malgrat tot, que, diccionari en mà, la paraula catalana "manefla" (entremetedor o persona inclinada a ficar-se en els afers d'altri per curiositat, pel plaer de saber, de dir-hi la seva, etc.) podria escaure d'allò més bé a l'activitat dels *hackers*.

En aquest sentit positiu, típic de la primera activitat dels *hackers*, el diccionari de Raymond, [RAY 91], cita com a setena accepció per *hacker*: "*una persona que gaudeix amb el repte intel.lectual de la creativitat per superar o esquivar limitacions*" el que, de nou, ens porta a una visió romàntica i positiva del *hacker* que estaria mogut per un afany de coneixement i de "superació de reptes" francament atractiu pel jovent que composa el creixent exèrcit dels *hackers*. Així fou, segurament, per a alguns dels primers hackers dels vells temps (anys seixanta i setanta).

El canvi, de gran importància, que Parker introdueix en el segon dels seus llibres sobre el delicte informàtic, [PAR 83], és precisament la constatació de la desaparició d'aquest romanticisme. Les terribles conseqüències de l'activitat dels *hackers* porten Parker a abandonar un cert to èpic i romàntic encara perceptible en el primer llibre, [PAR 76], per assolir una descripció menys sensacionalista dels delictes informàtics i dels seus perpetradors i abandonar definitivament la pàtina de curiositat intel.lectual que comportava una tecnologia com la informàtica, molt més nova i sorprenent als anys seixanta i setanta, que no pas avui. El romanticisme desapareix del tot i els *hackers* passen a ésser considerats com el que són: gent fora de la llei (*outlaws*) que provoquen perjudicis a d'altri.

Com no podia ésser menys, fins i tot diccionaris com el de Raymond, escrit des de l'òptica del "*bon hacker*" dels anys seixanta i setanta, no pot esquivar aquesta nova accepció de *hacker* que inclou en una vuitena i darrera accepció per a dir que el *hacker* és "*un entremetedor maliciós que intenta descobrir informació sensible xafardejant pels sistemes*".

No és aquest el lloc adient per detallar les activitats dels *hackers*. Malauradament la bibliografia sobre el tema és ja prou abundant i detallada. A més de les informacions incloses en els llibres de Parker ja esmentats, cal citar, sobretot, el treball, ja clàssic, de Clifford Stoll, [STO 89], sobre la utilització de *hackers* alemanys per part del KGB soviètic per intentar obtenir secrets militars nordamericans. L'intent es realitzà a partir d'explotar l'existència d'una "porta falsa" en el sistema operatiu del sistema informàtic del Lawrence Berkeley Laboratories que Stoll fou encarregat, provisionalment, de supervisar. El que resulta fins i tot sorprenent és que les investigacions de Stoll, narrades quasi com una novel.la policíaca i amb gran amenitat, topen amb la desídia i poc interès dels responsables de les institucions encarregades de gestionar la seguretat dels sistemes informàtics a Nord-Amèrica. El cas narrat per Stoll s'ha convertit en clàssic i es

recull en d'altres llibres sobre el tema. Alguns, com [CLM 92] o [HAM 91], fins i tot, i gràcies al fet d'ésser posteriors, incorporen dades més recents (per exemple sobre el resultat dels judicis) que les incloses en el llibre del mateix Stoll.

Un altre cas famós és el de Robert T. Morris i el seu programa que, en difondre's i duplicar-se repetides vegades, va arribar a bloquejar la xarxa INTERNET nordamericana el 2 de novembre de 1988. El fet curiós en aquest cas, i tal vegada intrigant, és la relació familiar de l'autor de la malifeta amb Bob Morris, director de la NCSC (*National Computer Security Center*) nordamericana encarregada, precisament, de la seguretat dels sistemes informàtics en aquell país. Per a alguns comentaristes, l'atac del Morris fill a la seguretat de la xarxa INTERNET podria estar relacionat amb les repetides, i no prou escoltades, peticions del Morris pare per reforçar la seguretat de la xarxa, encara que, com era d'esperar, pare i fill neguen la relació. El cas es recull amb prou detall a [HAM 91] i també a [CLM 92].

