INFORMÀTICA FORENSE I VALIDACIÓ DE MÈTODES

Josep M. Arqués Soldevila
Divisió de Policia Científica, Mossos d'Esquadra

Manel Blanquez Piquero
Unitat de Ciberseguretat, Comissaria General de les Tecnologies de la Informació i la Comunicació

1. Què són les ciències forenses?

En termes generals coneixem com a ciència forense la que té per objecte l'aplicació de pràctiques científiques dins del procés legal [1].

Normalment, la ciència forense s'anomena només amb el terme *forense*, el qual, acceptat arreu del món, s'usa sovint com a sinònim de *legal*. La ciència forense inclou tant la branca civil com la penal [1].

La ciència forense s'ha expandit tant que, actualment, hi ha moltíssimes branques de les ciències que hi donen suport en la resolució dels problemes que planteja el dret. A títol orientatiu, algunes d'aquestes branques són:

- La *lofoscòpia*, l'estudi i l'anàlisi, amb finalitat d'individualització, de les empremtes deixades per les crestes papil·lars localitzades en les mans i els peus d'un individu.
- La *genètica forense*, el conjunt de tècniques d'anàlisi de la variabilitat genètica entre individus amb la finalitat d'individualitzar les restes d'origen biològic que s'han trobat en l'escena d'un crim.
- L'*anàlisi forense de fibres i pintures*, el conjunt de tècniques i metodologies emprades per a dur a terme l'estudi de fibres i pintures trobades a l'escena d'un crim (per exemple, per a comparar la pintura d'una bicicleta, que ha estat envestida per un vehicle, amb les marques de pintura trobades en el vehicle del sospitós).

En definitiva, a més de les disciplines que ja intuïm directament vinculades de manera exclusiva a la criminalística, qualsevol disciplina pot esdevenir forense en ser aplicada en la col·laboració amb la justícia. Per exemple, entenem per *lingüística forense* l'estudi i interpretació de la llengua per a utilitzar-la com a prova jurídica [1].

Per a poder relacionar els autors amb els fets ocorreguts i presentar les troballes recollides com a prova jurídica, un principi fonamental aplicat a totes les disciplines forenses és l'anomenat *principi d'intercanvi* o *transferència de Locard.*

1.1. *Principi de Locard*

Edmund Locard (1877-1966) va elevar a la categoria d'imprescindibles una sèrie de proves forenses que abans es consideraven inútils o fins i tot s'ignoraven. El principi d'intercanvi de Locard es pot resumir en la frase «cada contacte deixa un rastre», que significa que en la majoria de les accions quotidianes hi ha un intercanvi [1].

Per exemple, el trencament d'un vidre per un cop de puny deixa restes de sang en l'escenari i fragments de vidre en la persona. De la mateixa manera, una trepitjada deixarà una petjada sobre el terreny i rastres de terra a la sola de la sabata. El principi de Locard ens assegura que, en la gran majoria de situacions, hi ha un intercanvi, només cal tenir la ment desperta i buscar-lo [1].

2. La informàtica forense (o forense digital)

En el món digital, el principi de Locard també es pot aplicar perquè qualsevol interacció amb un ordinador n'afecta l'operativa, l'estat de la memòria i, fins i tot, el que s'escriu en el disc dur, de manera que un expert pot trobar traces d'aquesta interacció i també tots els detalls que permeten reconstruir els fets i identificar-ne els autors. Si bé és cert que les proves informàtiques (o evidències digitals) poden ser fràgils, això no vol dir que no existeixin i, per tant, que no es puguin obtenir proves de molta rellevància en sistemes informàtics [2].

De fet, en els darrers anys, una de les ciències forenses que ha experimentat un auge més notable, com a conseqüència de la seva presència en tots els àmbits de la vida quotidiana, és la informàtica forense o ciència forense digital, definida com aquella ciència forense que s'encarrega d'assegurar, identificar, preservar, analitzar i presentar la prova digital, de manera que sigui acceptada en un procés judicial [2].

2.1. *Fiabilitat de les disciplines forenses*

Tot i que, com a disciplina, la ciència forense digital és molt jove, ni que sigui de manera intuïtiva, és fàcil que ens

adonem de la seva rellevància. Tant des del punt de vista dels investigadors com dels tribunals, la informàtica forense ha permès la resolució de molts successos en els quals hi ha involucrades qüestions tan diverses com ara el monitoratge de comunicacions, les transaccions comercials, les ubicacions, els comptes bancaris, els documents digitalitzats, els arxius multimèdia, entre moltes altres possibilitats inherents a la implantació de les tecnologies de la informació a la nostra vida quotidiana. És normal doncs que, seguint el curs d'altres disciplines forenses, la comunitat judicial i policial estigui particularment interessada a assegurar la fiabilitat de les eines i mètodes emprats en la ciència forense digital [3].

No obstant això, queda un llarg camí al davant per recórrer, ja que, com s'ha fet palès en diverses ocasions, les ciències forenses encara pateixen moltes mancances i febleses, revelades en molts casos rellevants i ben coneguts fins i tot per al gran públic [3].

A tall d'exemple, a l'article d'opinió «Junk Science at the F.B.I.» [4], s'explica que, com a conseqüència de la identificació d'una mostra de cabells (prova forense prèvia a l'aparició de l'ADN en criminalística), feta pels analistes de l'Oficina d'Investigació Federal, es va condemnar una persona innocent. Els errors comesos en aquesta prova pericial varen provocar que l'Oficina d'Investigació Federal hagués de revisar més de 2.500 casos en els quals les identificacions de cabells havien estat considerades evidències fonamentals.

