Tema 7. Dictàmens i peritatges Informàtics

Si duo imperata inter es repugnantia simili tibi faciuntur, ambo sequere.
Si reps dues ordres contradictòries, compleix-les totes dues.

De la instrucció a les legions de la Roma imperial

La figura del pèrit informàtic pot semblar una cosa difusa, amb una visió que des de fora pot tenir més de ficció que de realitat, gràcies a les novel·les, els còmics, els pseudodocumentals, les sèries de televisió i les pel·lícules procedents dels Estats Units, que ens presenten el ciberforense com una barreja de Sherlock Holmes i Bill Gates. No s'acaba d'apreciar què és el que es fa en aquesta activitat professional en concret, un dels híbrids més perfectes entre la disciplina jurídica i la informàtica.

Ben poc de ficció, però, i molt de realitat té aquesta eixida professional que es presenta als titulats de la carrera d'Informàtica. No obstant això, les particularitats que presenta requereixen esbossar almenys unes línies mestres que servisquen de llit per al riu de l'experiència i tot allò que aquest vaja aportant.

Al llarg del present tema es tractarà d'establir aquest llit, o almenys una base per a crear-lo. Després d'una breu introducció, on assentarem els conceptes bàsics, farem una classificació dels tipus de treball, els tipus de peritatges que es poden trobar més comunament; no sols pensant en el món judicial, sinó també en el de les relacions entre empreses, per a la qual cosa recorrerem a fonts procedents bàsicament del món anglosaxó, ja que allí aquesta via professional està molt més desenvolupada. Ens queda descriure el pèrit en si mateix, les competències que li són necessàries i el marc en què es mou, i, per descomptat, centrar-nos en el resultat en què es plasma el seu treball: el dictamen, del qual veurem alguns exemples.

Com fem en tots els temes, aquest el tancarem també amb un apartat bibliogràfic, del qual cal destacar de forma anticipada un conjunt d'adreces URL on podem trobar eines d'ajuda per al treball del pèrit.

1. Breu introducció. Conceptes

Quan dues parts volen dirimir les seues diferències, des dels inicis de la humanitat civilitzada, s'acaba recorrent a una tercera part que les dues litigants accepten com a *bona*, és a dir, com a justa. Encara que no sempre passa així, com veurem en aquest tema, la figura d'aquesta tercera part la sol representar un jutge o jutgessa. No ens és difícil adonar-nos que el jutge o jutgessa no pot saber-ho tot de totes les matèries del coneixement humà. La medicina forense és un exemple de com un expert ajuda *el just* que pren les decisions.

Fent una mica d'història, tot seguint Noblett (4-5), podem remuntar-nos per trobar referències a la *medicina legal* al segle VI, i de forma rutinària als tribunals, a partir del segle XVI. No obstant això, els orígens de la moderna ciència forense els trobem a mitjan segle XIX. Alguns dels primers esforços per a definir la ciència forense, sempre segons Noblett, podrien ser:

• L'any 1844, el Dr. Mathieu J. B. Orfila, considerat com el pare de la toxicologia, va publicar un tractat científic sobre la detecció de verins i els efectes d'aquests en animals.

• El 1855, el doctor Bergeret d'Arbois utilitza la infestació d'insectes per a estimar el temps de la mort.

• En la dècada del 1890, Edward Henry i el treball pioner de Francis Galton van menar als mètodes per a classificar i ordenar les empremtes dactilars.

• L'any 1900, Edmond Locard va estudiar probabilitats sobre bales que s'aparellen, pèls, i patrons d'esquitxades de sang, i va demostrar que es pot connectar un delinqüent a una escena del crim per mitjà de partícules de pols.

• En 1914, Leone Lattes va desenvolupar mètodes per a determinar els tipus de sang de les taques de sang seca.

• En la dècada del 1920, Calvin Goddard va perfeccionar les tècniques necessàries per a determinar si una bala es va disparar des d'un arma sospitosa.

A manera d'anècdota, per a centrar-nos en el treball d'un pèrit, recordem un fet esdevingut l'any 1978, moment que sembla pròxim en el temps, però de fet és prou llunyà perquè els costums de la nostra societat hagen donat un gir copernicà. Llavors es va celebrar un judici a la Magistratura de Treball Madrilenya, on l'empresa demandada era el Gay Club, un local amb un espectacle a càrrec de transvestits, cosa que llavors tenia una popularitat emergent dins l'oferta d'oci urbà.

L'agutzil va cridar les parts per començar la vista oral:

- Fulgencio Suárez Villaplana!

Va entrar a la sala una, en aparença, esplèndida dona, de poderós bust, llargues pestanyes i malucs ondulants, molt marcats per la minifaldilla. El jutge va preguntar amb sorpresa:

- Però vostè qui és?

- Fulgencio, per servir-lo.

- Que el reconega el forense, perquè jo no m'ho crec.

En aquesta anècdota, presa de Vizcaíno, el forense, funcionari de l'estat, usa els seus coneixements en l'anatomia humana per determinar alguna cosa que al jutge se li escapa.

Però per a poder entendre de què parlem, necessitem usar conceptes que esmentarem al llarg de tot el tema. I ja que hem portat a col·lació el terme *forense*, comencem per aquest.

El terme *forense* es pot definir com l'aplicació de la ciència a una qüestió de dret. I, pel que ens toca a nosaltres, podríem centrar-nos en la ciència forense digital, o informàtica forense: la informàtica forense seria la recol·lecció, preservació, anàlisi i presentació de proves electròniques per a usar-les en l'àmbit jurídic de manera que siga vàlida a efectes legals tot fent servir eines i pràctiques d'acceptació general. En concret, *anàlisi forense digital* seria l'aplicació de la tecnologia informàtica a una qüestió de dret en la qual les proves inclogueren elements creats per persones i elements creats per la tecnologia com a resultat de la interacció amb una persona. Per exemple, les dades creades per un procés requereixen una màquina que es puga programar, i que va ser executada per una persona o fins i tot per un procés automàtic que en darrer terme va executar una persona. (Daniel, 3)

Una altra definició molt pròxima la prenem de López Manrique (López Manrique, 25-35), que diu que la computació forense (evidentment, depenent de les fonts, termes com *computació* o *informàtica* s'entremesclen sense que hi haja cap diferència aparent entre aquests) és la ciència d'adquirir, preservar, obtenir i presentar dades que han sigut processades electrònicament i desades en un mitjà computacional. També es defineix com el procés d'identificar, preservar, analitzar i presentar proves digitals de forma que puguen ser acceptades en la solució d'un cas en què estiga involucrada la tecnologia digital per a investigar un crim tecnològic.

Però per a poder portar a terme aquest procés d'anàlisi, cal tenir *alguna cosa*. I aquesta cosa es diu *perícia*. Així, definim *perícia* com experiència, pràctica o habilitat en un art o una activitat concreta. Podem, per tant, considerar *pèrit* la persona que posseeix un títol o que és especialista en alguna cosa determinada. El pèrit, seguint el *Diccionari normatiu valencià* (DNV), és la "Persona experta en una matèria determinada que dictamina en un juí sobre fets que requerixen els seus coneixements". Segons el diccionari jurídic, seria la "Persona que posseeix un títol. Especialista en alguna cosa determinada. Jurídicament ens referim a la que informa en un procediment, sota jurament, sobre qüestions litigioses relacionades amb la seua especialitat o experiència" (del Peso Navarro, 2001).

El peritatge podem considerar-la com la facultat de ser escoltat en els casos en què, per raó dels coneixements o la professió del pèrit, aquest puga contribuir a decidir els punts dubtosos per mitjà del seu informe o dictamen, terme aquest que desenvoluparem, per l'especial rellevància que té, en un epígraf a banda.

El dictamen, o, més ben dit, el peritatge, el podem interpretar (seguint el DNV) com "un treball o informe que fa un pèrit" a fi de corroborar determinades circumstàncies o fets. O, en termes col·loquials, seria com fer una foto d'una situació donada, documentant objectivament el que s'analitza i generant-ne un informe clar, concís i expeditiu.

Resta parlar de l'objecte del treball del pèrit. Allò sobre què efectua el seu estudi, les seues anàlisis, on opera: les proves (per a nosaltres, proves electròniques o digitals –*e-evidence* en anglès) (Volonino, 9).

Visitant de nou el DNV, veiem que *prova* es defineix com a "Raó, argument o qualsevol altre mitjà amb què es pretén mostrar la veritat o la falsedat d'alguna cosa".

Si ens referírem a un cas convencional, no informàtic, podríem parlar, com en les pel·lícules de sèrie B, d'una pistola, una empremta en un got… però nosaltres necessitem marcar una sèrie de diferències.