També cal esmentar, a Europa, el programa *Christmas* (desenvolupat, segons sembla, per un estudiant de Hannover) que es presentava com una felicitació nadalenca informatitzada. El problema fou que, mentre es mostrava en la pantalla de l'usuari que executava el programa *Christmas*, aquest buscava mentrestant la llista de corresponsals electrònics de l'usuari i enviava còpies del programa a tots els corresponsals. Un clar exemple de "cavall de Troia" en la denominació de Parker. El que possiblement fou inicialment una broma, fins i tot no malintencionada, es convertí en un problema greu quan, després de superar la xarxa informàtica de la Universitat Clausthal-Zellerfeld a Hannover, va arribar a la xarxa informàtica al servei de la recerca europea EARNET (*European Academic Research Network*), per saturar finalment la xarxa VNET interna d'IBM a Europa el 15 de desembre de 1987. Allò que va començar possiblement com un joc, acabà amb un perjudici greu a una companyia privada que, des de llavors, s'ha vist obligada a implementar sistemes de seguretat que detectin la presència del programa indesitjable i l'esborrin automàticament. Un cas típic de com la inconsciència d'un *hacker* pot arribar a produir un greu perjudici.

Hi ha molts més casos documentats i llibres com [CLM 92] o [HAM 91] que els exposen amb prou detall. El més preocupant és el creixement dels casos clarament orientats a l'activitat delictuosa. Per posar-ne un exemple, recollit a [CLM 92], es pot esmentar el cas de "Kyrie" Leslie Lynne Doucette, una canadenca que, en ésser detinguda el maig de 1989, gestionava una xarxa de uns 150 *hackers* que s'especialitzaven en obtenir informació sensible i fer-la servir per robatoris. Li foren trobades 118 targes de crèdit Visa, 150 de Mastercharge, 2 d'American Express i 171 targes d'utilització de telèfons de les companyies ATT i ITT així com 39 codis d'autorització de centraletes telefòniques i de dades PBX. Tot un botí d'una actuació clarament delictuosa, obtingut mitjançant els *hackers*.

Una altra de les activitats dels *hackers* és la creació i difusió de virus ja abastament coneguda i divulgada en llibres com, per exemple, [LUN 89] o [CLM 92]. De fet, el virus és una rutina o subprograma, afegit a un altre programa normal que, en ésser executat, activa també al virus que realitza, per exemple, alguna acció destructiva en el sistema informàtic sobre el que s'està treballant. El més important i perillós d'un virus, i d'aquí la similitud biològica i mèdica de la seva denominació, és la capacitat "reproductora" del virus per "infectar" altres unitats de disc i així difondre's ràpidament a l'empara, per exemple, de la creixent pirateria de software existent en el món de la microinformàtica.

Els especialistes reconeixen diverses varietats de virus, com els cucs (*worms*) que no depenen d'altres programes i són, en sí mateixos, un programa aï llat i autosuficient com passava, per exemple, en el cas del programa que Robert T. Morris escampà per la xarxa INTERNET a finals de 1988. També, utilitzant sovint la nomenclatura emprada per Parker i ja esmentada en aquest text, cal parlar de "cavalls de Troia" com podria ésser el programa de l'estudiant de Hannover que va col.lapsar la xarxa interna de la IBM europea, o de bombes lògiques con

l'anomenat "Divendres 13" que s'activa precisament en tal data i que els periodistes han fet fins i tot famós.

Cal dir que, un cop coneguda la idea de que és factible fer un virus informàtic, la senzillesa tècnica de la seva realització fa que el nombre del virus registrats hagi augmentat de forma impressionant en poc temps, i el seu cens es compti ja per milers. Fins i tot han aparegut empreses i programes especialitzats en la detecció i lluita contra els virus tan freqüents en la microinformàtica. El text de Clough i Mungo, [CLM 92], comenta amb detall el tema dels virus i dóna una particular atenció al que hom anomena la "fàbrica búlgara" de virus i l'activitat del *hacker* conegut com *Dark Avenger* ("el venjador tenebrós")

Tot i que varen començar amb un aura de romanticisme, de superació del repte que oferia una nova i prometedora tecnologia, la realitat és que els *hacker*s d'avui poden arribar a ésser, de fet, un greu problema públic. Els qui no són conscients de la gravetat i el perill dels seus actes (que ells contemplen, fins i tot, com a joc) o els qui són clarament conscients del seu ús de coneixements informàtics per portar a terme robatoris d'informació sensible o difusió de programes indesitjables, composen l'exèrcit de delinqüents informàtics potencials que cal deturar per no malmenar les possibilitats d'una tecnologia de gran potencialitat com la informàtica.

L'increment de les mesures de seguretat en els sistemes informàtics ha arribat a ésser una nova responsabilitat dels professionals conscients, per desgràcia no sempre massa abundants en una professió sovint condicionada per les presses i els requeriments econòmics en la instal.lació apressada de nous sistemes.