Més recentment, i a prop nostre, cal destacar la polèmica suscitada per l'anomenat *cas Bretón*, en el qual, en un primer moment, un antropòleg forense va determinar que les restes òssies trobades a les deixalles del que semblava una foguera es corresponien a restes òssies d'animals. Posteriorment, dos informes forenses (sobre les mateixes evidències) varen corroborar que aquelles mostres no pertanyien a cap animal, sinó a dos nens, fet que les va convertir automàticament en proves fonamentals per a la resolució del cas [5].

És per això que, en els darrers anys, les ciències forenses han estat molt qüestionades per part de la comunitat científica, no només pels mètodes de treball que empren, sinó per la base en què se sostenen i, fins i tot, la manera com s'expressen i mostren els resultats obtinguts en els informes pericials.

La ciència forense digital, com qualsevol altra disciplina forense, també es troba subjecta a aquesta mateixa crítica i és, precisament, la necessitat de garantir la fiabilitat dels seus mètodes i eines, un dels principals eixos motivadors d'aquest document.

3. El marc normatiu europeu

Com a conseqüència de les necessitats exposades en l'apartat anterior, el Consell de la Unió Europea, el novembre del 2009, va publicar la Decisió marc 2009/905/JAI [6], sobre l'acreditació de prestadors de serveis forenses (entenent com a prestador de serveis forenses qualsevol organisme públic o privat que dugui a terme activitats de laboratori forense a petició de les autoritats policials i judicials) [3].

Amb aquesta iniciativa, la Unió Europea es va proposar establir un marc de cooperació policial i judicial en matèria penal entre els estats membres que permetés l'intercanvi d'informació relativa a les proves forenses, determinant normes comunes per als prestadors de serveis forenses amb la finalitat d'assegurar una base mínima d'entesa i pràctica comuna a tots els laboratoris de la xarxa forense europea [3].

Fins al dia d'avui, tot i que no és una tasca que s'hagi assolit completament, s'han produït diverses iniciatives que, amb sort diversa, han deixat empremta. A tall d'exemple, la xarxa ENFSI (European Network of Forensic Science Institutes) ha elaborat diversos manuals de bones pràctiques que estableixen directrius bàsiques vàlides per a moltes disciplines forenses, laboratoris tan prestigiosos com ara el NFI (Netherlands Forensic Institute) han ofert formacions tècniques molt avançades (adreçades al personal tècnic dels laboratoris europeus), s'han dut a terme proves interlaboratorials en l'àmbit europeu i, fins i tot, s'ha intentat (de moment sense èxit) establir uns criteris mínims per a l'avaluació de la competència del personal de la policia científica. D'entre totes aquestes iniciatives destaca la implantació progressiva de la norma ISO/IEC 17025 als laboratoris d'assaigs de ciències forenses. La implantació d'aquesta norma a assajos tan diferents i allunyats dels propòsits inicials de l'ISO/IEC 17025 com són l'estudi de fibres o d'elements balístics és una tasca complexa i amb molts buits que cal interpretar per tal d'adaptar l'operativitat del laboratori al contingut de la norma [3].

3.1. *Aplicació de la norma ISO/IEC 17025 a les disciplines forenses*

Tot i que moltes de les iniciatives forenses europees no tenen un caràcter obligatori, la norma ISO/IEC 17025 és una excepció per a alguns assajos, per als quals, amb independència de la normativa de cada país, l'acreditació és preceptiva. Això és el que passa, concretament, amb els assajos relatius a l'obtenció de perfils d'ADN i la identificació de dades dactiloscòpiques (empremtes dactilars). El caràcter preceptiu de la norma ISO/IEC 17025 queda determinat a l'article 1 de la Decisió marc europea 2009/905/JAI, on s'exposa:

> 1.2. Dicha finalidad[1] se logrará garantizando que los prestadores de servicios forenses que llevan a cabo actividades de laboratorio sean acreditados por un organismo de acreditación nacional que certifique que las actividades de laboratorio cumplen la norma EN ISO/IEC 17025.

1. Per *finalitat* s'entén que les activitats de tot laboratori sota la norma ISO/IEC 17025 siguin fiables i puguin ser reconegudes per qualsevol altre laboratori, de qualsevol estat membre, que operi sota la mateixa norma.

I a l'article 7, la Decisió marc condiciona un termini d'implantació de la norma ISO/IEC 17025 per a les dues disciplines de la policia científica abans esmentades (obtenció de perfils d'ADN i identificació de dades dactiloscòpiques):

> 7.1. Los Estados miembros tomarán las medidas necesarias para dar cumplimiento a lo dispuesto en la presente Decisión marco en relación con los perfiles de ADN a más tardar el 30 de noviembre de 2013.
>
> 7.2. Los Estados miembros tomarán las medidas necesarias para dar cumplimiento a lo dispuesto en la presente Decisión marco en relación con los datos dactiloscópicos a más tardar el 30 de noviembre de 2015.

Val a dir que tots els cossos policials de l'Estat varen assolir les seves respectives acreditacions en aquest àmbit abans de la finalització dels terminis indicats a la Decisió marc.

A partir de l'assoliment d'aquestes fites obligatòries, els laboratoris de policia científica de tot el país han fet molts esforços per a estendre el paraigua de la norma ISO/IEC 17025 a tota la resta de ciències forenses, que inclouen assajos tan diversos com ara l'escriptura manuscrita, la distància de tret, la balística identificativa, entre moltes altres disciplines criminalístiques.

Posteriorment a la publicació de la Decisió marc, el desembre de 2011, el Consell de la Unió Europea va aprovar unes conclusions relatives a la creació de l'Espai Europeu de Policia Científica i es va posar com a horitzó per al seu assoliment l'any 2020 [7].

