>> Jorge Dávila

Evidencias, identidades y pruebas... ¿electrónicas?

Todos los indicios indican que algo se mueve en el páramo de la prueba y evidencia digital. Quizás ahora se ponga en marcha el desarrollo de soluciones que permitan poder saber qué ha ocurrido y quién ha hecho qué en un sistema de información. Esto pasa por replantear la Identidad Digital, por aquilatar los sistemas de monitorización y registro, y por incluir en este esfuerzo, y en su justa medida, a los colectivos profesionales que conforman el mundo de la administración de justicia y vinculados.

El pasado mes de marzo asistí a una interesante jornada, organizada por esta misma revista[1], que estuvo consagrada al atractivo tema de las denominadas "*evidencias digitales*". El aforo se completó varias semanas antes de su celebración y eso pone de manifiesto el interés que ha despertado este tema en los profesionales de la seguridad informática y en los de la administración de justicia. La asistencia fue mayoritaria del lado de la tecnología, pero la minoría de abogados se hizo notar claramente e hizo aportaciones muy interesantes que ponen de manifiesto el inexorablemente acercarse del día en el que ellos tendrán que incluir la irrealidad virtual en sus quehaceres profesionales.

En esas jornadas se reunieron algunos representantes de los que reparten aquello que se entiende por justicia dentro de nuestro ordenamiento constitucional, y los que venden soluciones tecnológicas para la gestión de "*logs*"[2]. Los primeros mencionaban la necesidad de afrontar el problema que supone probar algo en el mundo digital, y los segundos proponían sus productos y soluciones como respuesta suficiente para ello. Sin embargo, ambas comunidades hablaban lenguajes bien diferentes, y apenas se atisbó el problema.

El *data logging* es la arcana actividad de registrar secuencialmente datos que se van observando, y el ordenamiento que se sigue suele ser cronológico. Sin embargo, el concepto de prueba o evidencia es mucho más complicado que un simple apunte de bitácora. En el método científico, una **prueba** es un **hecho conjeturado** por alguna teoría y cuya presencia o ausencia sólo es compatible con una o varias teorías, a la vez que descarta a otras. Así pues, las pruebas científicas permiten discriminar qué interpretación (teoría) encaja correctamente un conjunto de hechos y cuáles no. Además, las pruebas científicas tienen un fuerte carácter **empírico**, de **experimento**, y son procesos que se pueden repetir siempre que se quiera, y que darán siempre el mismo resultado.

La evidencia[3] científica sirve para señalar como cierta a una determinada teoría o hipótesis y, a la vez, sirve para descartar otras. **La evidencia es la información, los hechos que, unidos al proceso de deducir unas conclusiones (inferencia), apoyan o rebaten una hipótesis. La evidencia científica es pública**, en el sentido de que permite a otros examinar las hipótesis de las que parte, y da a conocer las suposiciones y razonamientos que se hacen para llegar al final del proceso de inferencia. Estas evidencias deben ser observables, empíricas y mesurables, así como someterse a los principios del razonamiento (lógico) en el proceso final de la evaluación de la hipótesis.

Las evidencias digitales que puedan ser útiles ante un juez deberán ser del tipo de las pruebas científicas. Aunque quedó bastante claro por parte de los asistentes del mundillo jurídico que en el ordenamiento español una prueba es todo aquello que (unilateralmente) acepte el juez como tal, esos mismos jueces deberán apoyarse en los informáticos y tecnólogos para adquirir los criterios que les permitan reconocer responsablemente lo que son pruebas y lo que no lo son. Además de esto, lo que quizás sea más importante es que deberán recurrir a los técnicos para saber, en cada caso, de qué pueden ser pruebas.

Me temo que el sistema jurídico español, por no ampliarme a otros, va a tener poco que hacer por si sólo en el tema de las evidencias y pruebas digitales, y que los jueces y las partes tendrán que seguir recurriendo al peritaje para dirimir sus antagonismos. Lo que sí es muy necesario es que esos peritos, esos tecnólogos, pongan en pie y hagan pública, con cierta urgencia, una Técnica Forense mucho más seria (probatoria) de la que hoy tenemos.