Dificultat d'investigació i prova del frau informàtic

Malauradament el frau i la delinqüència informàtica, a més de presentar una gran varietat, resulta francament difícil de detectar i, encara més, de provar.

Hi ha característiques concretes de la tecnologia que expliquen aquest aspecte típic de la delinqüència informàtica. Castillo i Ramallo, a [CAR 89], recollien ja una sèrie de factors, no tots d'igual importància, del tipus dels que s'indiquen a continuació:

- la concentració de la informació típica de la informàtica que facilitaria en certa forma, per la seva localització centralitzada, el robatori de dades, tot i que cal pensar que amb els moderns sistemes distribuï ts aquesta característica resultarà cada dia menys important.
- la manca de registres visibles que fa més difícil i complicada la investigació dels fets.
- la possibilitat d'alterar programes i dades sense deixar pràcticament cap rastre o pista que permeti descobrir l'alteració efectuada.
- la facilitat d'eliminar les proves, simplement fent desaparèixer programes i dades amb una senzilla operació al teclat d'un sistema.
- la dispersió territorial dels punts d'entrada als sistemes informàtics i, per tant, l'augment dels punts d'origen de l'atac dels *hackers*.
- la manca de controls interns i de mecanismes de seguretat de la gran majoria dels sistemes informàtics i la seva manca de protecció en front de l'atac dels *hackers*.
- la manca, encara més greu, de seguretat envers dels propis operadors i del personal tècnic responsable dels sistemes, que poden ésser, també, perpetradors de fraus i delictes informàtics.
- etc.

Aquestes són algunes de les característiques pròpies de la tecnologia informàtica que permeten explicar la dificultat de detectar un frau o un delicte informàtic. Aproximacions com les que es donen a [HIS 81] són precisament això: aproximacions condemnades a resultar ràpidament

superades pel dinamisme del fet informàtic i per l'evolució i augment de les capacitats d'intrusió dels *hackers*.

Per detectar el frau o delicte informàtic i, sobretot, per a obtenir-ne de forma indiscutible les proves, calen coneixements tècnics que, com passa també en el cas de l'auditoria informàtica, resulten difícils (sino impossibles) d'obtenir per causa de la varietat i multiplicitat dels sistemes informàtics existents.

Per a un especialista en l'auditoria informàtica com Del Peso, obligat a creure en l'efectivitat final del procés d'auditar sistemes informàtics, la solució sembla deixar-se en mans dels professionals d'aquesta moderna vessant de l'auditoria i control de sistemes.

Amb tota seguretat no és aquesta l'única ni la millor de les solucions possibles per impedir, detectar i provar el delicte informàtic. Els problemes que el mateix Del Peso a [DEP 89] considera com a inevitablement presents resulten difícilment superables. Comentem-ne alguns:

- desaparició dels elements de la prova pel propi dinamisme del sistema informàtic o com a fruit d'una manipulació interessada.
- aparent desvinculació temporal del delinqüent informàtic amb el delicte o frau preparat amb molta antelació, ja que el fet delictuós pot presentar-se molt després d'ésser preparat com succeeix, per exemple, en el cas de les bombes lògiques activades temporalment.
- manca de coneixements específics entre els auditors informàtics o entre els membres dels cossos de seguretat de l'estat per procedir a la detecció del delicte i l'obtenció de les proves.
- manca de legislació específica per al reconeixement i sanció del frau i la delinqüència informàtica.
- dificultat d'acceptació de les proves en l'ordenament jurídic actual per causa, per exemple, de la seva incorporeï tat.
- possibilitat de que el delinqüent formi part del personal de les empreses o organitzacions investigades i, per tant, disposi d'informació sobre el desenvolupament de la investigació i pugui interferir en la mateixa.
- etc.

Com es pot veure, tot un conjunt de dificultats afegides a un problema de per sí difícil, complex i amb gran variabilitat i dinamisme.

Ètica i deontologia professional

Tal vegada pot semblar una fugida lateral o una renúncia a resoldre el problema, però el fet real és que una gran majoria dels especialistes informàtics que han estudiat amb detall el tema del frau i la delinqüència informàtica acaben coincidint en la pràctica impossibilitat de que el dret reculli i reguli tots els aspectes del delicte informàtic. Les possibilitats tecnològiques són moltes i canviants, les modalitats de frau augmenten dia a dia, el nombre i la capacitat dels *hackers* augmenta també amb la creixent difusió de la microinformàtica i dels sistemes distribuï ts, i les característiques de la tecnologia informàtica fan especialment difícil la detecció i la prova del delicte.

