

# LA PRUEBA EN INFORMÁTICA: EVOLUCIÓN, ESTADO ACTUAL Y PROPUESTA DE FORMALIZACIÓN

JOAQUÍN ANGUAS BALSERA

Perito Ingeniero en Informática

## Resumen

Durante los más de 30 años de vida de la prueba en base a evidencias informáticas, no se ha consolidado un acercamiento fundamentado, compacto y estructurado a la epistemología de la prueba en informática.

Es de destacar cómo a pesar de esta falta de consistencia, nuestro ámbito jurídico ha generado una terminología y *status quo* normativo y *de facto* que son legado y consecuencia de la asimilación de conductas en ocasiones no asentadas y/o relativas a sistemas jurídicos que presentan diferencias sustanciales con el nuestro propio.

En esta ponencia presento una posible formalización de la prueba en informática de forma abstracta e independiente del contexto jurídico, que pretende ser un punto de partida para una sistematización del estudio de la misma.

## Particularidades de las evidencias informáticas

Esta sección presenta una serie de conceptos previos necesarios para la comprensión de los siguientes apartados.

Para que las evidencias informáticas puedan ser accesibles y por tanto susceptibles de ser tratadas, deben mostrar las siguientes características.

### Persistencia

La persistencia es la capacidad de mantener inalterado el estado de un sistema. No es posible el estudio de aquellos elementos que no pueden ser dotados de persistencia.

Las señales de luz que fluyen a través de un cable de fibra óptica, circunscritas al ámbito mismo del cable, no nos son accesibles. Son únicamente tratables en el contexto de un elemento de red que sí permita la persistencia, por ejemplo un dispositivo enrutador o conmutador de red.

Los elementos que permiten la persistencia están dotados de un medio de almacenamiento que mantiene inalterados los valores que contienen bien de forma autónoma o bien con el auxilio de elementos externos que permiten la copia de dichos valores a medios de almacenamiento persistente.

### Coherencia

Las evidencias informáticas no se encuentran nunca aisladas sino que existen siempre en un contexto. Dicho contexto constituye una red de coherencia que permite el contraste de dichas evidencias.

Siguiendo con el ejemplo anterior, la marca, modelo y configuración del dispositivo de red, su relación con otros dispositivos de red, etc, constituyen el contexto en el que existen las evidencias que puedan adquirirse del mismo.

El ámbito de coherencia depende del nivel al que se esté estudiando el sistema. Una persona con conocimientos profundos del sistema objeto de estudio tendrá a su disposición un entorno de coherencia mucho más amplio que alguien con un conocimiento superficial del mismo.

### **Intangibilidad y ausencia de significado propio**

Aquellos elementos que nos son accesibles se encuentran almacenados en los dispositivos que los dotan de persistencia en forma de campos magnéticos en la superficie de un disco o como electrones en una celda de memoria, por poner dos ejemplos comunes.

Estas formas de almacenamiento no permiten la percepción directa de las evidencias, siendo siempre necesaria la intervención de diferentes medios que traducen dichas evidencias a símbolos que sí podemos percibir.

Por otro lado, las evidencias informáticas carecen por completo de sentido propio, siendo únicamente interpretables en el contexto del sistema en el que residen.

### **Manipulación y copia**

Las evidencias en base informática son susceptibles de ser manipuladas y copiadas de forma exacta e indistinguible del original, siempre que se respete la coherencia del sistema.

Como ya se ha apuntado en un punto anterior el ámbito de coherencia depende de los conocimientos del sistema o el acceso al mismo que pueda tener aquel que lo estudia.

Así, para intervenir en una evidencia y modificarla de forma que sea indistinguible del estado original del sistema, es necesario modificar todo el ámbito de coherencia al que puede tener acceso quien estudie la evidencia.

### **Previo**

En esta sección explicita el objetivo de la ponencia, su alcance y su objeto.

### **Objetivo**

El objetivo de esta ponencia es proponer una formalización de la prueba en informática desde el punto de vista epistemológico que permita establecer un punto de partida para la sistematización de su estudio técnico-legal.

### **Objeto: la prueba informática**

En el contexto de la presente ponencia se considera prueba en informática la acción o efecto de introducir hechos en un litigio en base a evidencias informáticas.

### **Alcance**

En el contexto de esta ponencia me referiré a la prueba en informática dentro de nuestro contexto jurídico propio actual.