Aunque quedó bastante claro por parte de los asistentes del mundillo jurídico que en el ordenamiento español una prueba es todo aquello que (unilateralmente) acepte el juez como tal, esos mismos jueces deberán apoyarse en los informáticos y tecnólogos para adquirir los criterios que les permitan reconocer responsablemente lo que son pruebas y lo que no lo son. Lo que sí es muy necesario es que esos peritos, esos tecnólogos, pongan en pie y hagan pública, con cierta urgencia, una Técnica Forense mucho más seria (probatoria) de la que hoy tenemos.

Si las pruebas son informaciones que permiten discernir entre hipótesis ciertas e inciertas, la mera acumulación de registros no puede suponer una prueba en el sentido de la evidencia digital que nos ocupa. Tomemos como ejemplo los problemas que plantea la identidad y la autoría de unos hechos dentro de un siste-

[1] **Respuestas SIC**: "*Evidencias electrónicas y pruebas: guardarse las espaldas*". 17 de marzo de 2009 en Madrid. 18 de marzo de 2009 en Barcelona.

[2] **To log** es un verbo inglés que deriva del sustantivo *logbook*, es decir, del término sajón para el cuaderno de bitácora, en castellano, que es el libro en el que los pilotos mercantes anotan el estado de la atmósfera, los vientos, los rumbos que se hacen, las distancias recorridas, las observaciones astronómicas, etc. Como verbo, significa *registrar en* un libro, y fue acuñado a principios del siglo XIX. En 1963 se utilizó para describir el registro sistemático de eventos concretos en el procesado de datos con ordenadores.

[3] **Evidencia**: (del latín, *video*, ver) Conocimiento intuitivo que nos permite afirmar su contenido como verdadero, con certeza, y sin sombra de duda. Certeza clara y manifiesta de la que no se puede dudar. Certidumbre de algo, de modo que el sentir o juzgar lo contrario sea tenido por temeridad.

ma informático. Un usuario legítimo puede acceder a su sistema con sus credenciales auténticas, puede iniciar una comunicación protegida, por ejemplo con SSL, entre su terminal y su banco, y luego realizar una transacción con su número secreto, mal denominado como "*firma digital*" por muchos bancos. Todos esos hechos pueden ser adecuada y minuciosamente "*logeados*" por el banco, e incluso por el propio terminal del usuario pero, sin embargo, esos apuntes no serían una evidencia o una prueba válida para un razonamiento causal o un proceso inculpatorio.

Imaginemos que en el ejemplo anterior, realmente se realizaron dos operaciones, y ambas fueron "*firmadas*" con la exhibición del número secreto fijado para tal fin. Los registros al uso no pueden probar cuál era el entorno en el que se realizaron ambas transacciones y, con ello, no pueden descartar que se estuviesen ejecutando otros procesos paralelos sin conocimiento del usuario. Al no poder probar la ausencia de "procesos parásitos" que hubiesen aprovechado el canal SSL y la exhibición de la pseudo-firma para realizar la segunda operación no reconocida por el usuario, no se puede concluir (probar) que ambas fuesen el resultado de la libre voluntad del usuario. Los *logs*, *per se*, sólo probarían qué ocurrió, pero no quién lo causó.

La Identidad Digital

Además de la relación causal que debe aportar, sin atisbo de duda, la evidencia o prueba digital, otro tema importante en este contexto es el de la Identidad Digital. Ningún sistema basado en la posesión o conocimiento de **secretos compartidos** sirve para probar nada en lo que se refiere a la relación entre una **Identidad Digital** (credenciales de acceso y operación) y una **Identidad no-Digital** (persona física). Todos los sistemas basados en nombres de usuario y palabras clave son sistemas de secreto compartido (la contraseña) entre el usuario y el sistema, por lo que **los administradores de los sistemas siempre pueden suplantar a cualquiera de sus usuarios menos privilegiados**. Mientras que el sistema usuario/contraseña es útil para organizar el acceso y separar a los agentes entre autorizados y no autorizados, no sirve realmente para distinguir, sin posible duda, quién hace realmente las cosas. Realizar operaciones a través de un túnel de comunicación SSL/TLS puede proporcionar autenticación de los extremos (si está bien montado) pero no supone la firma de las transacciones que circulan a través de él. Cualquier sistema de firma requiere, previamente, haber establecido una sólida Identidad Digital.