Així, segons Daniel:

Una prova digital pren moltes formes. Generalment són dades electròniques, ja siga en forma d'una transacció, un document, o algun tipus de mitjà de comunicació, com ara un enregistrament d'àudio o de vídeo. Les transaccions poden comprendre transaccions financeres creades durant el procés de fer una compra, pagar un compte, retirar diners en efectiu o, fins i tot, escriure un xec. I és que, si bé escriure un xec podria semblar un mètode passat de moda que no és digital o electrònic, el processament de la verificació sí que és electrònic, i s'emmagatzema així al banc. Quasi qualsevol tipus de transacció d'avui dia es digitalitza en algun moment, de manera que les proves d'aquesta transacció esdevenen digitals: així, deixen rastre digital els fets d'anar a cal metge, obtenir receptes, registrar un xiquet a la guarderia, o, fins i tot, vacunar un gos contra la ràbia.

En el món connectat d'avui, és quasi impossible per a ningú estar completament *fora de la xarxa* de tal manera que les seues activitats no generen cap mena de registre electrònic.

L'explosió de les xarxes socials, al seu torn, ha creat tota una nova àrea de proves electròniques alhora penetrants i persistents. La gent avui comparteix el seu dia a dia, les seues activitats, pensaments, fotos personals, i fins i tot la seua ubicació a través de Twitter o Facebook, entre altres coses. A això cal afegir encara l'explosió de la blogosfera, on els individus actuen com a periodistes (Daniel, 4).

De forma més concisa, Volonino ens defineix *prova* com el material utilitzat per a persuadir el jutge o el jurat de la veritat o falsedat d'un fet controvertit. (Volonino, 335). Proves electròniques o digitals (*e-evidence*) serien les que tenen forma digital o electrònica, com ara els arxius de correu electrònic d'ordinador, els missatges instantanis, els calendaris i els PDA (Volonino, 335).

Una col·lecció de definicions més formals la podem prendre de Carvajal (89):

S'anomena *prova digital* qualsevol registre generat o emmagatzemat en un sistema de còmput que es puga usar com a prova en un procés legal.

Vegem-ne algunes definicions:

"Qualsevol informació, subjecta a una intervenció humana o una altra de semblant, que s'haja extret d'un mitjà informàtic" (HB:171 2003 Guidelines for the Management of IT evidence).

“Una vegada reconegudes, les proves digitals s’han de preservar en l’estat original. Cal tenir en ment que la llei requereix que les proves siga autèntiques i sense alteracions” (Casey, Eoghan, “Digital Evidence and Computer Crime”, 2000).

Carvajal conclou definint característiques de les proves digitals que resulta interessant destacar en aquest moment:

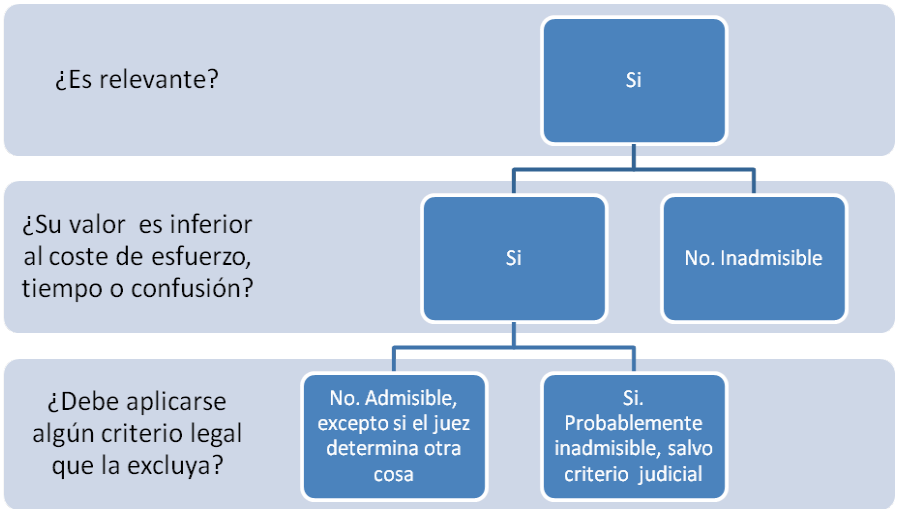
És la matèria primera dels investigadors, és volàtil i anònima, és modificable, és a dir, que es pot duplicar, esborrar o alterar però és part fonamental de l’escena del delicte; si es comprometen les proves es pot perdre el cas administratiu o legal de la recerca forense. És crític recordar que les proves es poden duplicar i, tot i això, aquesta còpia és original respecte dels entorns digitals.

Són aquestes característiques les que fan atípiques les proves electròniques respecte de les proves convencionals, i són també les que fan difícil el treball d’un pèrit informàtic. Així, una mala actuació pot corrompre una prova electrònica.

Seguint López Manrique (25-35), precisem que l’aspecte més important a l’hora de recollir proves és la preservació de la integritat d’aquestes. Altres consideracions interessants del mateix autor ens fan reflexionar sobre quina quantitat de proves electròniques cal agafar quan aquestes estan basades en suports físics. Ens emportem un equip complet, per no arriscar-nos a deixar peces d’informació potencialment rellevants? I si ens demanden per perjudicar la vida d’una persona o d’un negoci més enllà del que era absolutament necessari? Quin seria el mínim que cal confiscar per a efectuar una recerca? En darrer terme, serà la duresa del crim investigat el que determine la forma d’actuar. D’altra banda, és obvi, no és el mateix investigar sobre una microSD que sobre un ordinador central.

El mateix autor apunta una cosa que és òbvia per a nosaltres: no totes les proves electròniques tenen suport físic. Moltes, cada vegada més, tenen presència únicament en les xarxes. Poden ser en ordinadors llunyans físicament… o bé desconeguts, de manera que cal fer un esforç explícit per capturar-les (per ex., mitjançant l’ús de detectors o *sniffers*). Un cas interessant el suposen les xarxes socials, com ara Facebook, tema tractat per Hoog (360).

Quines proves aprofiten? Totes? La millor manera de donar resposta a aquest interrogant és de forma gràfica, en la imatge següent:



És rellevant? / Sí / Té un valor inferior al cost d'esforç, temps o confusió? / Sí / No. Inadmissible. / Cal aplicar algun criteri legal que l'excloga? / No. Admissible, llevat que el jutge determine una altra cosa. / Sí. Probablement inadmissible, llevat que el criteri judicial determine una altra cosa.

Quan és admissible una prova digital? Font: adaptat de Volonino (25)

Hi ha algun altre concepte interessant que hem de començar a considerar, i per tant no convé que ens el deixem al tinter en aquests moments inicials: així, definim, seguint Volonino, una *cadena de custòdia*. Seria la cura, el control i la rendició de comptes de les proves a què està obligat el pèrit en cada pas d'una recerca, per a verificar la integritat de les proves; el procés de validació de com es va recollir la prova digital, el seguiment i la protecció en un tribunal de justícia. Si no existeix, no hi ha proves. (Volonino, 332)

Dins de les particularitats que poden presentar les proves, hi ha les proves demostratives: un tipus de proves que s'ofereix per a explicar, o bé un resum d'altres proves. No se solen admetre en un judici. Exemples: gràfics i mapes generats per ordinador (Volonino, 333).

Tancant l'apartat de definicions, no podem deixar escapar un terme que de vegades sembla confús: el de *deposició*, d'ús habitual als jutjats. Seria el testimoniatge sota jurament davant la presència d'un tribunal (Volonino, 333).

Per acabar, i centrant-nos en la prova pericial, que seria la que nosaltres crearíem, podríem definir-la com l'instrument mitjançant el qual experts aliens a les parts en litigi, amb coneixements rellevants en alguna ciència, art o professió, recapten i analitzen informació i la posa en coneixement d'un jutge, i donen a més la seua opinió fundada sobre la interpretació i l'apreciació d'aquesta informació.

Però què diu la llei? Quins mitjans de prova podrem emprar en un judici? Seguint l'article 299 de la Llei d'enjudiciament civil (LEC, Llei 1/2000, de 7 de gener, d'enjudiciament civil), aquests serien:

- Interrogatori de les parts

- Documents públics
- Documents privats
- Dictamen de pèrits
- Reconeixement judicial
- Interrogatori de testimonis

Un peritatge informàtic pot abraçar totes les àrees de la informàtica, i fins i tot alguna àrea que tinga una relació menor amb aquesta.

Exemples possibles: des del desenvolupament de sistemes, al plagi entre aplicacions, passant per equips, característiques de documentació com un manual d'usuaris, etc.

Cal deixar clar des del primer moment que la prova pericial és apreciada per jutges o tribunals en funció de la *sana crítica*, i per tant és de lliure ponderació pel tribunal.

Els dictàmens pericials, amb tota la importància que tenen en determinades matèries, són elements de judici, estimables en les conclusions, no sols pel fet que els haja emès un tècnic, sinó pels raonaments que hi condueixen, basats en les normes objectives de la ciència o de la tècnica.

Tot això, sense oblidar el principi rector que *allò que no es troba en les actuacions no existeix legalment*.