Las referencias a actividades o sistemas ajenos al nuestro se incluyen únicamente para mostrar su influencia en nuestro propio contexto o para contextualizar y enriquecer la práctica y uso de la prueba en informática.

### **Contexto histórico y evolución**

La presente sección repasa la evolución histórica de la prueba en informática.

Debe subrayarse que en esta sección se recoge principalmente la evolución de la prueba y las diferentes disciplinas asociadas a los procesos penales, ya que aunque es seguro que en la época en la que se desarrolló la prueba en informática existían conflictos civiles en los que la informática era objeto o medio de prueba, no es fácil encontrar referencias significativas al respecto.

Las frecuentes referencias al ámbito estadounidense se justifica por su carácter pionero en los avances que se producen.

#### ***Evolución histórica***

A finales de los años setenta y principios de los ochenta vio la luz una actividad que requeriría un replanteamiento de diferentes conceptos jurídicos.

Con la desafortunada publicación de la referencia del sistema de control por tonos de sus centralitas de teléfonos por parte de la compañía Bell, se abriría la puerta al uso fraudulento de las mismas por parte de diferentes tipologías de individuos en su mayoría curiosos por conocer los entresijos de los complicados sistemas que soportaban las comunicaciones telefónicas<sup>1</sup>.

Contemporáneos con la popularización de los sistemas computadores, ambos ámbitos entraron en contacto y se nutrieron de una misma curiosidad y afán de conocimiento.<sup>2</sup>

Las empresas de telecomunicaciones no podían permitir la intrusión de terceros en sus infraestructuras ni los estados consentir la intervención incontrolada en elementos críticos de los servicios de telecomunicación, viéndose ambos impelidos a perseguir estas actividades.<sup>3</sup>

Por otro lado, la generalización de los sistemas de computadores se infiltra en primer lugar en los departamentos financieros de las empresas, por lo que se convierte también en objeto de estudio para las organizaciones de persecución del fraude de los diferentes gobiernos, promulgándose en Estados Unidos la *Computer fraud and abuse Law* en 1986.<sup>4</sup>

Se inicia en esta época el seguimiento de estas y otras conductas anómalas asociadas al uso de la informática, naciendo unidades especializadas de las fuerzas de seguridad y la inteligencia nacional para estudiar y contrarrestar este tipo de acciones.<sup>5</sup>

---

<sup>1</sup> Véase <http://es.wikipedia.org/wiki/Bluebox> y DAVID PRICE, *Blind Whistling Phreaks and the FBI's Historical Reliance on Phone Tap Criminality CounterPunch*, June 30, 2008

<sup>2</sup> Véase COLIN COVERT, *High-Tech Hijinks Seven Curious Teenagers Wreak Havoc Via Computer*, en Detroit Free Press, 28 de Agosto de 1983, p.1F.

<sup>3</sup> Véase <http://www.washingtonpost.com/wp-dyn/articles/A50606-2002Jun26.html>

<sup>4</sup> Véase <http://www.law.cornell.edu/uscode/18/1030.html>

<sup>5</sup> Véase <http://www.fbi.gov/libref/historic/history/rise.htm>

Con la aparición de los ordenadores personales aparecen nuevas fuentes de riesgo como los virus de ordenador, aunque durante un tiempo y debido a lo limitado de las conexiones de red, sus efectos se mantendrán acotados, concretándose su impacto en la reducción del rendimiento de los sistemas o la modificación o borrado de información local.

Durante años las redes de ordenadores se mantuvieron asociadas a entidades gubernamentales, de defensa y/o inteligencia y universidades, pero poco a poco se fueron popularizando formas de conexión de ordenadores, primero basadas en la propia red telefónica y después en redes dedicadas a la transmisión de datos.

En los años 90 las redes que anteriormente tenían un uso reservado empiezan a hacerse más comunes: la “navegación” web, el correo electrónico y los protocolos de noticias se hacen cada vez más accesibles y presentes.

El impacto de las intrusiones y los virus de ordenador y sus variantes (actualmente llamados *malware*) son cada vez más notorios y diferentes organizaciones gubernamentales comienzan a preocuparse por la seguridad de las redes y ordenadores, considerándose pronto un asunto de seguridad nacional.

