Frau Informàtic i Etica Professional

Miquel Barceló
Dept. Llenguatges i Sistemes Informàtics (LSI-UPC)

INTRODUCCIO.

Tecnologies amb molt dinamisme com la informàtica generen amb gran rapidesa possibilitats d'ús i abús que, naturalment, van per davant de la possibilitat de regulació jurídica de les seves conseqüències i responsabilitats. Per aquesta raó, el problema del delicte i el frau informàtic és un problema jurídic que, en la seva solució planteja temes d'ètica i deontologia professional que afecten a la totalitat dels informàtics com a grup professional.

DELICTE I FRAU.

Quan es parla de frau i delinqüència informàtica de forma genèrica és, potser, per la dificultat de parlar concretament del "delicte informàtic" com a tal. Sovint s'entén el delicte informàtic com aquella acció dolosa que provoca un perjudici a persones o entitats i en la que es fan intervenir dispositius o programes informàtics.

De fet, la legislació sobre delictes informàtics és avui molt limitada a la majoria dels països, i potser encara més a Espanya. Per això és encara molt comú evitar parlar de "delicte informàtic" i referir-se al "frau informàtic" o a una genèrica "delinqüència informàtica" entenent per frau aquella conducta realitzada mitjançant un sistema informàtic amb la que es vol aconseguir un benefici il.lícit. I això amb independència de si tal conducta ha estat o no tipificada als codis penals.

També cal parlar d'un altre tipus de frau informàtic no intencionat, l'"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 a d'altres usuaris o per als propietaris del sistema.

NOUS DRETS I FIGURES DELICTIVES.

Les noves possibilitats que ofereix la societat de la informació exigeixen unes noves respostes tant a l'àmbit ètic com al jurídic. Morris, a [MOR 92], parla dels "quatre drets bàsics que són rellevants en l'era de la informació".

A- Privacitat *(privacy)*, 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 *(access)*, ja que cal permetre un accés adequat a la informació, però de forma estrictament controlada. Per alguns autors aquestes exigències jurídiques 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 sovint es suggereixen 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 aquestes cinc figures delictuoses amb els drets 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, sovint, resulta insuficient per a cobrir totes les particularitats del fet informàtic. De fet, els estudis sobre legislació comparada marquen clarament 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.

Per exemple, les accions il.lícites incloses 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 maquinària, 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 la llei recull 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 recollits en els codis jurídics, i que difícilment ho estaran precisament per la multiplicitat, dinamisme i variabilitat de la tecnologia informàtica.

Algunes de les figures il.lícites abans esmentades requererien 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, sindicats 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.

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 explícitament els drets d'autor dels creadors del software (14 de maig de 1991).

TIPOLOGIA DEL FRAU INFORMATIC.

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.

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)*
- cavall de Troia *(Trojan horse)*
- tècnica del salami *(salami technique)*
- ús no autoritzat de programes especials *(superzapping)*
- portes falses *(trap doors)*
- bombes lògiques *(logic bombs)*
- atacs assíncrons *(assynchronous attacs)*
- recollida d'informació residual *(scavenging)*
- divulgació no autoritzada de dades reservades *(data leakage)*
- entrada a cavall *(piggy- backing and impersonation)*
- "punxar" línies *(wire- tapping)*
- simulació i modelatge de delictes *(simulation and modelling)*

Fins aquí la llista, ja clàssica, d'una tipologia del modus operandi del frau informàtic prou divulgada i coneguda. Hi ha també intents d'ampliar i d'actualitzar la llista incorporant noves "tècniques" de frau informàtic que superin el caràcter

conjuntural d'una llista elaborada ja fa anys. No és aquest el lloc més adient per detallar i comentar cada una de les tècniques i es remet el lector als llibres de Parker [PAR 76] i [PAR 83] o a resums actualitzats com el de [BAR 93].

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 fenòmen. 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 com diu el mateix Parker al prefaci.

Possiblement tot va començar amb els *phreakers*, els manipuladors no autoritzats de les línies telefòniques nord-americanes dels anys seixanta. La voluntat d'utilitzar fraudulentament les línies telefòniques de la companyia telefònica Bell (la principal als Estats Units de Nord-Amèrica), per obtenir gratuïtament 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* (gratuït, 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'altre 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 dels 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 nord-americana el 2 de novembre de 1988. El fet curiós, i tal vegada intrigant, en aquest cas és la relació familiar de l'autor de la malifeta amb Bob Morris, director de la NCSC *(National Computer Security Center)* nord-americana 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 del 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*.

Tot i que varen començar amb una aura de romanticisme, de superació del repte que oferia una nova i prometedora tecnologia, la realitat és que els *hackers* 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.

ETICA 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 distribuïts, i les característiques de la tecnologia informàtica fan especialment difícil la detecció i la prova del delicte (tema del que no hi ha espai per parlar-ne aquí. El lector interessat en trobarà una referència més detallada a [BAR 93]).

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 escombreries, 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 dels 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 93] - BARCELO, Miquel (1993): *El frau i la delinqüència informàtica: un problema jurídic i ètic*, Report de Recerca LSI-93-19-R, Departament de Llenguatges i Sistemes Informàtics, UPC, Barcelona, 1993.

[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).

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

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

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

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

[MOR 92] - MORRIS, A. B. (1992): *Ethics and Information Systems Prac-tice*, 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.

[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 Apli-cada, Madrid, 1993.

Call for papers

La próxima revista saldráen Abril, por lo que requerimos una vez más la colaboración de nuestros lectores y asiduos colaboradores. La fecha límite de entrega de artículos es el 11 de Marzo del 1994, las colaboraciones recibidas con posterioridad se publicarán en el número de octubre de 1994. Dado que el número de páginas es limitado, se efectuará un proceso de selección de los artículos recibidos, quedando en el archivo de la revista aquellos que no sean publicados.

Las colaboraciones han de entregarse en formato PC, en cualquier procesador de textos conocido. Las gráficas han de entregarse por separado, indicando el programa gráfico en que se han realizado, así como una copia en papel, del texto y de las gráficas. La copia nos permitirá detectar los posibles errores que surjan en la importación, así como respetar en lo posible la configuración que el autor desee para su artículo.

Es deseable que el artículo esté acompañado de un breve curriculum, y una dirección que permita poner en contacto a los lectores y a los articulistas.

Aconsejamos a los autores de los artículos, que estos se acompañen de gráficos y fotografías (la publicación de las fotografías dependerá de la situación económica de la asociación). Recordamos que la principal idea es la divulgación de trabajos y proyectos que se realicen en la U.P.C. y otras facultades adscritas a los temas del I.E.E.E., no una demostración de conocimientos.