L'objectiu (encara no assolit) d'aquest espai és la facilitació de la cooperació entre els estats membres, pel que fa a les ciències forenses, compartir resultats, mantenir i millorar la qualitat d'aquestes disciplines, i encoratjar tots els laboratoris de la Unió Europea a treballar sota estàndards de sistemes de qualitat.

Més endavant, l'any 2016, el Consell de la Unió Europea va publicar les conclusions sobre el camí que calia seguir per a l'assoliment de la creació de l'Espai Europeu de Policia Científica.

No és estrany doncs, que en aquest document, *Conclusiones del Consejo y Plan de acción sobre el camino a seguir para la creación del Espacio Europeo de Policía Científica*, del Consell de la Unió Europea (juny 2016) [8], s'aprofundeixi en els mateixos aspectes que la Decisió marc 2009/905/JAI, amb una clara voluntat de teixir complicitats per a assolir la creació d'un espai forense europeu. Aquest document posa un èmfasi especial en la utilització de manuals de bones pràctiques per a les disciplines de policia científica, estimula l'intercanvi d'informació forense procedent de bases de dades, promou la realització de proves d'aptitud i exercicis de comparació interlaboratorials, promou la conscienciació sobre la tasca de la policia científica i la formació sobre aquest particular, destinada a les comunitats policials i judicials, i estimula l'acreditació voluntària dels prestadors de serveis forenses i l'assegurament, de forma voluntària, de la competència del personal científic policial.

Justament, en el darrer apartat del document sobre l'Espai Europeu de Policia Científica, s'esmenta explícitament la informàtica forense:

> Referencia 5. Conclusiones del Consejo y Plan de acción sobre el camino a seguir para la creación del Espacio Europeo de Policía Científica:
>
> Elaboración de un plan de acción para estimular la acreditación de los procedimientos de policía científica de forma voluntaria, centrado en los ámbitos de armas y municiones, explosivos, drogas e informática forense, así como estimular la acreditación voluntaria de normas unificadas para la recogida de pruebas en el lugar del delito (Comisión).

Per tant, l'aplicació de la norma ISO/IEC 17025 als laboratoris d'informàtica forense (especialment els policials) és una qüestió encara oberta, a causa del seu marge interpretatiu, la qual ja no es pot defugir. Per dur a terme aquesta implementació no n'hi ha prou d'aprofitar els manuals de bones pràctiques ja desenvolupats, sinó que cal saber com avaluar les característiques pròpies de cada laboratori.

En aquest apartat hem vist, doncs, el marc que origina la necessitat d'establir un paraigua europeu comú per a les ciències forenses i la decisió d'articular-ne la fiabilitat i garantia al voltant de la norma ISO/IEC 17025, la qual, d'origen, no està específicament adreçada als assajos de policia científica. Tot seguit es veurà quines implicacions té l'adopció d'aquesta norma en els assajos que es pretenen acreditar.

4. Validació de mètodes i eines en forense digital

Podem entendre un mètode forense com aquell conjunt d'operacions ordenades i establertes amb la finalitat d'assolir un determinat objectiu en l'àmbit forense.

Tot i que les eines forenses no constitueixen, en si mateixes, cap mètode, sí que conformen una de les etapes més importants de qualsevol metodologia d'anàlisi d'informàtica forense. Les eines forenses proveeixen els resultats de l'anàlisi, més enllà de moltes altres qüestions molt importants, com ara la traçabilitat i la integritat de les evidències o l'expressió dels resultats. La fiabilitat de les eines forenses és un dels elements clau que cal tenir en compte quan es comprova que el mètode és apte per a l'ús previst.

De fet, tots els mètodes forenses a l'empara de la norma ISO/IEC 17025 han de ser convenientment verificats o validats abans que puguin ésser utilitzats, la qual cosa ens obliga a quantificar d'alguna manera els errors que es puguin produir en l'aplicació del mètode o en l'ús de l'eina.

Un mètode, en informàtica forense, és un procés sencer que inclou moltes fases, entre les quals hi hauria l'aplicació de l'eina forense a les evidències digitals. Per tant, un dels eixos sobre els quals bascula la validació ha de ser, necessàriament, l'eina forense que és la que, al cap i a la fi, ens proporciona els resultats de l'anàlisi. Tot seguit veurem algunes estratègies i paràmetres de validació que ens permetran avaluar la fiabilitat d'una eina forense. Òbvia-

ment, en informàtica forense també es produeixen errors, però són molt diferents dels conceptes habituals d'error sistemàtic i aleatori.

4.1. *El concepte d'error en l'àmbit forense digital*

Al marge de la necessitat de validar els nostres mètodes (si treballem a l'empara de la norma ISO/IEC 17025), ens trobem en la necessitat d'explicar en un judici que els nostres resultats són fiables. Però, ho són realment? Fins a quin punt en podem estar segurs? Podem parlar d'error? El podem acotar?

En altres disciplines forenses (comparació d'empremtes dactilars, informes pericials fisonòmics o de documentoscòpia, comparació de roderes, etc.), ja s'han començat a incorporar quantificacions de l'error (taxes de falsos positius i negatius, entre altres paràmetres similars) a les validacions dels mètodes i informes pericials. En aquests casos, la comparació s'efectua entre dos ítems (el dubtós i l'indubtable). Es fa, doncs, un únic examen o test per a cada parella dubtós/indubtable i, a l'hora de comptabilitzar les taxes d'error, se sol partir d'exercicis de comparació interlaboratorial, en els quals l'organitzador de l'exercici coneix si efectivament el dubtós es correspon o no a l'indubtable. A partir d'aquí, és senzill calcular les taxes esmentades. Per generalitzar aquest tipus d'exàmens criminalístics emprarem el terme *matching*, en referència al resultat que obtindrem en fer la prova, és a dir, si dos ítems, en ser comparats, donen o no un *match*. En aquest tipus d'exàmens, de manera natural, es desprenen les taxes d'error i la fiabilitat es pot expressar en termes probabilístics[2].