Durante estos últimos años el uso de la informática ha ido impregnando cada vez más parcelas de la actividad tanto privada como empresarial o pública, de manera que ahora es difícil imaginar algunas actividades sin el soporte de la informática.

En nuestro país, se crean a mediados de los años 90 unidades dedicadas a la persecución de delitos cometidos en o a través de Internet: en 1997 se crea el Grupo de Delitos Telemáticos, dentro de la Unidad Central Operativa de la Guardia Civil tras una primera investigación en el año anterior, principalmente orientada en origen a la investigación de intrusiones y accesos ilegales o no autorizados. Pasa a llamarse Departamento de Delitos de Alta Tecnología en 1999 por la influencia internacional de las unidades de *High Tech Crime* y posteriormente Departamento de Delitos Telemáticos, para finalmente adquirir su nombre actual de Grupo de Delitos Telemáticos en 2003.<sup>6</sup>

Anteriormente, en 1995 se crea en el seno del Cuerpo Nacional de Policía la Brigada de Investigación Tecnológica (BIT).<sup>7</sup>

Siempre en el marco de la persecución de delitos asociados a la informática, las diferentes unidades de los cuerpos de seguridad desarrollan su actividad y se coordinan de forma más o menos formal, estableciendo guías de buenas prácticas que nacen de su experiencia al trasladar las evidencias recogidas en sus investigaciones a las causas penales que las requieren.

Son de destacar las publicadas por la ACPO<sup>8</sup> (Asociación de Jefes de Oficiales Jefe de Policía de Reino Unido) en Europa y US-CERT<sup>9</sup> en Estados Unidos.

---

<sup>6</sup> Véase [http://es.wikipedia.org/wiki/Grupo\\_de\\_Delitos\\_Telematicos](http://es.wikipedia.org/wiki/Grupo_de_Delitos_Telematicos)

<sup>7</sup> Véase [http://es.wikipedia.org/wiki/Brigada\\_de\\_Investigacion\\_Tecnologica\\_\(España\)](http://es.wikipedia.org/wiki/Brigada_de_Investigacion_Tecnologica_(España))

<sup>8</sup> Véase [http://www.7safe.com/electronic\\_evidence/ACPO\\_guidelines\\_computer\\_evidence.pdf](http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf)

En todo caso hay que insistir en que dichas guías se centran en la práctica de la llamada *informática forense*, pero en ningún caso se aborda la prueba en informática como un elemento indiciario en general ni de forma independiente de la vía -civil o penal- a la que se asocia.

Lo que sí es cierto es que el establecimiento de buenas prácticas y la mayor abundancia de actividad de los cuerpos de seguridad, locales y especialmente federales, de Estados Unidos tienen una notable influencia en la configuración e incluso en la terminología que se acaba empleando en Europa en general y en nuestro ámbito jurídico en particular.

Es especialmente relevante en nuestro caso que se presente la *informática forense* como una disciplina, cuando se trata de un conjunto de técnicas y métodos de preservación y análisis de evidencias informáticas, subconjunto de la actividad pericial en informática.

## **Estado actual**

### **La prueba científico-técnica**

De forma previa, vale la pena destacar que en general se da una dicotomía que no deja de sorprender a primera vista: mientras que la necesidad de la prueba es simétrica en los casos civiles y penales, no es ni mucho menos así su estudio desde el punto de vista científico-técnico.

Por un lado se encuentran las llamadas *ciencias o ingenierías forenses*, que estudian y se preocupan principalmente de la prueba en la jurisdicción penal, mientras que la prueba civil se encuentra de facto huérfana de disciplina y de actores que la estudien y evolucionen.

De hecho en nuestro ámbito jurídico, ni siquiera para la jurisdicción penal se da una estructura mínimamente cohesionada de entidades que trabajen sobre la prueba científico-técnica, reduciéndose el *status quo* de la misma a algunas unidades de las fuerzas y cuerpos de seguridad y algunos departamentos universitarios para algunas disciplinas concretas.<sup>10</sup>

### **El escenario que dibuja el informe de la NAS**

A falta de dicha estructura resulta revelador un estudio como reflejo del estado de la prueba técnico-científica a nivel mundial, en la medida que puede ser extrapolable.

En el año 2005 el Congreso de los Estados Unidos requiere a la *National Academy of Sciences* para que cree un comité que estudie el estado de las diferentes disciplinas asociadas a la prueba científico-técnica.