2. Quins tipus de faena fa un pèrit informàtic?

Una vegada descrits els conceptes bàsics, el nostre pas següent és aclarir el tipus de tasques a què es pot enfrontar un pèrit informàtic. A priori podem tenir la impressió que aquestes es redueixen a les seues actuacions davant els tribunals i poc més, i sempre centrant-se en delictes purament tecnològics, com ara robatoris de bases de dades o espionatge industrial, però no és així. López Manrique ens indica (López Manrique, 25-35) amb encert que la informàtica forense no s'usa només per a investigar crims tecnològics, com ara l'accés no autoritzat a una xarxa o la distribució de material il·legal, sinó que també es fa servir per a investigar qualsevol crim en què un ordinador pot tenir alguna prova emmagatzemada (per exemple, un intercanvi de correus electrònics entre una víctima de violació i el violador). Així, entre els possibles camps d'actuació, veiem que molts provenen de la vida diària, i no cal que estiguen relacionats directament amb la informàtica; es pot, per exemple, cercar proves per al *món no digital*, com ara divorcis, assegurances, assetjament psicològic…

Això fa que el pèrit haja d'estudiar molts mètodes (Dube) i tècniques (Hoog, 196 i següents), ja que la recerca pot anar per diverses vies, des de l'estudi d'arxius en núvol (Lillard, 6) fins al de dispositius mòbils complexos, com ara telèfons intel·ligents (López Tarraella, 259), o bé de virus en les diferents classificacions taxonòmiques (Filiol, 81 i següents), o de la captura de trànsit en la xarxa (Lillard, 23)...

Una primera aproximació a la classificació de les faenes que pot fer un pèrit informàtic ens ve de la mà de Vacca (35 i següents), que en fa una divisió elemental, segons l'àmbit de treball:

- Àmbit militar. Carvajal (86) segueix aquesta via en parlar de recerques sobre ciberterrorisme, i particularitzant-ho als virus, podem seguir Filiol (338).
- Àmbit judicial/legal, que és el que se sol considerar com el principal.
- Àmbit empresarial, al qual tornarem quan parlem dels arbitratges.

El mateix Vacca (83) ens proporciona una classificació de tipus de treball, aplicable a qualsevol dels tres àmbits:

- Anàlisi forense de sistemes informàtics
- Sistemes de seguretat per a Internet
- Sistemes de detecció d'intrusos
- Sistemes de seguretat basats en tallafocs
- Seguretat per a emmagatzematge en xarxa
- Sistemes de recuperació de desastres
- Sistemes de seguretat amb clau pública
- Sistemes de seguretat de xarxa sense fil
- Comunicacions via satèl·lit encriptades
- Missatgeria instantània
- Sistemes de privadesa de xarxa
- Gestió d'identitat
- Prevenció de robatori d'identitat

No és l'únic que fa aquest tipus de categorització. Així, Daniel (18 i següents) ens facilita una alternativa:

- Tipologia en la informàtica forense
- Resposta a incidents
- Estudi de telefonia mòbil
- Estudi de GPS
- Estudi de dispositius d'emmagatzematge

- Anàlisi forense de mitjans socials
- Vídeo digital i anàlisi forense de fotos i càmeres digitals
- Anàlisi forense d'àudio digital
- Estudi forense de jocs multijugador
- Estudi forense de consoles de videojocs

Però tornem als àmbits d'actuació. Els dos que ens ocupen principalment són els que es desenvolupen al voltant dels tribunals o la vida empresarial. I potser semblarà que és una cosa lineal i simple: res més lluny de la realitat. Fins i tot en el món judicial, que sembla menys complex des de fora que l'enormement variat món empresarial, la vida del pèrit pot tornar-se molt complexa. Així, podem veure l'exemple que ens n'ofereix Volonino:

Paper exercit	Tipus de cas	Condicions de treball	Quan està involucrat
Suport al demandant	Civil	Amistós	Abans de tota actuació legal
Suport al demandat	Criminal	Neutral	Durant la recerca electrònica
Actuació com a part neutral	Laboral	Manca de suport	Durant la captura de dades
Investigar per a un particular/empresa	Divorci	Hostil	Durant la revisió i l'anàlisi de les dades
Investigar per a un particular/empresa	Frau	Mode invisible	Just abans de l'inici del judici

Adaptat de Volonino, 121 i següents

En aquesta taula podem veure diferents papers exercits als tribunals, amb diferències evidents. Entre aquests factors que poden influir en la recerca destaquen les condicions de treball. Volonino les descriu com segueix:

- Ambient hostil: exemple: pèrit contractat per l'advocat del demandant en un cas que implica el robatori de plànols d'enginyeria per un exempleat. Se sospita que l'empleat en va donar còpies al seu nou cap, sense cap més informació rellevant per a l'investigador. Aquest intenta copiar fitxers i el correu electrònic del sospitós en el seu antic PC de l'oficina, així com els registres de la xarxa per revisar-los. El personal de sistemes de TI fa mala cara, ja que eren ells els responsables de controlar l'accés a arxius confidencials i del filtratge de correu electrònic, en què òbviament van fallar. A

més, l'advocat no s'hi presenta, per la qual cosa el pèrit hi és tot sol, i la xarxa fa una hora que ha caigut, de manera que no sembla haver-hi ningú que tinga temps per a ell.

- Mode invisible: el director de Recursos Humans contracta el pèrit per a inspeccionar un ordinador d'un empleat per saber si aquest està violant la política de l'empresa veient pornografia. Cal fer la recerca sense alertar l'empleat o qualsevol altra persona. Es treballa després de les 10 de la nit, quan l'oficina és buida, per fer còpies dels fitxers.

- Ambient neutral: l'advocat d'un acusat envia al pèrit un CD que conté la imatge de l'ordinador del seu client. També rep els detalls de les galetes (*cookies*) i els arxius utilitzats fa poc. L'acusat està acusat d'haver comprat o descarregat a propòsit pornografia infantil. La revisió i l'anàlisi demostren la presència d'un petit nombre de possibles fitxers d'imatges, totes amb grandàries d'arxiu menors de 10 kilobytes (KB), i la majoria menors de 5K. Les grandàries d'arxiu indiquen la grandària de les miniatures de les imatges. No hi ha evidència dels típics indicadors de comportament pederasta (per exemple, els arxius d'imatges no estaven organitzats, sense directoris, noms d'usuari o comptes de correu electrònic que indicaren interès en aquests). La revisió mostra moltes visites a llocs pornogràfics per a adults (les miniatures podrien haver-se descarregat sense saber-ho l'acusat).

- Entorn amistós o mancat de suport: just una setmana abans que comence el judici, un fiscal demana a un pèrit que confirme que el sospitós sota custòdia ha enviat per correu electrònic amenaces, que corroboren altres tipus de proves (cartes, faxos i amenaces en persona). Es formulen al fiscal dues preguntes, "Com es pot lligar aquests correus al sospitós? Com se sap que era ell i no una altra persona qui va enviar el correu?". Ningú pot respondre a això. L'anàlisi mostra que el correu s'havia enviat des d'un compte que usava el sospitós, però se segueix sense poder vincular el sospitós als missatges.

Anem a pams, però. Pel que fa a les actuacions fora dels tribunals, intervenint entre empreses, hem de centrar-nos en la figura de l'arbitratge.

S'entén per *arbitratge* la institució per la qual les persones físiques o jurídiques poden sotmetre, amb conveni previ, a la decisió d'un o diversos àrbitres les qüestions litigioses sorgides o que puguen sorgir en matèria de la seua lliure disposició segons dret. L'article 1r de la Llei d'arbitratge de 5 de desembre de 1988 assenyala que "Mitjançant l'arbitratge les persones naturals o jurídiques poden sotmetre previ conveni a la decisió d'un o diversos àrbitres les qüestions sorgides o que puguen sorgir en matèria de la seua lliure disposició segons dret".

Hi ha una sèrie de qüestions que queden excloses de l'arbitratge:

- Aquelles sobre les quals haja recaigut una resolució judicial ferma i definitiva.

- Les matèries inseparablement unides a alguna altra sobre la qual les parts no tinguen poder de disposició.

- Les qüestions en què, segons les lleis, ha d'intervenir el ministeri fiscal en representació i defensa dels qui, per mancar de capacitat d'obrar o de representació legal, no poden actuar per si mateixos.

- Les qüestions laborals.

Quant als tipus d'arbitratges, podem classificar-los en informals o formals.

L'informal és el que es fa al marge de la Llei d'arbitratge i pel qual dues o més persones pacten la intervenció diriment d'un tercer, o de més d'un, i accepten expressament o tàcita la seua decisió després que haja sigut emesa. Aquest acord és vàlid i obligatori per a les parts si hi concorren els requisits necessaris per a la validesa d'un contracte.

En aquest cas es requereix l'acceptació de la decisió del tercer després que s'haja emès, i aquesta produeix els efectes d'un vincle contractual, per la qual cosa si la decisió no es compleix cal acudir a la via judicial per a aconseguir el compliment del contracte.