Aquesta quantificació, d'aplicació a mètodes humans (la comparació entre el dubtós i l'indubtable, l'efectua una persona qualificada per a l'assaig), presenta diversos inconvenients, com ara la dificultat de projectar en el futur la capacitat d'encert dels analistes que practiquen la prova, o la dependència de l'encert amb el nivell de qualificació de l'equip professional. Si més no, a més de l'aspecte puramment numèric, l'actualització periòdica d'aquestes taxes d'error permet caracteritzar la fiabilitat del mètode i registrar les tendències del laboratori al llarg del temps.

En el cas de l'anàlisi forense digital, no és tan senzill. No hi ha un únic test o prova, sinó múltiples funcionalitats que cal verificar (cerca de cadenes, *carving*[3] d'imatges, etc.). Això fa que la validació de les eines forenses sigui un procés molt complicat per la feina exhaustiva que suposa (tant a l'hora de dissenyar les proves que s'han de fer, com per la realització mateixa i l'explotació dels resultats obtinguts).

4.1.1. *Matrius de confusió i mesura de la fiabilitat*

Les disciplines criminalístiques basades en la comparació d'un element dubtós amb un element indubtable sovint empren matrius de confusió per a objectivar el rendiment o la fiabilitat dels seus mètodes.

Aquestes taules consten de dues files que es corresponen al resultat d'aplicar el mètode o algorisme, i dues columnes que representen els valors de referència coneguts de la mostra analitzada. Les diferents combinacions de la taula mostren el nombre de positius veritables (*true positives*), falsos positius (*false positives*), falsos negatius (*false negatives*) i negatius veritables (*true negatives*) (figura 1).

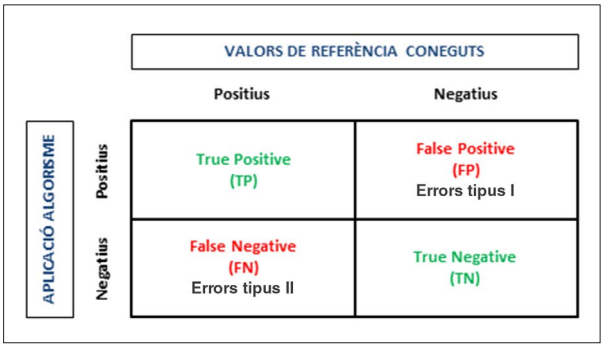

FIGURA 1. Matriu de confusió per a objectivar el rendiment o fiabilitat dels mètodes basats en la comparació d'un element dubtós amb un element indubtable.

Per a l'avaluació d'un mètode o algorisme, tenen una rellevància especial els falsos negatius, també anomenats *errors de tipus II* i els falsos positius o *errors de tipus I*.

Els errors de tipus I fan referència als elements rellevants que no s'han detectat, i els errors de tipus II, als elements detectats com a rellevants incorrectament. Tot i que no hi ha cap tipus d'error desitjable, normalment l'error de tipus I, o fals positiu, és l'error més greu i que cal evitar (podria implicar, per exemple, l'empresonament d'una persona innocent).

Un possible enfocament, per tal d'equiparar la validació d'eines forenses digitals amb els paràmetres de rendiment emprats en altres disciplines forenses més consolidades, consistiria a crear matrius de confusió per a les diferents eines i analitzar els paràmetres estadístics que s'obtenen per a poder arribar a definir uns criteris de validació.

Com ja s'ha dit, en el cas de l'anàlisi forense digital, els càlculs d'aquests paràmetres no es desprenen de manera natural, tal com passa amb les disciplines criminalístiques de *matching.*

Un primer aspecte que hem de tenir en compte per a simplificar els mètodes de validació d'eines forenses digitals seria l'avaluació per separat de les diferents funcionalitats que ofereixen, i no intentar validar la totalitat d'una eina forense a causa de la gran complexitat que això comportaria.

2. Algunes disciplines forenses incorporen raons de versemblança (*likelihood ratios*) en l'expressió dels resultats dels informes pericials.

3. *Carving* és un terme en forense digital que designa el procés pel qual s'extreuen dades estructurades a partir de dades en brut *(raw data*), basant-se en característiques específiques del format presents a les dades estructurades. Per exemple: recuperació de fotografies esborrades a partir de les dades contingudes en els clústers no assignats.

Un altre aspecte que cal valorar és com abordar els *tipus d'errors* específics del forense digital. Els errors que ens trobem quan avaluem eines forenses digitals no són de la mateixa naturalesa que els errors de mesura d'aparells en altres disciplines científiques, en els quals sempre ens apareix un error sistemàtic i un component aleatori, mesurat en termes d'incertesa. Des del punt de vista de les funcionalitats d'aquestes eines, els principals tipus d'errors que ens podem trobar són els següents [9]:

- *Incompletesa*: es produeix quan tota la informació rellevant no ha estat adquirida o trobada per l'eina. Per exemple, una adquisició[4] podria ser incompleta o una cerca podria no identificar tots els elements existents.
- *Imprecisió*: es produeix quan l'eina no informa d'una manera precisa sobre les dades analitzades o sobre la seva adquisició. Aquests errors d'imprecisió poden ser ocasionats per *errors d'existència*, quan l'eina afegeix dades que no estaven presents en l'original, per exemple, duplicant el número dels correus enviats realment; *errors d'alteració*, quan l'eina canvia el significat de les dades, per exemple, intercanviant les dates d'entrades i sortides de correus electrònics; *errors d'associació*, quan l'eina agrupa elements no relacionats, per exemple, associant totes les cerques d'internet a un únic usuari de la màquina, quan realment existeixen més usuaris registrats al sistema fent ús d'internet, i *errors de corrupció*, que es produeixen quan l'eina forense detecta i compensa les dades que falten o estan corruptes amb dades que poden sorgir de diferents fonts, com ara sectors erronis trobats durant l'adquisició.
- *Mala interpretació*: es produeix quan els resultats s'han interpretat incorrectament. L'eina pot presentar la informació extreta o analitzada d'una manera ambigua i això fa que l'analista interpreti incorrectament els resultats obtinguts.