---

<sup>9</sup> Véase [http://www.us-cert.gov/reading\\_room/forensics.pdf](http://www.us-cert.gov/reading_room/forensics.pdf)

<sup>10</sup> Véase [http://es.wikipedia.org/wiki/Policia\\_cientifica](http://es.wikipedia.org/wiki/Policia_cientifica)

El resultado es un informe titulado *Strengthening Forensic Science in the United States: A Path Forward*<sup>11</sup> presentado en 2009 y que arroja un resultado que merece tenerse en cuenta.

El informe se centra en la prueba criminal y resulta muy crítico, llegando a afirmar que se trata de:

“...un sistema plagado por la escasez de buena investigación, fragmentación, prácticas inconsistentes y gobierno débil...”

“...interpretaciones subjetivas y testimonios exagerados...”

El informe ha producido un intenso debate y múltiples reacciones al respecto.

### **Confusión en la nomenclatura**

En nuestro ámbito jurídico se han introducido con poca fortuna conceptos que provienen de culturas jurídicas diferentes.

En general tanto la legislación como la práctica habitual es referirse a la prueba en base a elementos informáticos como “prueba electrónica”.

En mi opinión el término es poco afortunado, siendo más adecuado “prueba informática”.

La informática es una disciplina que maneja conceptos con un alto nivel de abstracción. El vocabulario casi hermético y la actitud, cultivada e intencionada en muchos casos, exclusiva y excluyente de algunos practicantes tampoco han contribuido a facilitar el acceso y la comprensión de la actividad por los demás actores en el proceso judicial.

Además, cuando actores externos a la disciplina han tenido que nombrar o referirse a conceptos que les son más o menos ajenos no han sido acompañados por la fortuna, dejándose llevar en general por conceptos propios de otras culturas jurídicas más precoces en la práctica de la prueba informática.

Son conceptos relacionados con la prueba informática: “informática forense”, “prueba electrónica” y “evidencia digital”. Una búsqueda de términos relacionados en el buscador Google arroja unos resultados que aunque carecen de valor científico alguno, pueden resultar interesantes.

Así el término más popular es el primero, “informática forense” con 56.100 resultados, seguido por “prueba electrónica” con 54.600 y “evidencia digital” con 30.800. El término “peritaje en informática” devuelve 149 resultados.

Que existe un problema de nomenclatura no debería escapársele a nadie que se vea expuesto al extenso, variado y en ocasiones incoherente vocabulario relacionado con la actividad. Se habla de “evidencias digitales”, “evidencias electrónicas”, “delitos informáticos”, “prueba electrónica”, “delitos telemáticos”, etc.

---

<sup>11</sup> COMMITTEE ON IDENTIFYING THE NEEDS OF THE FORENSIC SCIENCES COMMUNITY; COMMITTEE ON APPLIED AND THEORETICAL STATISTICS, *Strengthening Forensic Science in the United States: A Path Forward*, National Research Council, 2009.

Teniendo en cuenta que existen tecnologías emergentes que no se basan en la electrónica, al menos en cuanto al cómputo o el almacenamiento de la información y que términos como “electrónica” o “digital” no coinciden con la disciplina que trata esos elementos, que sería la informática, quizás sería conveniente unificar y simplificar vocabulario alrededor de este último término: informática<sup>12</sup>.

### **Mezcla de disciplinas**

Diferentes disciplinas se interesan en extraer hechos de evidencias informáticas.

Podrían dividirse en dos enfoques: aquellas que se centran en probar (probáticas) y aquellas que se enfocan en conocer (investigativas). La diferencia radica básicamente en el punto de vista que se toma respecto al tratamiento de las evidencias.

Cuando se pretende probar deben extremarse las precauciones en la captura y el tratamiento de las evidencias para evitar cualquier posible contaminación, así como documentar cada acción realizada sobre la misma con objeto de garantizar la reproducibilidad de lo observado, minimizando la posibilidad de repudio de la misma.

En cambio, cuando únicamente se pretende conocer, el concepto de repudio pierde su influencia, dichas precauciones se relajan y los flujos de trabajo se vuelven más directos.