Els formals són aquells arbitratges que es porten a terme d'acord amb el que es disposa en la Llei d'arbitratge. Se'n distingeixen dos tipus: arbitratge de dret i arbitratge d'equitat. El de dret és aquell en què els àrbitres han de decidir sobre la qüestió com si foren jutges, segons dret. Els àrbitres han de ser advocats. En el d'equitat els àrbitres resolen segons el seu parer, i per tant actuen sense estar, com els jutges ordinaris, sotmesos a l'imperi de la llei.

Són les parts les qui han de triar el tipus d'arbitratge. Si no ho fan, la Llei estableix que els àrbitres resoldran en equitat.

Per a les empreses, recórrer a els arbitratges té una sèrie d'avantatges. Per exemple, la rapidesa, perquè un arbitratge es tramita en poc de temps, i les parts poden establir el termini màxim dins del qual cal dictar el laude[1]. Destaca també l'eficàcia, ja que les parts poden escollir àrbitres pèrits en la matèria per raó de la seua titulació o professió.

Un altre avantatge és l'absència de publicitat, ja que es poden resoldre les diferències entre les parts de forma privada, de manera que no es generen aquests judicis paral·lels que els mitjans de comunicació solen produir, sobretot quan es tracta de casos amb un cert pes econòmic.

Finalment cal destacar la voluntarietat, perquè ambdues parts s'adhereixen lliurement al sistema de manera que resten vinculades a les resolucions, i l'executivitat, perquè els laudes –resolucions arbitrals– són d'aplicació obligada.

Per a tancar el capítol dels arbitratges, ens queda parlar de la clàusula arbitral. La clàusula arbitral és un element clau que cal incloure en els contractes perquè estiga assegurat el

[1] **laude** (de *laudar*) 1.*m*. DRET Decisió dictada pels àrbitres o amigables componedors. (DNV)

compliment de la voluntat de les parts de recórrer a l'arbitratge de la Cort posat cas que sorgisquen controvèrsies. Aquesta clàusula ha d'expressar la voluntat inequívoca de les parts de sotmetre a l'arbitratge la solució de totes les qüestions litigioses, o d'algunes d'aquestes, sorgides o que puguen sorgir de les relacions jurídiques en qüestió, siguen o no contractuals; també ha d'expressar l'obligació de complir la decisió que en resulte. No cal que la clàusula designe els àrbitres, però pot fer-ho.

El model recomanat per la Cort d'Arbitratge de la Cambra de Comerç de Madrid és el següent: "Les parts intervinents acorden que tot litigi, discrepància, qüestió o reclamació resultants de l'execució o interpretació del present contracte o relacionats amb aquest, directament o indirecta, es resoldran definitivament mitjançant arbitratge en el marc de la Cort d'Arbitratge de la Cambra de Comerç i Indústria de Madrid, a la qual es recomana l'admissió de l'arbitratge i la designació dels àrbitres d'acord amb el seu Reglament i Estatuts. Igualment les parts fan constar expressament el seu compromís de complir el laude arbitral que es dicte."

I ens resta encara, per a tancar aquest punt, tractar de l'actuació judicial del pèrit informàtic en els seus diferents àmbits. Seguint el Codi civil (CC) tindríem: la via civil (art. 1484 CC), la mercantil (art. 172 CC) i la laboral (art. 77 CC)

Perquè un pèrit puga actuar com a tal, l'ha de nomenar el jutge o tribunal, a proposta de les parts interessades o del mateix tribunal, a fi que puga ser recusat[2] per causes com ara el parentiu pròxim, haver informat anteriorment en contra del recusant, el vincle professional o d'interessos amb l'altra part, l'interès en el judici, i l'enemistat o l'amistat manifesta (art. 124 LEC) (Llei d'enjudiciament civil).

En la mateixa LEC trobem articles relatius a quan s'ha de fer la recusació (art. 125 LEC), com s'ha de fer (art. 126 LEC), la possibilitat que el pèrit no accepte la recusació (art. 127 LEC) o la condemna en costes per la recusació (art. 128 LEC). Cal deixar clar que un pèrit ha d'acceptar (o rebutjar) explícitament un peritatge si vol (o no vol) fer-lo (no s'aplica ací la frase feta *qui calla hi consent*). A més de les causes exposades, un pèrit ha de rebutjar el treball si el peritatge no correspon al perfil d'un informàtic, i se li assigna per error. Sobre aquest tema, són d'interès els art. 343 i 344 LEC.

El pèrit pot renunciar també si el seu nivell de coneixements o experiència no el faculten per a dictaminar sobre la matèria en qüestió, però si no es dona cap causa real, no hauria de rebutjar un peritatge judicial, per a evitar retards en el procés judicial.

Posat cas que la proposta de designació siga per part del jutge o tribunal, s'ha de fer bé a instància de part (art. 341 LEC) o bé sense instància de part, és a dir, mitjançant l'assignació d'ofici del pèrit per part del tribunal. El nomenament del pèrit ve també pautat per la LEC (art. 342 LEC).

---

[2] Segons el DNV, *recusar* és "No voler admetre (a algú) com a jutge, testimoni o àrbitre".

3. El pèrit. La seua responsabilitat i els seus drets

Parlem ara una mica sobre el pèrit en si, deixant de costat la seua possible activitat com a ciberdetectiu (Vacca, 155). Hem tractat del seu pas pels tribunals, com un element probatori més (article 1.215 del Codi civil, "les proves poden fer-se per instruments, per confessió, per inspecció personal del jutge, per pèrits, per testimonis i per presumpcions"). Referent a això, cal indicar que es diu explícitament que la prova per pèrit "només es pot utilitzar quan per a apreciar els fets siguen necessaris coneixements científics, artístics o pràctics". (article 1.242 CC). De la titulació del pèrit, en parla la LEC (article 615).

Evidentment, les actuacions davant els tribunals són una cosa molt seriosa, i una mala actuació pot comportar fortes sancions. Durant l'acompliment dels seus actes, hom pot incórrer en responsabilitats en els àmbits civil, penal i professional, per ser el culpable o per ser el causant, àdhuc de forma indirecta, del dany que es puga ocasionar.

Sobre la responsabilitat civil, cal assenyalar que el mer incompliment, per dol o negligència, és una possibilitat ben certa. És important, atès que quan, per culpa o negligència, es causa dany a algú, s'està obligat a reparar el dany produït. Hi ha tres classes de responsabilitat civil: la contractual (article 1.101 CC), l'extracontractual (articles 1.902 i següents CC) i la delictual, originada per un acte delictiu tipificat en el Codi penal (article 1.902 CC i articles del 109 al 119 del Codi penal). És important recordar una cosa que ja es va veure en la part de professionalisme: la importància de tenir una assegurança de responsabilitat civil, que cobrisca les possibles implicacions civils en què puga incórrer un pèrit informàtic en l'exercici de la seua activitat professional.

Quant a la responsabilitat penal, a diferència del cas anterior, ací és necessària la voluntarietat. S'hi inclouen el fals testimoniatge, el suborn (rebre alguna cosa a canvi de *mirar cap a una altra banda*) o la falta de compliment.

Sobre la responsabilitat professional, refrescant els temes ja vistos de professionalisme, n'hi ha prou de dir que hi entra l'ètica, ja que cal considerar que podem perjudicar altres parts (clients, la societat…).

No podem deixar passar una altra qüestió: els honoraris. Quant, i quan, ha de cobrar un pèrit. Si es tracta d'un afer extrajudicial, entra en el dia a dia d'allò que anomenem eufemísticament *mercat laboral*. Però quan es tracta d'una actuació davant els tribunals, atesa d'una banda l'aurèola de rigor que envolta la justícia, i de l'altra, la seua lentitud sempiterna, fins i tot en els pagaments, cal fer una sèrie de consideracions:

Els qui presten informe com a pèrits per ordre judicial tenen dret a reclamar els honoraris o les indemnitzacions que siguen justs. El jutge o la sala els poden impugnar si els consideren excessius, i després de sentir el dictamen de l'acadèmia, el col·legi o el gremi a què pertanguen els pèrits, aproven la taxació o manen fer-hi les alteracions que consideren justes, i a costa de qui s'escaiga. Els honoraris s'han de reclamar mitjançant una minuta detallada i signada. Com

es valora aquesta minuta? La veritat és que no hi ha una norma única per a fer-ho: depèn de factors tan diversos com el temps que s'haja emprat en la faena, la complexitat d'aquesta o les despeses associades (totes amb els justificants corresponents), com ara els desplaçaments.

Atesa aquesta lentitud a què al·ludíem adés, és fortament recomanable demanar una provisió de fons per a atendre les despeses que puguen produir-se i, almenys, preveure's. Sovint aquesta provisió seran tots els diners que el pèrit arribarà a veure, lamentablement.