4.1.2. *Metodologia d'avaluació de funcionalitats de les eines forenses*

Per tal de poder validar les diferents funcionalitats de les eines forenses és important establir procediments i metodologies per a dur a terme les proves adients que ens permetin implementar les matrius de confusió. Per a dur a terme aquestes proves és necessari disposar de conjunts de dades (*data sets*) amb *dades de referència* inserides que, un cop processades pels diferents algorismes de les funcionalitats forenses, ens permetin verificar que s'han recuperat i interpretat satisfactòriament (figura 2). Per exemple, podem considerar una sèrie de fotografies conegudes com a dades de referència, fragmentar-les en un disc dur i analitzar el comportament d'una funció de recuperació de fitxers d'una o més eines forenses.

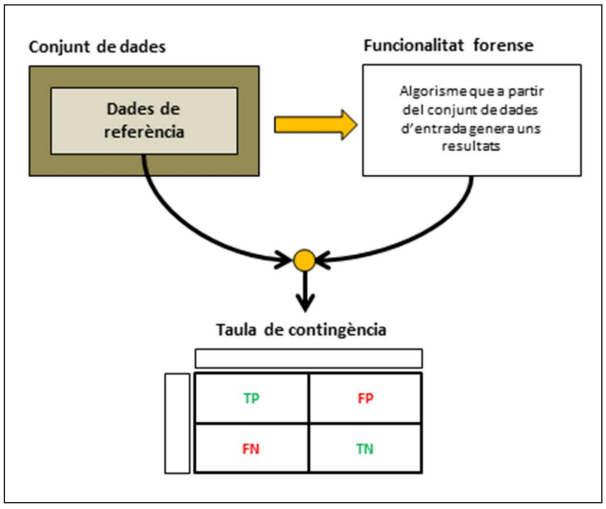

FIGURA 2. Metodologia per a la implementació de les matrius d'avaluació de les funcionalitats forenses a partir d'un conjunt de dades de referència i els resultats de l'aplicació d'un algorisme.

Les dades de referència són l'element clau que ens permetrà poder avaluar el resultat dels algorismes de les diferents funcionalitats que volem validar. Per tant, aquests conjunts han de ser adequats a la funcionalitat que es vol validar i han de poder reproduir situacions com més properes a la realitat millor. D'altra banda, hauran d'estar correctament etiquetats, indicant l'origen, les característiques tècniques de creació i les funcionalitats concretes que pretenem avaluar. A part, per a complir amb l'objectiu de validar una funcionalitat concreta, hi hauria d'haver una quantitat suficient de conjunts de dades per a cadascuna de les funcionalitats que cal validar i així poder garantir uns resultats de qualitat.

Per a simplificar els mètodes de validació, aquests conjunts de dades haurien de ser específics per a determinades funcionalitats concretes. Així, les dades de referència, segons la funcionalitat que es vol validar, podrien contenir imatges, missatges de text, consultes a internet, documents esborrats, etc., en definitiva, qualsevol element *atòmic* que volem avaluar d'una funcionalitat forense digital concreta, juntament amb les seves metadades, i informació addicional que sigui rellevant des d'un punt de vista forense.

Per exemple, si volem avaluar una funcionalitat d'extracció d'imatges en format JPG, a part d'inserir les imatges de control en el conjunt de dades, hauria de quedar documentada la localització dels sectors on s'emmagatzemen, o si han estat esborrades o no, en el cas de voler avaluar la seva possible recuperació total o parcial, etc.

Un dels problemes que apareixen en fer la comparació entre les dades de referència i la sortida dels resultats dels algorismes, tant en les eines comercials dels diferents desenvolupadors com en les eines de programari lliure, és que no existeix cap estàndard que en permeti

4. En informàtica forense s'entén per *adquisició* l'obtenció de la informació que potencialment conté les evidències digitals que volem analitzar (per exemple, un tipus d'adquisició d'evidències podria ser la clonació d'un disc dur).

l'automatització. Aquest fet fa que el procés de comparació, necessari per a crear les matrius de confusió, resulti molt problemàtic.

4.1.3. *Construcció de les matrius de confusió*

La definició de les matrius de confusió no és una qüestió senzilla. L'objectiu és la comparació d'unes dades de referència (DR) amb els resultats obtinguts per una eina forense, considerant una determinada funció forense, com per exemple, una funció de cerca de cadenes de caràcters i un determinat operador de comparació (figura 3). Notem que, en termes generals, no té sentit parlar de *True Negatives* (TN).

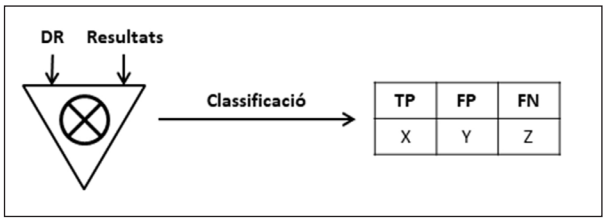

Figura 3. Construcció de les matrius de confusió emprant un determinat operador aplicat a dades de referència i resultats obtinguts de l'execució d'un algorisme.