Otro nivel de diferencia entre los enfoques probático e investigativo radica en el contexto. Mientras que en el investigativo una buena parte del contexto en el que se encuentra la prueba es conocido y explícito, el probático requiere conocimientos y capacidades más allá de la simple técnica de tratamiento de la prueba, al ser imprescindible añadir y hacer explícito dicho contexto, por ser el destinatario del mismo, el juzgador, completamente ajeno al mismo.

La seguridad informática es una disciplina que se centra en el estudio de los sistemas informáticos enfocada maximizar su disponibilidad, integridad e inviolabilidad. Los expertos en seguridad informática realizan actividades investigativas orientadas a conocer el estado de los sistemas y trazar hasta su origen cualquier eventualidad o intrusión.

Pero en ocasiones dichas actividades investigativas pudieran devenir actividades probatorias cuando lo que se descubre es una actividad delictiva o ilícita.

No es recomendable que el profesional de la seguridad informática se involucre en la actividad orientada a probar los hechos objeto de investigación. En primer lugar por estar contaminado de necesidad por su posición en la organización. Y en segundo lugar por carecer a priori de los conocimientos que le van a permitir introducir los hechos en el conflicto de forma efectiva y sólida.

---

<sup>12</sup> De hecho notables juristas como Michele Taruffo se refieren a la prueba electrónica como prueba informática (MICHELE TARUFFO, *La prueba*, Ed. Marcial Pons 2008, p. 85).

Del mismo modo la auditoría en informática, siendo una disciplina que se centra en la gestión del riesgo en sistemas de información, presenta esa misma vertiente investigativa.

Pero por el contrario, en el caso de la auditoría, si el auditor es externo a la organización, aunque le faltaría un componente de conocimiento del proceso, puede perfectamente hacer valer su independencia y actuar como garante de la prueba, siempre naturalmente aplicando las prácticas recomendadas a tal efecto.

No es el caso de la investigación privada en base a evidencias informáticas, que tiene una componente únicamente investigativa.

El perfil de estos profesionales suele incluir una sólida base en técnicas de investigación, que junto al conocimiento de las técnicas de informática forense les va a permitir extraer hechos simples de dichas evidencias. Su falta de formación en sistemas de información les impide a priori extraer hechos de cierta complejidad y añadir el debido contexto a los mismos.

Por último el peritaje en informática tendría una visión eminentemente probática de los indicios y no se quedaría en hechos simples sino que estaría en disposición de extraer hechos complejos y de alto nivel de las evidencias observadas, incluso cuando estos hechos de alto nivel requieren de una capacitación para su interpretación o valoración. El perfil del perito debe incluir conocimientos de los sistemas de información sobre los que tenga que actuar, las técnicas de informática forense y siendo el objeto de su trabajo la introducción de hechos en un litigio, un mínimo conocimiento de las reglas que operan en el procedimiento a este respecto.

Cabe reseñar que el perito en informática interviene siempre que es necesaria la opinión de un experto en informática en un litigio, por lo que su actividad no se limita a la captación, interpretación y presentación de indicios, bien sea en conflictos con objeto tecnológico u otros.

Como experto está en disposición de opinar y valorar elementos y circunstancias como por ejemplo el grado de cumplimiento de una obra o servicio informático.

### **Figuras ajenas al sistema jurídico**

La llamada *informática forense* no tiene una correspondencia en nuestro marco jurídico.

En general las referencias a la informática forense la describen como un conjunto de técnicas que se enfocan a la adquisición, preservación y presentación de la prueba informática. Son así las mejores prácticas para la adquisición y tratamiento de evidencias informáticas y son transversales a las demás disciplinas que tratan la prueba informática. El concepto más importante para la informática forense es el “no repudio”.

Su origen está en los Estados Unidos, y se encuentra asociada al literal de la regla 702 de las *Federal Rules of Evidence*<sup>13</sup>:

“Rule 702. Testimony by Experts

If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case.”

En concreto se identificaría con aquellos principios y métodos del numeral (3) de la misma.

Debe tenerse en cuenta que la figura del *expert witness* en la jurisdicción estadounidense es diferente a la del perito de nuestro marco jurídico.

### **Estado general de la prueba en informática**

Existe actualmente cierta confusión al respecto de la naturaleza y uso en el proceso de la prueba en informática.

Sin entrar en aspectos jurídicos que me son ajenos, mi experiencia es que dicha confusión viene provocada a menudo por la apariencia documental que presentan algún tipo de evidencias informáticas.