Cal recordar, per acabar, que aquesta és una activitat professional, la qual cosa la subjecta a l'impost sobre activitats econòmiques.

4.Els dictàmens i informes pericials

Arriba el moment de definir el resultat del treball, aquest informe que es lliura per a ser estudiat i que passa a convertir-se en una prova, i que el pèrit haurà d'exposar (deposar) responent a preguntes que li facen el jutge i les parts.

Per les característiques molt particulars que presenta, ens centrarem en la justícia espanyola. Per a les persones interessades en el món anglosaxó, resulta interessant el capítol 5 del llibre de Philipp (358), autor que en pàgines precedents s'ocupa de catalogar els dictàmens (Philipp, 343) tot destriant-hi *grosso modo* entre **interns**, per a l'organització o empresa que els sol·licita, però que no seran divulgats de cap manera; **públics** (o **declaració**), a manera d'auditoria que pot ser difosa fins i tot usant mitjans de comunicació; i **externs** (en un tribunal), que són els que ens ocupen ara.

Endavant, doncs. Un dictamen és un informe escrit sobre una determinada matèria, degudament motivat i raonat, que emet un professional versat en aquesta matèria. Ha de ser clar, concís, fonamentat i justificat.

Dictamen, que acabem de definir com a 'informe', es relaciona amb *dictaminar*. Sembla que estem barrejant paraules, termes, la qual cosa no ens deixa cap més remei que acudir de nou al diccionari i comprovar que bàsicament parlem del mateix: de branques del mateix tronc. *Dictaminar* apareix en el DNV com "Emetre (un dictamen) sobre un tema determinat." *Informar* hi és definit com "Parlar davant del tribunal, els fiscals i els advocats, en compliment del seu càrrec."

Sempre que siga possible, cal contrastar les conclusions amb altres experts (garantint la confidencialitat dels continguts); és a dir, amb persones que, a partir de la documentació que els lliurem, puguen determinar si, a parer seu, les conclusions són adequades i estan degudament sustentades. El motiu d'això és obvi: podem ser experts en el nostre camp d'actuació, però ningú ho sap tot mai, sempre poden aparèixer llacunes que no aconseguirem esmenar ni mitjançant la bibliografia ni esmerçant hores i hores a fer proves tot cremant-nos les còrnies davant d'un monitor. En aquests casos esdevé imprescindible consultar amb altres persones que ens puguen il·luminar en la nostra foscor.

No oblidem que amb el peritatge pretenem ajudar aquells qui, per no tenir els coneixements tècnics necessaris, no poden respondre per si sols a algunes preguntes que els van sorgint, preguntes que ens traslladen i que seran el gruix d'aquesta prova que esdevé l'informe en si mateix, motiu pel qual aquest s'ha d'escriure pensant en el lector, exposant-hi les conclusions de manera raonada i comprensible als llecs en la matèria.

L'informe, com veiem, ha de ser escrit i cobrir l'objectiu de respondre a aquestes preguntes. S'ha de lliurar exclusivament a qui el va demanar, el qual decidirà si en lliura còpies, a qui i sota quines condicions.

Sovint es complementa amb algun annex que continga documentació tècnica o ampliacions de les respostes, que podrien semblar pobres argumentalment atesa la brevetat que ha de tenir una cosa orientada a algú que no en siga expert. Amb aquest document es pretén cobrir-se les espatles de cara a possibles revisions per altres pèrits, encarregades per alguna de les parts. Òbviament, no pot contradir el cos principal del dictamen.

Més documents que s'hi solen adjuntar:

- Una relació dels elements no rellevants que es retornen: ordinadors portàtils, càmeres, etc., i els que sí que resulten rellevants. El pèrit no ha de conservar cap element intervingut en finalitzar la recerca pericial.

- Una relació de fitxers, comptes de correu, etc., amb una breu descripció que explique el contingut que els fa rellevants.

Respecte al contingut de l'informe, no hi ha regles exactes, una recepta de cuina que ens done el pastís perfecte. Per exemple, un índex només caldria si la grandària del dictamen ho fa aconsellable. La bibliografia, les fonts consultades hi són sempre necessàries, així com les limitacions que hàgem trobat (si se'ns ha vetat l'accés a algun lloc, si no hem pogut entrevistar-nos amb algú, si s'ha descobert que certa informació que podria haver sigut rellevant per a la recerca ha sigut esborrada, etc.).

A manera d'esquema orientatiu, podríem dir que un model d'informe podria tenir les parts següents:

- **Consulta:** s'exposa breument la consulta que ens fan. Si la planteja un jutjat, cal plasmar les dades del jutjat, el nombre d'actuacions, la classe de judici i el nom i els cognoms del demandat.

- **Antecedents:** es detallen de forma clara i concisa.

- **Limitacions**: s'indica si s'ha pogut o no disposar de determinada informació, si s'ha pogut o no entrevistar una persona clau, l'obtenció de proves…

- **Al·legacions i consideracions**: en funció de tot l'anterior, es fan les al·legacions de caràcter tècnic, científic i jurídic. Han de tenir una base pràctica (basada en la pròpia experiència) i una altra de teòrica (basada en textos, manuals, etc.).

- **Conclusions:** s'acaba el dictamen amb l'opinió que a nosaltres ens mereix l'assumpte. Hem de mirar de no incloure-hi termes tècnics, que poden aparèixer, si són necessaris, en altres annexos, per evitar, p. ex., que un jutge interprete de forma equivocada la nostra opinió.

- **Observacions:** destinades als possibles lectors que desconeguen la matèria.

- **Signat:** preferentment en tots els fulls.

Una vegada vist què és el dictamen, haurem d'ocupar-nos, ni que siga per damunt damunt, de com és i com es fa.

Vacca (191 i següents) proposa una sèrie de passos molt simples:

1. Recuperació de dades

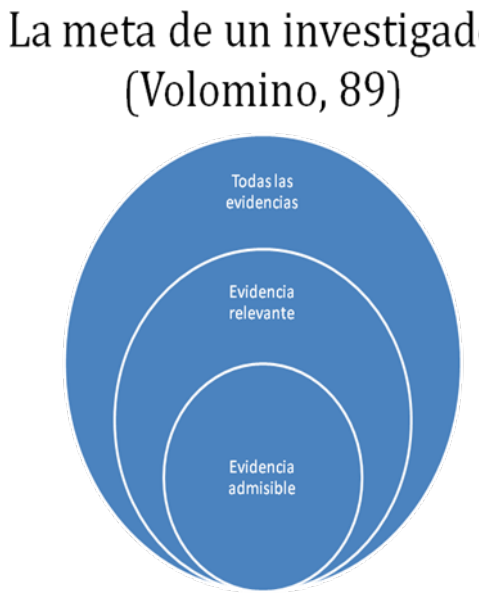
2. Recol·lecció de proves i confiscació de dades

3. Duplicació i preservació de les proves digitals

4. Verificació i autenticació d'imatges digitals

Potser el punt principal és el primer, el de la recollida de dades. Hem de tractar d'obtenir la informació necessària per a cobrir els objectius del treball que cal portar a terme. No tenir-la pot portar-nos a rebutjar l'encàrrec. I no parlem tan sols, encara que és la més important, de la informació presa com a prova, sinó de tota informació que ens puga servir de suport per a la nostra recerca, tant si aquesta procedeix de l'ús generalitzat (que pot no tenir valor per a un jutge en un moment determinat) com del bibliogràfic.

Sobre el segon punt, la recollida de proves, cal indicar que no tota prova té el mateix pes, com vam veure al principi d'aquest tema. La imatge següent ens ho mostra de forma gràfica (Volonino, 89):



La meta d'un investigador (Volomino, 89) / Totes les proves / Proves rellevants / Proves admissibles

La tercera i quarta fase entrarien dins del que podríem catalogar com *mètodes i tècniques*, que, com es pot entendre, són prou amplis i diversos perquè no convinga aprofundir-hi en aquest moment. Efectivament, depenent de l'objectiu del peritatge i l'entorn en el qual treballem, poden anar del mer estudi de la documentació que rebem a l'estudi de variacions en el codi font d'alguns programes, passant per entrevistes, estudis estenogràfics o qualsevol alternativa imaginable: creació de *scripts* que s'executen de forma automàtica; simulació de dades fictícies d'un proveïdor, client, etc.; preses de memòria; inclusió de rutines en els programes que s'executen per a poder fer estudis sense afectar els resultats reals; simulacions en paral·lel; traçat d'execucions (com el que s'usa en el desenvolupament per a depurar errors)…

Abans de començar a treballar hem de tenir clar que tenim tota la documentació i les fonts d'informació que calen per a cobrir els objectius del treball que cal fer; si no és així, caldrà reflectir-ho en l'apartat de limitacions, i en casos extrems, aquest fet ens pot portar a rebutjar l'encàrrec tot exposant-ne els motius.

És obvi que, a mesura que el pèrit va avançant en el seu estudi, pot fer noves troballes, descobrir noves proves, que haurà de reflectir en el seu informe.