Un dels problemes amb què ens podem trobar a l'hora de construir la matriu és que, segons l'operador de comparació que s'empri, el resultat pot ser molt diferent, i això pot dificultar la interpretació dels resultats i la comparació entre diferents eines forenses.

A l'exemple de la figura 4 podem veure quatre imatges que conformen les dades de referència (DR). Una vegada aquestes imatges s'han inserit en el conjunt de dades que cal examinar i s'ha executat l'eina forense, s'han recuperat quatre imatges (el quadrat blanc correspon a la imatge «Hello!», no recuperada per l'eina forense). Segons l'operador de comparació, veiem que es construeixen diferents matrius de confusió (com ja s'ha esmentat prèviament, notem que no té sentit parlar de TN):

- *Funció hash*: amb aquests tipus de funcions podem comprovar si la recuperació del fitxer ha estat completa. Només la imatge recuperada situada més a l'esquerra satisfà aquesta condició. El resultat és: 1 TP, 3 FP, corresponents a tres imatges incorrectament recuperades, i 1 FN, corresponent a la imatge «Hello!», no recuperada.
- *Magic numbers*: amb aquestes seqüències d'octets anomenades *magic numbers,* habitualment ubicades al principi dels arxius, els programaris informàtics poden reconèixer el tipus d'arxiu (per exemple, un format JPG). Per tant, si utilitzem com a operador de comparació aquestes seqüències, tots els fitxers recuperats poden conservar aquests octets, encara que la imatge sigui incompleta o contingui trossos d'altres imatges. El resultat és de 4 TP, encara que tres de les imatges siguin incorrectes.
- *Recuperació de més del 50 % del contingut:* si tenim en compte aquest criteri que, des del punt de vista forense, té molt sentit (una imatge, encara que només sigui parcial, pot ser molt rellevant en una investigació criminal), s'obtenen 2 TP, un dels quals correspon al fons blau i blanc.

4.2. *El concepte d'incertesa en forense digital*

Quan, per exemple, volem calibrar una balança, fem servir pesos de referència per al càlcul de l'error sistemàtic i de l'error aleatori, i obtenim diferents lectures del mateix pes. En el cas de la informàtica forense, aquest procés no es pot dur a terme: donat un conjunt de dades concret (*data set*), quan és processat per una eina forense, sempre obtenim el mateix resultat (el resultat és determinista) (figura 5), sempre que no hi hagi cap error de programació (*bug*).

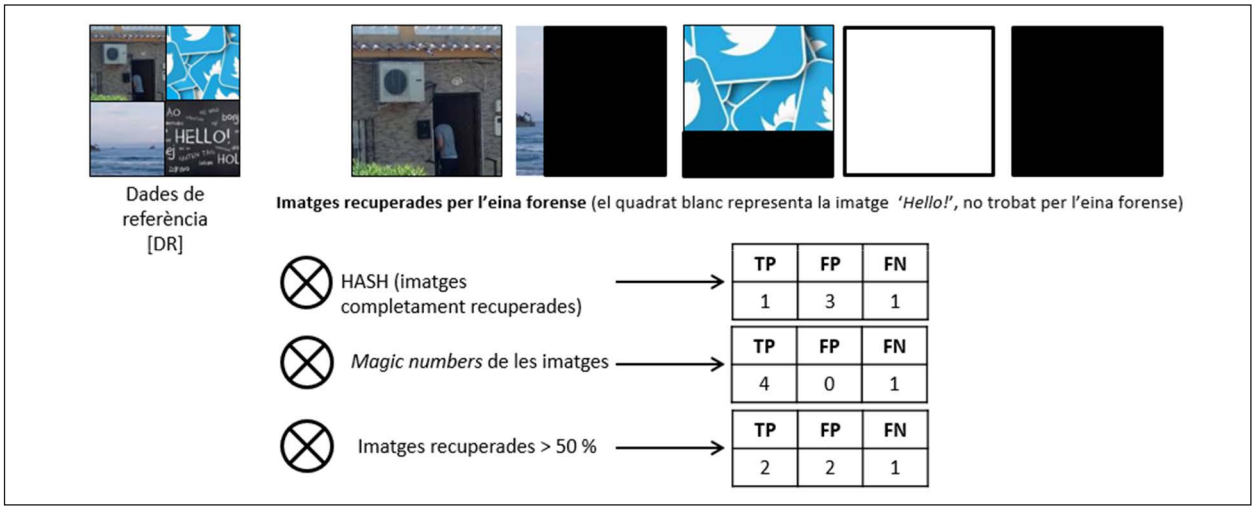

Figura 4. La variació en les matrius de confusió segons l'operador de comparació pot dificultar la interpretació del resultat i la comparació entre diferents eines forenses.

Tanmateix, donades unes dades de referència, aquestes es poden organitzar de manera imprevisible en cada conjunt de dades, i donar lloc a una certa variació en la sortida de l'eina, tal com podem veure en la figura 6.