Aquest és un panorama no pas engrescador que ha portat, cada cop més, a posar l'accent en la responsabilitat social dels professionals informàtics que construeixen els sistemes posats a disposició dels usuaris. La crida a la responsabilitat es centra en la necessitat de no deixar "portes falses", de protegir la informació sensible, de detectar "cavalls de Troia" i "bombes lògiques" que vulguin introduir-se en els sistemes, de prendre molta cura fins i tot amb allò que es llença a les escombraries, de protegir les línies de comunicació amb sistemes d'encriptat, etc. En definitiva es tracta d'augmentar significativament la seguretat dels sistemes informàtics per a resistir als inevitables intents d'intrusió dels *hackers* de tota mena.

S'inicia així un nou tema: el de la necessitat d'incidir en l'ètica i la deontologia professional dels informàtics que, altra vegada, ha rebut una important empenta amb els treballs del pioner Parker ja des de 1981, a [PAR 81], i que s'ha seguit desenvolupant posteriorment pel mateix Parker i els seus col.laboradors Swope i Baker a [PSB 90], o per d'altres autors com Johnson [JOH 85], Forrester i Morrison [FOM 90], Ermann, William i Gutierrez [EWG 90] i tants d'altres.

El problema, no pas banal, és convèncer la comunitat professional informàtica de la necessitat d'un comportament ètic, seriós i responsable en la seva activitat professional quotidiana. El mateix Parker ja posava de relleu a [PAR 83] el seu convenciment de com, de totes les possibles mesures preventives del frau i la delinqüència informàtica, la més eficient havia d'ésser l'acceptació dels professionals informàtics d'uns estàndards ètics que els permetin respondre al repte que el frau i la delinqüència informàtica representen per a tota la tecnologia informàtica. En paraules de W. G. Frederick a la *Computing Review* parlant dels professionals informàtics i el perill del delicte informàtic: "*a menys que responguem a aquesta amenaça, la nostra imatge professional pot patir tant com la dels químics de la indústria dels pesticides*". Una volenterosa, però encertada, forma de considerar que la informàtica sense controls pot arribar a ésser una tecnologia fins i tot perjudicial per la societat que la fa servir.

En aquest sentit, és bo destacar la bona resposta institucional de les principals associacions mundials de professionals de la informàtica: la IFIP ja esmentada anteriorment, i l'ACM (*Association of Computing Machinery*) que estan, ambdues, en el procés d'elaborar i perfeccionar codis ètics que puguin guiar l'activitat professional dels creadors de sistemes informàtics.

Afortunadament, també alguns del textos sobre ètica professional informàtica han estat ja concebuts fins i tot com a suport docent per a la formació dels futurs professionals informàtics. Fins i tot al nostre país hi ha experiències com les que es concreten en el recent text sobre deontologia informàtica de Vázquez i Barroso, [VAB 93] o, més propera a la realitat catalana, la inclusió, en els nous plans d'estudi de les enginyeries informàtiques a la Facultat d'Informàtica de la Universitat Politècnica de Catalunya, d'una nova assignatura anomenada precisament "*Impacte social i ètica professional de la informàtica*". L'objectiu és, evidentment, sensibilitzar els futurs enginyers informàtics respecte de les seves responsabilitats envers la societat.

Bibliografia

[BAR 87] - BARCELÓ, Miquel (1987): *Usos i abusos de la informàtica*, Revista de Catalunya, nova etapa, núm. 14, Barcelona, desembre 1987.

[BAR 92] - BARCELÓ, Miquel (1992): *Els sistemes d'informació: fins on es pot arribar?*, Persona, Avencos tecnològics i Dret, Papers d'estudi i formació, Barcelona, núm. 9, juny 1992.

[BER 92] - BERLEUR, Jacques (1992): *Risk and Vulnerability in an Information and Artificial Society*, IFIP-WG9.2 "position paper", IFIP Transactions (A-13), Education and society: Information Processing 92 - Vol. II, R. Aiken Editor, pags. 295-313, North-Holland, Elsevier Science Publishers, Amsterdam, 1992

[CAR 89] - CASTILLO Jimenez, María Cinta y RAMALLO Romero, Miguel (1989): *El delito informático*, ponència presentada al congrés sobre "Derecho Informático", Facultad de Derecho, Universidad de Zaragoza, junio 1989.