Podria ser necessari fer alguna actuació sense avís previ, sempre amb autorització judicial prèvia i en coordinació amb la policia judicial, de manera que la informació vindria de forma directa. Això comporta un problema addicional: la precisió amb la qual es pot treballar en aquest moment de pressa i rebombori, amb els empleats de cara a la paret i veient, amb una barreja de sorpresa i indignació, com el pèrit els saforeja els ordinadors, mentre el secretari judicial volta pel local i afig encara angoixa al pèrit. Les dades obtingudes han de conservar la qualitat necessària perquè el treball no es desvirtue.

Em qualsevol cas, un dictamen ha de ser clar i ben explicat, fins i tot per a profans en la matèria, concís (això no vol dir que haja de ser breu: pot ser tan extens com es vulga, però molt concret en les conclusions), fonamentat (no basat en abstraccions i consideracions subjectives), justificat, de manera que no deixe espai per al dubte al possible lector, i amb una presentació tan agradable com es puga aconseguir.

Incloguem una precisió en aquest punt. Poden donar-se dos casos de dictàmens judicials d'aquest tipus: per la via civil, siga aportats amb la demanda (art. 336.2 LEC), siga nomenats pel tribunal (art. 346 LEC), o bé per la via penal (art. 346 i 348 LEC). En aquest darrer cas, la norma sí que indica alguna cosa sobre la composició del dictamen. Concretament, diu que:

L'informe pericial ha d'estar compost pels punts següents:

Descripció de la persona o cosa que en siga objecte, en l'estat o de la manera en què es trobe.

Relació detallada de totes les operacions practicades pels pèrits i el resultat d'aquestes.

Les conclusions que, en vista d'aquestes dades, formulen els pèrits, segons els principis i les regles de la seua ciència o art.

Una vegada lliurat el treball, resta valorar-lo. Aquesta valoració és de lliure ponderació pel tribunal, que pot rebutjar l'informe per diverses raons, com per exemple que considere que el pèrit no posseeix la titulació adequada a la naturalesa de la prova sol·licitada o no és l'idoni per al cas. El pèrit no prova res per si mateix, només subministra una base científica, tècnica, artística o pràctica per a jutjar sobre allò a què es refereix el dictamen. O, com diu la vella dita, *no som ningú*.

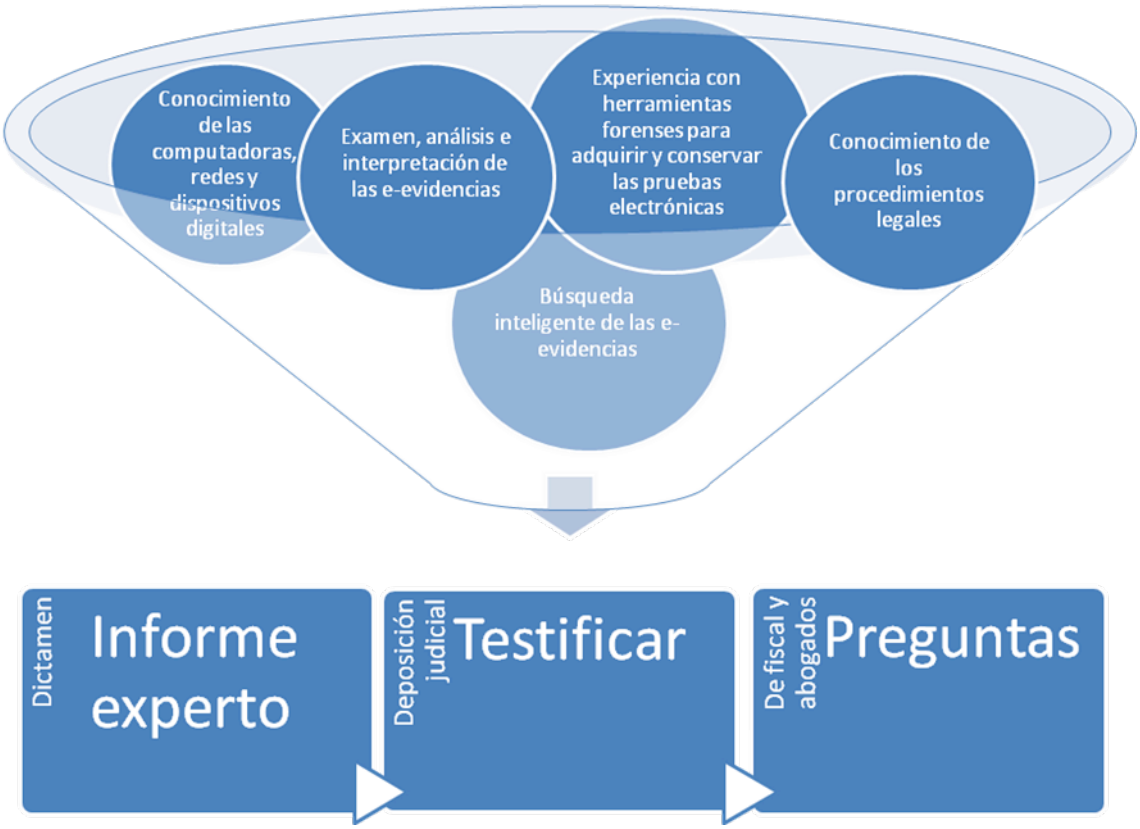
Les parts i els seus defensors poden concloure l'acte de reconeixement pericial i fer als pèrits les observacions que consideren oportunes per a esclarir les causes que han conduït a les conclusions de l'informe. I quan han intervingut diversos pèrits en el cas, poden confrontar els seus resultats, motiu pel qual seria avantatjós obtenir de manera anticipada els dictàmens dels pèrits de les altres parts. Si es tracta d'un cas complex (recordem, per exemple, l'11-M) en què treballen diversos pèrits, i tots o alguns d'ells estan d'acord, han de donar o estendre el seu dictamen en una única declaració signada per tots, cosa que estalvia un munt de temps en el procés judicial.

No podem tancar aquest fil argumental sense citar el principi rector que diu que *allò que no es troba en les actuacions no existeix legalment*, ja que sustentar decisions sobre informació no existent podria generar indefensió. Això obliga a prescindir totalment de la prova pericial que no s'haja practicat amb totes les garanties processals.

Lliurat l'informe, resta efectuar-ne la defensa a la sala. Si hi ha altres pericials practicats, seria interessant disposar-ne amb antelació per a analitzar-los i trobar arguments adequats, encara que, com pot imaginar-se, aquesta situació no és l'habitual. El que sí que ha d'emportar-se el pèrit a la sala és tot el material necessari per a defensar les seues conclusions: una de les parts, o el jutge, pot demanar explicacions al pèrit respecte als seus fonaments, per la qual cosa cal

tenir a mà tota la documentació possible, si cal, ordenada cronològicament, i fins i tot amb altres índexs auxiliars que permeten al pèrit localitzar alguna cosa en un termini de temps breu i raonable.

Tanquem aquest apartat amb una adaptació d'una figura de Volonino (296) que ens mostra el pas del conjunt d'habilitats que ha de tenir el pèrit per a exercir el seu treball al dictamen en si, considerat de forma àmplia.



Coneixement de les computadores, les xarxes i els dispositius digitals / Examen, anàlisi i interpretació de les proves electròniques / Experiència amb eines forenses per a adquirir i conservar les proves electròniques / Coneixement dels procediments legals / Cerca intel·ligent de les proves electròniques / Dictamen / Informe expert / Deposició judicial / Testificar / Del fiscal i els advocats / Preguntes

De les habilitats al treball del pèrit. Adaptat de (Volonino, 296)

5. Exemples

Un tema com aquest quedaria coix si no hi afegíem algun exemple. Òbviament, per qüestions d'extensió, aquests s'han simplificat tant com ha sigut possible, per deixar reduïts al màxim els dictàmens, i, és clar, substituint-hi les dades que es podrien relacionar amb persones reals per dades fictícies. Que ningú no s'hi senta identificat, per tant, i si ho fa, que quede entre ell i la seua consciència.

Primer exemple: possible robatori de dades. Uns empleats descontents se'n van de l'empresa amb, suposadament, una col·lecció de dades de clients amb les quals poden començar de nou, lluny dels seus caps anteriors.

L'infrascrit ALBERT MARIA POPEYE EL MARINER, graduat en Informàtica, designat pèrit per al Jutjat d'Instrucció número 14 de Klow en *les PRÈVIES 1674/2021 - A*, segons el seu parer, emet el següent

Dictamen

Consulta

Comprovar si els fitxers de dades que figuren en l'empresa Alabutxacaicapacasa SL procedeixen de l'empresa Socundespotasiquepassa SA.