Per tant, tot i que l'eina forense no té cap incertesa en si mateixa, la variabilitat observada té el seu origen (origen de la incertesa) en la forma en què les dades de referència s'emmagatzemen en els conjunts de dades i s'ex-

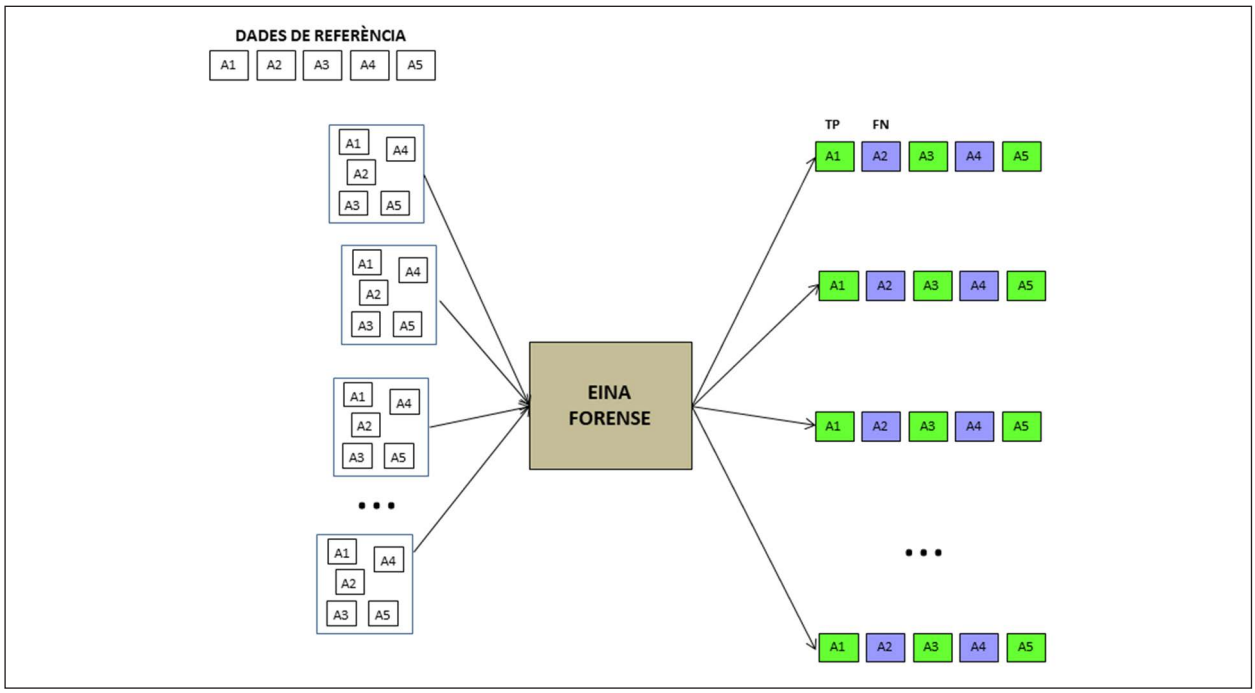

FIGURA 5. Donat un *data set* concret que és processat per una eina forense digital, el resultat obtingut és determinista.

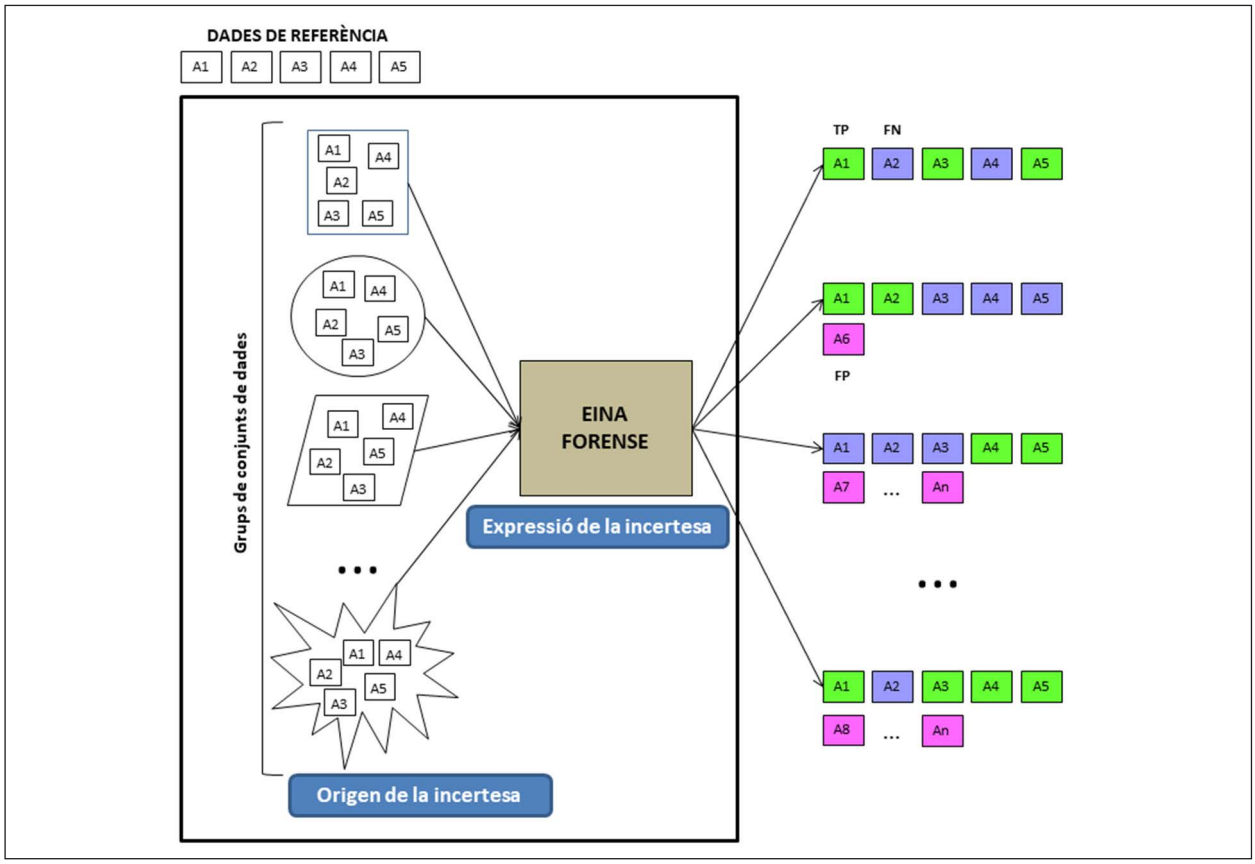

FIGURA 6. Organitzant les dades de referència en *data sets*, de manera imprevisible, es produeix una variabilitat que no té el seu origen en l'eina forense.

pressa en la sortida de l'eina forense (expressió de la incertesa).