El diferente tratamiento y consideración de la prueba documental y la prueba pericial provocan que se busque en ocasiones evitar el perito, a veces sin tener en cuenta factores en los que me extenderé más adelante y que imponen dicha figura se quiera o no.

A modo de ejemplo de lo anterior, la introducción de comunicaciones por correo electrónico en un litigio es una práctica que no acaba de delimitarse con claridad. Como comentaré posteriormente, sí se puede hacer accesible al juzgador el contenido de la comunicación y el mismo puede realizar un juicio de pertinencia de la misma en el contexto del litigio, no sería en principio necesaria la intervención de un perito.

Hay quien se queja de que en este escenario es anacrónica la introducción de las comunicaciones impresas en lugar de en su formato original informático. En mi opinión dicha fórmula no representa un problema en sí misma.

Una vez aceptada la comunicación por el juzgador, la parte contraria puede impugnar su validez o veracidad.

Si los elementos en los que se basa la impugnación son, de nuevo, accesibles al juzgador, no será necesaria la intervención de un perito. Por ejemplo si alega que él no pudo escribir dicha comunicación por encontrarse aislado en una isla desierta de vacaciones.

---

<sup>13</sup> Véase <http://www.law.cornell.edu/rules/fre/rules.htm#Rule702>

Si por el contrario los elementos en los que se basa la impugnación tienen base en informática y no son de común conocimiento, sí será necesaria la intervención de un perito que los valore y ponga sus conclusiones en forma que pueda ser relevante a lo alegado por las partes.

Existe por otro lado legislación adicional a la meramente procesal que en ocasiones causa también confusión.

Me referiré en concreto a la Ley 59/2003, de 19 de diciembre, de firma electrónica. En dicha ley se delimita y regula el uso de la llamada firma electrónica.<sup>14</sup>

Genera especial confusión su disposición adicional décima, en la que se dice lo siguiente:

*“DISPOSICIÓN ADICIONAL DÉCIMA. Modificación de la Ley de Enjuiciamiento Civil.*

*Se añade un apartado tres al artículo 326 de la Ley de Enjuiciamiento Civil con el siguiente tenor:*

*Cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá con arreglo a lo establecido en el artículo 3 de la Ley de Firma Electrónica.”*

El artículo 326 queda así con el siguiente redactado:

*“Artículo 326. Fuerza probatoria de los documentos privados.*

*1. Los documentos privados harán prueba plena en el proceso, en los términos del artículo 319, cuando su autenticidad no sea impugnada por la parte a quien perjudiquen.*

*2. Cuando se impugne la autenticidad de un documento privado, el que lo haya presentado podrá pedir el cotejo pericial de letras o proponer cualquier otro medio de prueba que resulte útil y pertinente al efecto.*

*Si del cotejo o de otro medio de prueba se desprendiere la autenticidad del documento, se procederá conforme a lo previsto en el apartado tercero del artículo 320. Cuando no se pudiere deducir su autenticidad o no se hubiere propuesto prueba alguna, el tribunal lo valorará conforme a las reglas de la sana crítica.*

*3. Añadido por Ley 59/2003, de 19 de diciembre. Cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá con arreglo a lo establecido en el artículo 3 de la Ley de Firma Electrónica.”*

---

<sup>14</sup> Si consideramos que la firma hológrafa sometida al escrutinio de un técnico grafólogo permite el no repudio, no sería correcto realizar la correspondencia firma hológrafa – firma digital. La firma digital precisa del uso de un contenedor criptográfico que contiene la clave asociada a la firma y que suele precisar de una contraseña secreta para su acceso. Si yo transmito algo que yo tengo (clave) y algo que yo sé (contraseña) a otra persona, dicha persona podrá actuar en mi nombre de forma arbitraria, cosa que es impensable con la firma hológrafa. La correspondencia sería quizás más correcta al concepto de sello digital.

La confusión que se genera es la siguiente:

Persiguiendo la máxima fuerza probatoria, es común que se pretenda que ficheros informáticos firmados digitalmente accedan a la consideración de prueba plena.

Si el contenido de dichos ficheros es accesible al juzgador efectivamente puede ser así.

Pero en el caso de que el contenido de los ficheros que se pretende introducir en el litigio no sea accesible al juzgador no es posible que dichos ficheros accedan al mismo como documentos, siendo necesaria la intervención de un perito, ya que el juzgador será incapaz siquiera de establecer un juicio de pertinencia al respecto.