No es formula cap pregunta precisa com a tal. Per a aconseguir l'objectiu exposat, es va fer una inspecció als locals de l'empresa Alabutxacaicapacasa SL durant la qual es va fer una còpia dels fitxers que componen la base de dades d'aquesta empresa. En la mateixa actuació, es van recollir uns documents que posteriorment, igual que els fitxers esmentats, es van contrastar amb la base de dades de l'empresa Socundespotasiquepassa SA, cercant-hi similituds.

Antecedents i limitacions

Pel que fa a l'actuació *in situ*, l'actitud cap al pèrit va ser de total col·laboració per part dels socis presents a l'empresa Alabutxacaicapacasa SL.

Per a l'estudi posterior, Socundespotasiquepassa SA va facilitar un CD d'instal·lació amb el programari de gestió de base de dades (ambdues empreses treballen amb el mateix programari de gestió, Gestió Desastrosa, programari basat en el Windows XP i comercialitzat per Aprengueremaprogramaralaparadeta SL) necessari per a l'estudi detallat dels fitxers que ja es trobaven a les mans del pèrit. Igualment es va facilitar al pèrit un PC portàtil amb una còpia de les dades de l'empresa Socundespotasiquepassa SA que calien per a fer les comparacions pertinents. Va caldre contactar amb l'empresa distribuïdora del programari de gestió de base de dades. Una vegada ens vam posar en contacte amb un tècnic d'aquesta, que responia al nom de pila d'Exuperanci, aquest va facilitar les claus precises per al funcionament de l'aplicació.

Al·legacions i consideracions

Les dimensions dissemblants de les bases de dades feien impossible una comparació *bit a bit*, és a dir, mecànica, registre a registre. La base de dades de Socundespotasiquepassa SA posseeix[3] 1.856 registres, mentre que la d'Alabutxacaicapacasa SL tan sols en té 69.

El primer acostament a aquest estudi va ser pel mètode anomenat en argot *de les empremtes digitals*. Aquest mètode consisteix a cercar, registre[4] a registre de la base de dades, similituds exactes, basant-se en el fet que, si ocorre una errata durant el tecleig per part de l'operador de les dades, aquesta errata té escassa probabilitat de repetir-se en un registre similar (que al·ludisca a la mateixa *fitxa* real) en una altra base de dades, de manera que pot dir-se, posat cas que es trobe aquesta coincidència en dos registres de bases de dades diferents, que aquest registre de la base de dades s'hi ha transferit[5] des de l'altra base de dades.

Després d'aplicar aquest mètode, tant *in situ* a les instal·lacions de l'empresa com posteriorment amb més calma, gràcies a la còpia que es va fer de la base de dades, no s'han trobat registres susceptibles de sospita d'haver sigut transferits automàticament. Aquest mètode, per raons òbvies, no implica que no s'haja fet cap còpia, tan sols que si s'ha fet, no ha sigut automàtica. Un registre es pot copiar de manera manuscrita a una fitxa de paper i després se'l pot introduir mitjançant el teclat en una altra base de dades. Això va implicar una posterior cerca manual, en la qual sí que es van trobar elements coincidents, que es detallen en l'apartat següent.

Es va sol·licitar posteriorment una confrontació de les fitxes manuals que s'havien recollit a l'empresa Alabutxacaicapacasa SL amb els registres de l'empresa Socundespotasiquepassa SA. Aquesta queda reflectida també en l'apartat següent.

Estudi de les dades

Comparació de les bases de dades

Per aconseguir una major claredat, ens referirem als registres per l'ordre seqüencial que els correspon en el fitxer de dades. En el fitxer de l'empresa Alabutxacaicapacasa SL els

---

[3] Ací convé fer un aclariment. En tot moment es parla en present dels continguts de les bases de dades, malgrat que per definició aquestes siguen canviants, atès que reflecteixen la vida de les empreses. Això es deu al fet que nosaltres ens centrem en l'estudi d'una *foto fixa* d'aquestes bases de dades, o en altres paraules, del contingut que tenien en un moment determinat, el moment en què es fa la còpia per a estudiar-les.

[4] Registre: en el món de les bases de dades, cadascuna de les fitxes que componen una taula. Taula: un conjunt de fitxes que tenen una certa homogeneïtat (per exemple, les dades dels nostres proveïdors podrien estar emmagatzemades en una mateixa taula).

[5] Migrat o copiat.

designarem amb els números d'1 a 69 (ja que 69 és el nombre total de registres que compon aquesta base de dades) i en el cas de l'empresa Socundespotasiquepassa SA, amb els números d'1 a 1856, sempre seguint-ne l'ordre seqüencial.

Per a determinar que un registre coincideix amb un altre, s'han verificat els camps més rellevants per a poder afirmar aquesta simultaneïtat. Aquests camps són l'adreça, el número, la població, el propietari i si es tracta de venda o lloguer. A la taula 1 apareixen reflectides aquestes coincidències. Per facilitar-ne la interpretació, apuntem que quan veiem a la primera fila amb dades un 11 a la columna "Registre Alabutxacaicapacasa SL" i en la segona, un 1421 en la columna "Registre Socundespotasiquepassa SA", significa això: *hi ha coincidència almenys en els camps adreça, nombre, població i propietari, i es tracta d'un immoble destinat al mateix tipus de transacció –lloguer o venda– en ambdues bases de dades.* Hi ha alguna excepció a aquesta norma general, ressenyada quan es produïsca en la columna "Observacions". Cal destacar que no es dóna una coincidència total en cap cas, però sempre per detalls menors, com pot ser el text del camp "Observacions", la forma d'escriure el nom del propietari –nom darrere o davant del cognom, abreviatures...– o el preu de venda –sempre variacions percentualment mínimes.

En l'annex 1 figura còpia impresa d'aquells registres duplicats; hi apareix sempre en primer lloc el registre pertanyent a la base de dades de l'empresa Alabutxacaicapacasa SL, i després el pertanyent a la base de dades de l'empresa Socundespotasiquepassa SA.

Dels 12 registres que presenten coincidències (en realitat n'hi ha un més, però sols perquè el registre 68 i el 69 de l'empresa Alabutxacaicapacasa SL resulten ser el mateix, i aquest és un dels coincidents amb la base de dades de l'empresa Socundespotasiquepassa SA), dos d'aquests, com s'especifica en el camp "Observacions" de la taula 1, no compleixen aquesta norma general que hem exposat més amunt. Es tracta, en tots dos casos, de registres que es refereixen al mateix immoble físic, però amb diferents modalitats (venda en lloc de lloguer i viceversa) i, en el segon cas, amb diferent nom de propietari.

Taula 1. Registres coincidents

Número de registre en la base de dades d'Alabutxacaicapacasa SL :	Número de registre en la base de dades de Socundespotasiquepassa SA:	
Registre d'Alabutxacaicapacasa SL	**Registre Socundespotasiquepassa SA**	**Observacions**
11	1421	
13	485	
20	1702	

21	827	
24	1145	Apareix com a lloguer en lloc de venda.
26	1784	
27	1138	
33	1345	
61	1042	
63	1412	Apareix venda en lloc de lloguer i un altre nom de propietari.
67	1376	
68 i 69 (duplicats)	722	

Referent a la segona part de l'estudi, confrontació de les fitxes manuals que s'havien recollit en l'empresa Alabutxacaicapacasa SL amb els registres de l'empresa Socundespotasiquepassa SA

Conclusions

Per tot el que s'ha expressat abans, i segons la documentació objectiva analitzada, la bibliografia consultada i la pràctica informàtica generalitzada, hem de concloure que hi ha alguna coincidència, que no ens atrevim a qualificar de significativa ja que per a això caldria tenir un coneixement del sector immobiliari del qual manca el pèrit infrascrit. D'altra banda, és impossible respondre a preguntes formulades, atès que no n'hi ha.

Tot això llevat que hi haja una opinió millor, a la qual ens sotmetem.

Klow, 31 de gener de 2020

Signat:

Albert Maria Popeye El Mariner

DNI: 99.999.999

Segon exemple: després de passar una enquesta en una empresa, hom creu veure-hi l'ús il·legal de programari. S'hi usen programes per als quals no s'han pagat les llicències oportunes. Presumptament, és clar. Aquest exemple és una adaptació del magnífic llibre de Del Peso, que es pot trobar en la bibliografia.

Consulta

Conclusions que es poden deduir respecte a la utilització de programari il·legal de l'enquesta sobre utilització de programari realitzada a l'empresa Informàtica Copiada SA

Dictamen

Antecedents

El cap de Sistemes d'Informació d'Informàtica Copiada SA contesta a una enquesta en què, entre altres preguntes, figuren les següents:

- Nombre d'estacions de treball de l'empresa

- Quins paquets de programari utilitza cada estació de treball

- Paquets de programari contractats per l'empresa

- Import total del programari contractat

Al·legacions i consideracions

En el present dictamen pretenem, a través de la informació recollida mitjançant una enquesta realitzada per Informàtica Copiada SA, determinar l'ús del programari (programes producte) que es fa en els ordinadors personals d'aquesta empresa, i també constatar si s'hi està infringint la Llei de propietat intel·lectual respecte als drets d'autor.