Aquesta variació no es pot considerar una incertesa en el sentit habitual metrològic, però sí que és interessant poder-la enregistrar d'alguna manera. Tot i que la norma ISO/IEC 17025 no obliga a calcular la incertesa (ja que no sempre és possible), sí que és interessant, com a mínim, conèixer els components que la conformen.

Com a possible opció per a obtenir una mesura numèrica d'aquesta variació es podria emprar, per exemple, un vector ternari format per les taxes TP (*True Positive*), FP (*False Positive*) i FN (*False Negative*). Com és habitual en aquest tipus de mesures, és difícil preveure quin pot ser el comportament de l'eina davant d'altres conjunts de dades en el futur, però sí que ens permet, com a mínim, comparar diferents eines entre elles.

En definitiva, l'eina forense no és robusta en els valors d'entrada perquè és sensible a com s'organitzen els valors d'entrada formant un conjunt de dades particular. En aquest sentit, considerem que la mesura d'incertesa proposada pot ser un bon indicatiu de com és de bona una eina en relació amb el soroll introduït (sensibilitat). Tot i no ser una mesura d'incertesa en el sentit habitual, podríem entendre aquest càlcul com una indicació de la robustesa de l'eina, el qual recull un cert tipus d'incertesa quantificable, dependent de com s'organitzen les dades de referència en els conjunts de dades.

5. Conclusions

La crítica científica a les anomenades *ciències forenses* n'ha permès la millora, no només a efectes de metodologia, sinó també en termes de fiabilitat i explicació dels resultats obtinguts.

Europa no ha quedat al marge d'aquesta tendència i, principalment, a través de la Xarxa Europea de Laboratoris Forenses (ENFSI), ha promogut l'intercanvi de coneixement entre els diferents països i l'homogeneïtzació de procediments i expressió de resultats en informes pericials.

Un dels paraigües homogeneïtzadors dels laboratoris forenses és la norma ISO/IEC 17025, que si bé no és una norma específicament pensada per a les ciències forenses, és un element d'uniformització de consens que cal tenir en compte.

La informàtica forense (o forense digital) és una més de les disciplines forenses que s'intenten encabir en aquesta tendència. Les seves peculiaritats, però, fan que sigui difícil incorporar-la a l'empara de la norma ISO/IEC 17025, ja que la dimensió de la tasca de validar les metodologies (i les eines que porten incorporades) és pràcticament inabordable i sotmesa a canvis continus. No obstant això, la reflexió motivada per aquesta qüestió ha permès millorar les metodologies, caracteritzar les eines que s'utilitzen, i veure si el seu ús és adequat als objectius dels laboratoris.

Referències

[1] Arqués, J. M.; Colobrán, M.; Iparraguirre, J. *Com s'ha de fer l'informe pericial d'un delicte informàtic?* Barcelona: UOC, 2016. (Col·lecció H2PAC) ISBN 978-84-9116-583-5.

[2] Colobrán, M.; Arqués, J. M.; Guasch, A. *Anàlisi forense de sistemes d'informació*: *Investigació de l'evidència digital*. Mòdul 1. Barcelona: FUOC, 2009.

[3] Blanquez, M. *Validació d'eines d'anàlisi forense digital sota la norma ISO/IEC 17025*. Treball final del Màster Interuniversitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC) de la UOC-UAB-URV-UIB, 2019.

[4] «Junk Science at the F.B.I.». *The New York Times* [en línia] (27 abril 2015). <*https://www.nytimes.com/2015/04/27/opinion/junk-science-at-the-fbi.html*>.

[5] «Cas José Bretón». *Wikipedia* [en línia]. <*https://ca.wikipedia.org/wiki/Cas_Jos%C3%A9_Bret%C3%B3n*>.

[6] Unió Europea. «Council framework Decision 2009/905/JHA of 30 November 2009 on Accreditation of forensic service providers carrying out laboratory activities». *Official Journal of the European Union* [en línia], L 322/14 (9 desembre 2009). <*https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:322:0014:0016:EN:PDF*>.

[7] Secretaria General del Consell de la Unió Europea. *Draft Council Conclusions on the vision for European Forensic Science 2020 including the creation of a European Forensic Science Area and the development of forensic science infrastructure in Europe* [en línia], 12391/2/11 REV 2 ENFOPOL 229 COPEN 209, 2011. <*https://db.eurocrim.org/db/en/doc/1700.pdf*>.

[8] Secretaria General del Consell de la Unió Europea. *Conclusiones del Consejo y Plan de acción sobre el camino a seguir para la creación del Espacio Europeo de Policía Científica* [en línia], doc. 8770/16, 8819/16, 2016. <*https://data.consilium.europa.eu/doc/document/ST-10128-2016-INIT/es/pdf*>.

[9] Scientific Working Group on Digital Evidence (SWGDE). *Establishing Confidence in Digital Forensic Results by Error Mitigation Analysis* [en línia], 2017. <*https://www.swgde.org/documents/published-by-committee/quality-standards*>.