### **Estudio epistemológico**

Con objeto de construir un marco de referencia sólido, unificado e independiente del entorno jurídico, presento un planteamiento basado en la semiótica, en el estudio de los signos asociados a los indicios informáticos.

### **Enfoque semiótico**

La semiótica se define como la ciencia de los símbolos. Como se ha avanzado anteriormente, la informática se basa en asociar un significado a diferentes señales eléctricas o magnéticas contenidas en diferentes dispositivos. Como también se ha comentado, el significado de dichas señales debe ser debidamente asociado al contexto en el que se encuentra.

### **Construcción de significados**

La construcción de significado de los símbolos que representan las diferentes señales que se preservan en los dispositivos viene condicionado por el contexto en el que se encuentran, pudiéndose atacar la construcción de un significado comprensible por una persona como un proceso en diferentes (a veces muchos) pasos. En cada paso se elevaría el nivel semántico de los símbolos asociándolos cada vez con una cantidad mayor de contexto.

### **Cotas semánticas**

En diferentes puntos de la cadena de construcción de significados podrían establecerse niveles o cotas de especial importancia.

El nivel o cota semántica que resulta más relevante es el del propio juzgador, asociado al conocimiento que resulta común. La relevancia de este nivel viene dada por su capacidad para delimitar aquello que puede acceder al proceso. Por debajo de dicho nivel no debería acceder ninguna prueba al proceso, ya que el juzgador no podrá siquiera realizar el debido juicio de pertinencia.

Es también importante la cota a la que accede el perito o experto. Como se ha comentado, prácticamente nadie accede a las evidencias al nivel del campo magnético en la superficie del disco, por lo que hay niveles por debajo del nivel que observa el perito. Dichos niveles quedarán sin contraste y se obvian en base a la confianza más o menos general de que son irrelevantes o que no aportan elementos que puedan ser significativos al proceso.

### **La prueba pericial científico-técnica**

Cuando se precisa elevar el nivel semántico de los indicios que se pretende utilizar para probar los hechos de interés en un litigio, nuestro ordenamiento legal ofrece la figura de la prueba pericial.

Aunque comparten métodos y filosofía, la ciencia no es peritaje y el peritaje no es ciencia.

Mientras que la ciencia pretende establecer teorías generales a partir de diferentes casos particulares utilizando métodos de investigación, la revisión por pares, etc, el peritaje está más asociado a la historiografía: a la reproducción de un estado o a la reconstrucción de unos hechos ocurridos en el pasado. La ciencia pretende construir conocimiento y el peritaje únicamente probar.

La ciencia trabaja en entornos controlados, mientras que en el peritaje el entorno nos viene dado.

Mientras que en la ciencia la experimentación se alinea con corrientes teóricas y hay un cierto nivel de estandarización, en el peritaje los casos suelen ser únicos.

En el peritaje influye además un factor extracientífico: la ley procesal aplicable.

En el peritaje en informática los *saltos semánticos* son muchos y en muchos casos implícitos.

### **Universo de Prueba**

Cualquier intento de establecer un marco de trabajo para la prueba en informática lo suficientemente general debe tener en cuenta el entorno en el que opera.

Aunque ante unas mismas evidencias informáticas dos expertos del mismo nivel de conocimiento de dos jurisdicciones diferentes puedan derivar hechos similares, en general, teniendo en cuenta las limitaciones que puede imponer la ley procesal correspondiente a cada caso, dichos hechos pueden llegar a diferir notablemente.

Defino un *universo de prueba* como un conjunto compuesta por:

- Un conjunto de reglas procedurales dentro de un ámbito jurídico.
- Un conjunto de evidencias de las que derivar un significado y su contexto relacionado.
- Un conjunto de reglas de derivación que permiten derivar significado de evidencias o de otras derivaciones.
- Un conjunto de niveles semánticos. Son especialmente relevantes aquellos que producen una diferencia en aquello que prescriben las reglas procedurales o en la posible interpretación de las evidencias.
- Un conjunto de elementos relativos a máximas de experiencia o praxis que permiten dotar al significado de un contexto dentro del propio caso en el que se pretende introducir la prueba.

El conjunto de reglas procedurales determina qué, cómo y cuándo puede acceder al proceso.