L'enquesta analitzada presenta els punts d'interès següents:

- L'enquesta respon a una sèrie de preguntes de caràcter innocu considerades aïlladament i pretén recaptar informació autèntica i veraç sobre la utilització de programari (programes producte) subjecte a llicència d'ús pels diferents subministradors; en aquest cas resulta bastant completa i encertada per a les finalitats que persegueix.

- En l'enquesta s'identifica clarament Informàtica Copiada, així com la persona que hi respon, el seu càrrec i les seues àrees específiques de responsabilitat.

- S'observa que la persona encarregada de respondre l'enquesta té responsabilitat real sobre: l'adquisició tant de maquinari com de programari, o l'aprovació per a adquirir-ne, i la definició dels requisits tècnics i els estàndards d'ús corresponents. Es dedueix d'això que, a més del coneixement del treball que té assignat per la companyia per a la qual treballa, té un coneixement perfecte i directe de la situació de la microinformàtica de l'empresa.

- Pel que fa a l'adquisició i la utilització de paquets de programari per la companyia, s'observa que de vuit paquets instal·lats, només un ha sigut adquirit a un distribuïdor. De les dades de l'enquesta es pot deduir que més d'un 90% dels programes instal·lats han sigut reproduïts internament de forma il·legal. És important ressaltar que, sent 600 les còpies existents i en ús permanent en els 80 ordinadors personals de l'empresa, tan sols 40 han sigut adquirides a un distribuïdor, mentre que les restants són reproduccions internes i no disposen de les llicències d'ús corresponents.

- Un altre punt que mereix especial atenció és l'alt nivell d'utilització d'aquest tipus de programari en la companyia corresponent, tant al Departament de Microinformàtica com a la resta dels departaments de la companyia que tenen ordinadors personals.

- Quant al capítol econòmic, hi ha una evident manca de correspondència entre el nombre de còpies utilitzades i la despesa corresponent a aquesta partida en la companyia: 600 còpies utilitzades i 800.000 xavos de despesa.

Conclusions

De l'estudi es dedueix clarament que en Informàtica Copiada s'ha usat programari de forma il·legal amb una clara infracció de la Llei de propietat intel·lectual, és a dir, s'ha fet el que col·loquialment es denomina *pirateria del programari*.

Tot això llevat que hi haja una opinió millor, a la qual ens sotmetem.

Catamarruc, 9 de març de 2025

Signat:

Albert Maria Popeye El Mariner

DNI: 99.999.999

6. Bibliografia

El present tema és una revisió més que profunda d'un altre que fou presentat en:

De Miguel Molina, María i Oltra Gutiérrez, Juan V. (2007). *Deontología y aspectos legales de la informática: cuestiones jurídicas, técnicas y éticas básicas*. Servei de Publicacions de la Universitat Politècnica de València, València.

Aquest volum, editat sense cap més ànim que el purament domèstic en la docència, ha sigut el que podríem anomenar –dins de la modèstia de la difusió dels textos universitaris– un *top* de vendes, i fins se'n van vendre exemplars en terres llunyanes i remotes. Intentarem trobar la música exacta, de nou, per a aquesta cançó.

Referències bàsiques:

Carvajal, Armando (2007). *Introducción a las técnicas de ataque e investigación forense, un enfoque pragmático*. Globalteksecurity, Colòmbia.

Daniel, Larry E.; i Daniel, Lars E. (2012). *Digital Forensics for Legal Professionals. Understanding Digital Evidence From the Warrant to the Courtroom*. Syngress, EUA.

Del Peso Navarro, Emilio. (2001). *Peritajes Informáticos*. Ediciones Diaz de Santos, Madrid. N'hi ha un precedent: *Manual de dictámenes y peritajes informáticos: análisis de casos prácticos*. Emilio del Peso Navarro. (1995)

Dube, Roger (2008). *Hardware-Based Computer Security Techniques to Defeat Hackers. From Biometrics to Quantum Cryptography*. Wiley, EUA.

Filiol, Eric (2005). *Computer viruses: from theory to applications*. Springer, EUA.

Hoog, Andrew (2011). *Android Forensics*. Syngress, EUA.

Lillard, Terrence (2010). *Digital forensics for network, Internet, and cloud computing: a forensic evidence guide for moving targets and data*. Syngress, EUA.

López Manrique, Yuri Vladimir (2006). *Computación forense: una forma de obtener evidencias para combatir y prevenir delitos informáticos*. Universitat de San Carlos, Guatemala.

López Tarraella, Aurelio (2012). *Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*. Springer, Holanda.

Noblett, Michael i Feldman, Adam (1999). *Computer Forensics: Tools & Methodology. Critical Review & Technology. Assessment Report*. IATAL, EUA.

Philipp, Aaron; Cowen, David; i Davis, Chris (2010). *Hacking Exposed Computer Forensics*. MC Graw Hill, EUA.

Vacca, John R. (2005). *Computer Forensics: Computer Crime Scene Investigation*. Thomson. Boston, EUA.

Volonino, Linda; i Anzaldua, Reynaldo (2008). *Computer Forensics For Dummies*. Wiley, EUA.

Referències útils per a saber-ne més, o per a complementar amb anècdotes:

Vizcaíno Casas, Fernando (1997). *Historias puñeteras*. Planeta, Madrid.

Boixo, Ignacio (2003). *Guía de buenas prácticas para el peritaje informático en recuperación de imágenes y documentos*, http://www.infoperitos.com/guiaimagenes.pdf (juliol del 2012)

Martos, Juan (2006). *El perito informático, ese gran desconocido*, http://www.recoverylabs.com/prensa/2006/10_06_peritaje.htm (juliol del 2012)

Oltra Gutiérrez, Juan V. (2008). *Introducción a los peritajes*, http://riunet.upv.es/handle/10251/1493 Universitat Politècnica de València. Escola Tècnica Superior d'Enginyeria Informàtica – ETSINF, UPV, València (juliol del 2012)

Farmer, Dan i Venema, Wietse (2005). *Forensics Discovery*, Addison-Wesley, EUA, http://www.porcupine.org/forensics/forensic-discovery/ (juliol del 2012). Aquests autors faciliten una col·lecció d'eines útils per a investigar en entorns UNIX, anomenades genèricament "The Coroner's Toolkit", disponibles en http://www.porcupine.org/forensics/tct.html .

Ram, Kylie (2008). *Introduction to Forensics*. Linux Journal (gener del 2008). Disponible en: http://www.linuxjournal.com/article/9922 (juliol del 2012).

Ram, Kylie (2011). *Introduction to Forensics* (conferència), http://greenfly.org/talks/security/forensics.html (juliol del 2012).

Normativa d'interès:

Codi civil, http://www.ucm.es/info/civil/jgstorch/leyes/ccivil.htm (juliol del 2012)

Llei d'enjudiciament civil, http://noticias.juridicas.com/base_datos/privado/l1-2000.html, matisada per la Llei 13/2009, de 3 de novembre, de reforma de la legislació processal per a la implantació de la nova oficina judicial http://civil.udg.es/normacivil/estatal/proceso/l13-2009.htm (juliol del 2012).

Llei d'enjudiciament criminal, http://noticias.juridicas.com/base_datos/penal/lecr.html (juliol del 2012)

Associacions professionals:

Acadèmia Americana de Ciències Forenses http://www.aafs.org/ (juliol del 2012)

American Board of Criminalistics, http://www.criminalistics.com/ (juliol del 2012)

Forensic Expert Witness Association, http://www.forensic.org/ (juliol del 2012)

Eines útils

Entorn Windows

Encase Forensic, http://www.guidancesoftware.com/ (juliol del 2012)

Eines *open source*, http://www2.opensourceforensics.org/tools/windows (juliol del 2012)

Entorn Linux

Penguin SLEUTH KIT (Knopix), http://www.sleuthkit.org/sleuthkit/desc.php ; també http://penguinsleuth.org/index.php?option=com_frontpage&Itemid=1 (juliol del 2012)

Local Area Security Linux (Knopix) http://jascha.me/projects/local-area-security/ (juliol del 2012)

Helix (knoppix), http://www.e-fense.com/products.php (juliol 2012). És interessant aquesta pàgina en italià: http://www.forlex.it/index.php

Knoppix STD http://s-t-d.org/ (juliol del 2012)

Altres pàgines d'interès::

Belgian Computer Forensic, http://www.lnx4n6.be/ (juliol del 2012)

El llibre de Volonino porta uns complements interessants, disponibles en: www.dummies.com/go/computerforensics (juliol del 2012)

Forensic and Incident Response Environment (FIRE) http://fire.dmzs.com/ (juliol del 2012)

Inside Security (INSERT), http://www.inside-security.de/insert_en.html (juliol del 2012)

IRItaly Live CD Project (**Gentoo** based), http://www.iritaly-livecd.org/ (juliol del 2012)

Índex