[CLM 92] - CLOUGH, Bryan & MUNGO, Paul (1992); *Approaching Zero*, Faber & Faber, London, 1992. (Hi ha edició en castellà com "*Los piratas del chip*", Ediciones B, Barcelona, 1992).

[DPE 89] - DEL PESO Navarro, Emilio (1989): *La auditoria como medio de prevención frente al delito informático*, Revista ALI (Asociación de Licenciados en Informática), Número 14, Madrid, 1990. El mateix text fou presentat com a ponència en una reunió de l'Universitat de Comillas el maig de 1989.

[EWG 90] - ERMANN, M. David; WILLIAM, Mary B. & GUTIERREZ, Claudio (1990): *Computers, ethics, & society*, Oxford University Press, Ney York, 1990.

[FOM 90] - FORRESTER, Tom & MORRISON, Perry (1990): *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*, MITPress, Cambridge (MA), 1990.

[FOR 85] - FORRESTER, Tom (1985): *The Information Technology Revolution*, Basil Blackwell Ltd., Oxford, 1985.

[HAM 91] - HAFNER, Katie & MARKOFF, John (1991): *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, A Touchstone Book, Simon & Schuster, New York, 1991.

[HIS 81] - *Agenda HISPAMER*, Corporación Financiera, Edic. Simancas, Madrid, 1981.

[JOH 85] - JOHNSON, Deborah, G. (1985): *Computer Ethics*, Prentice Hall, Englewood Cliffs (NJ), 1985.

[LUN 89] - LUNDELL, Allan (1989): *Virus: the secret world of computer invaders that breed and destroy*, Contemporary Books, Inc., Chicago, 1989.

[MAR 91] - MARCELO, Julian (1991): *Libertad e Informática en Europa*, Revista NOVÄTICA, Barcelona, Parte I: Antecedentes (hasta 1980), Vol. XVII, núm. 94, 1991; Parte II: Década actual y bases jurídicas, Vol. XVIII, núm 95, 1992.

[MAS 86] - MASON, Roger O. (1986): *Four Ethical Issues of the Information Age*, MIS Quarterly, Vol 10, 1986.

[MOR 92] - MORRIS, A. B. (1992): *Ethics and Information Systems Practice*, IFIP Transactions (A-13), Education and society: Information Processing 92 - Vol. II, R. Aiken Editor, pags. 363-369, North-Holland, Elsevier Science Publishers, Amsterdam, 1992

[PAR 76] - PARKER, Donn B. (1983): *Crime by Computer*, Charles Scribner's Sons, New York, 1976.

[PAR 81] - PARKER, Donn B (1981): *Ethical Conflicts in Computer Science and Technology*, AFIPS Press, Arlington, 1981.

[PAR 83] - PARKER, Donn B. (1983): *Fighting Computer Crime*, Charles Scribner's Sons, New York, 1983.

[PSB 90] - PARKER, Donn B; SWOPE, Susan & BAKER, Bruce N. (1990): *Ethical Conflicts: in Information and Computer science, technology and business*, Q.E.D. Information Sciences, Wellesley (MA), 1990.

[RAY 91] - RAYMOND, Eric S. Editor (1991): *The New Hacker's Dictionary*, The MIT Press, Cambridge (MA), 1991.

[SIE 86] - SIEBER, Ulrich (1986): *The International Handbook on Computer Crime*, John Wiley & Sons, New York, 1986.

[SIE 90] - SIEBER, Ulrich (1990): *General Report on "Computer Crime"*, 13th International Congress of International Academy of Comparative Law, University of Bayreuth, 1990.

[SNE 90] - SNEYERS, Alfredo (1990): *El fraude y otros delitos informáticos*, Tecnologías de Gerencia y Producción SA, Madrid, 1990.

[STO 89] - STOLL, Clifford (1989): *The Cuckoo's Egg*, Doubleday, New York, 1989. (Hi ha edició en castellà com "*El huevo del cuco*", Planeta, Barcelona, 1990).

[VAB 93] - VAZQUEZ, Jesús María y BARROSO, Porfirio (1993): *Deontología de la informática (esquemas)*, Instituto de Sociología Aplicada, Madrid, 1993.

[WAS 92] - WASIK, Martin, (1992): *Legal Control of IT Misuse: Limited Relevance of the Criminal Law*, IFIP Transactions (A-13), Education and society: Information Processing 92 - Vol. II, R. Aiken Editor, pags. 385-392, North-Holland, Elsevier Science Publishers, Amsterdam, 1992