Las evidencias deben estar fijadas en cualquier forma de sustrato que permita la persistencia y se acompañan del contexto en el que se encuentran.

Las reglas de derivación deben dar soporte a las diferentes formas de derivación lógica como la deducción, la inducción, la inferencia, etc. Es de señalar que dadas las características de maleabilidad de las evidencias informáticas habitualmente se hacen afirmaciones en base a juicios de plausibilidad.

Los niveles semánticos más relevantes son aquellos referidos a la capacidad del juzgador de establecer un juicio de pertinencia sobre la prueba que se pretende presentar y el que establece la capacidad del posible experto que pueda verse expuesto a las evidencias asociadas.

Las máximas de experiencia permiten poner las derivaciones procedentes de las evidencias en el contexto del caso que requiere la prueba.

El universo de prueba determina qué está accesible a la prueba dentro de un litigio.

### **El papel del perito en informática**

Como se ha indicado anteriormente, en ocasiones puede ser necesaria la intervención de un experto en la materia objeto de prueba. Esta figura se concreta en nuestro ámbito jurídico en el perito, al que las normas procedimentales suelen referirse como alguien con conocimientos en la materia objeto de prueba.

Dicha experiencia es la que permite al perito modificar el nivel semántico de las evidencias objeto de su estudio para adecuarlo al nivel semántico accesible al juzgador, de forma que pueda realizar, si es necesario, un juicio de pertinencia de la misma previo a su introducción en el litigio y evaluar las consecuencias que se derivan de los hechos asociados a las mismas en la justificación de su decisión final.

### **El papel del juzgador**

Aunque en general las jurisdicciones civiles suelen derivar la responsabilidad al respecto de la calidad de la prueba a las partes, en el proceso penal las jurisdicciones suelen dar al juzgador un papel más o menos explícito de *guardián* de la prueba.

Como la ciencia, la valoración de la prueba viene a normalmente a basarse en conceptos como la reproducibilidad y la falsabilidad: aquellos elementos que permitan el debido contraste de la misma.

### **Propuesta de definición de la prueba en informática**

La prueba en informática sería el acto o efecto de la introducción de hechos en un litigio en base a evidencias informáticas.

Las evidencias se introducen en el litigio dentro del marco de un universo de prueba, compuesto por:

- Un conjunto de reglas procedurales.
- Un conjunto de evidencias.
- Un conjunto de reglas de derivación.
- Un conjunto de niveles semánticos.
- Un conjunto de elementos relativos a la praxis en el contexto del caso.

Las evidencias en informática en las que se basa la prueba tienen asociado un nivel semántico que las hace susceptibles de ser comprendidas y contrastadas por diferentes actores en el litigio.

En caso de que dichas evidencias puedan ser comprendidas por alguien sin conocimientos especializados y sus circunstancias no se discutan o también sean comúnmente accesibles, no será necesaria la intervención de un experto para que puedan acceder al proceso, comportándose como un documento.

En caso contrario será necesaria la intervención de un experto, que pondrá las evidencias en su debido contexto, adecuará su nivel semántico y derivará aquellos hechos que sean relevantes para el litigio.

La cadena de derivaciones empleada por el posible experto deberá ser explícita y deberá detallar aquellos elementos relevantes que permitan el debido contraste de los mismos.

Los niveles semánticos por debajo de los considerados por los posibles peritos o expertos, quedan fuera de toda posibilidad de contraste.

## **Conclusiones**

Durante los más de 30 años de vida de la prueba en base a evidencias informáticas, no se ha consolidado un acercamiento fundamentado, compacto y estructurado a la epistemología de la prueba en informática.

En esta ponencia se propone una estandarización de la terminología utilizada alrededor del término “informática” que ayude a mitigar la confusión terminológica y ofrece una formalización que debería ser válida para diferentes entornos jurídicos y que pretende ser un punto de partida para una sistematización del estudio de la prueba en informática.

En concreto se describe la *evolución y estado actual* de la prueba en informática, se realiza un *estudio epistemológico* de la misma en el que se describe un *acercamiento semiótico* a la misma, se introducen un conjunto de *niveles o cotas semánticas*, se define un entorno *universo de prueba*, se incide en el papel del juzgador y el posible perito y por último se propone una definición de prueba informática compacta e independiente del sistema jurídico.