La Identidad Digital requiere que la instancia del secreto sobre el que se sustenta sea única, sin copias ni *backups*, y que sea sólo **conocida y operada por un único ente o agente**; si además ese secreto fuese innato, voluntariamente mutable y no transferible, mucho mejor. La realidad tecnológica actual es que las cosas no son así.

Los modelos y leyes de Firma Digital, no sólo la española, apuntan y exigen muchas características que son buenas y necesarias para poder probar la autoría de los hechos en el mundo digital, pero no son perfectas, entre otras cosas, porque son transferibles. Alguien decía en la jornada a la que asistí, que más que una firma digital, lo que realmente tenemos en la legislación española es un **sello** o **tampón digital,** ya que cualquiera puede entregar su DNI electrónico a otro y darle su PIN de activación y eso es, además de cierto, obvio; pero lo que no se dijo es que, muy probablemente, es imposible que sea de otro modo.

Los críticos de los sistemas actuales de firma digital invocan la inclusión de factores biométricos para crear una verdadera firma digital; sin embargo, esos factores biométricos no sirven, ya que todos ellos son factores públicos o potencialmente públicos. Invocar la biometría con la esperanza de hacer no transferible la capacidad de firma es un error y el mejor modo de hacerla transferible de modo no percibido. **Una característica biométrica es estable, no cambia, no se renueva, y puede ser medida sin la colaboración explícita y consciente de su propietario.** Las huellas dactilares las dejamos por todas partes, nuestro iris aparece en todas las fotos y filmaciones de nuestra vida, así como nuestra forma de andar o la forma de nuestras orejas. Nuestra voz la ha podido grabar cualquiera y nuestro ADN está accesible en cualquier ropa o cosa que hayamos tocado o vestido. Los datos y características biométricas deben considerarse públicos y en posesión del atacante, y una Identidad Digital precisa de un secreto único para poder construirse. Cualquiera puede entender que es fácil hacer público un secreto, pero **es imposible hacer secreto algo público**.

La Identidad Digital requiere que la instancia del secreto sobre el que se sustenta sea única, sin copias ni backups*, y que sea sólo conocida y operada por un único ente o agente; si además ese secreto fuese innato, voluntariamente mutable y no transferible, mucho mejor. La realidad tecnológica actual es que las cosas no son así.*

Dejando a un lado la peliaguda tarea de probar la autenticidad de los registros de log*, es necesario pensar si conviene que esos apuntes se tomen y se concentren en equipos que son los encargados de procesarlos. Esa geometría centralista tiene el problema de convertir al sistema central en una pieza especialmente sensible y atractiva para los atacantes.*

Cuestionamiento de la monitorización

Volviendo al tema de los que proponen la monitorización intensiva de los sistemas como herramienta para poder saber lo que pasa en dichos sistemas, es necesario cuestionarse sobre la conveniencia o no de tal práctica. La recogida generalista de datos, la monitorización indiscriminada no necesariamente aporta evidencias o pruebas digitales que permitan establecer, sin sombra de dudas, relaciones causales sobre los hechos y menos aún autorías responsables. Sin embargo, esa monitorización puede ser muy útil para depurar los sistemas y hacerlos mucho más eficientes y seguros, en el sentido más amplio del término.

Dejando a un lado la peliaguda tarea de **probar la**

autenticidad de los registros de *log*, es necesario pensar si conviene que esos apuntes se tomen y se concentren en equipos que son los encargados de procesarlos. Esa geometría centralista tiene el problema de convertir al sistema central en una pieza especialmente sensible y atractiva para los atacantes. Como una máxima de la seguridad es que es muy fácil proteger aquello que no existe, quizás no compense centralizar la gestión de *logs*.

Supongamos que se produce un incidente en un escenario en el que todos los sistemas están dispersos, cada uno tiene sus *logs*, pero no se combinan en ningún sitio. Para elucidar qué es lo que ha pasado, un equipo humano perfectamente identificado y autorizado tendrá que ir recopilando datos y declaraciones para, al final, emitir un único y específico informe sobre lo ocurrido. Ese informe sólo tratará de un incidente en concreto y, según se distribuya, podrá ser conocido por unos pocos o por muchos.

Pasemos a otro escenario en el que, en previsión, se cuenta con un sistema que recopila los registros dispersos y los integra en una inmensa base de datos, de modo que el futuro investigador autorizado sólo tenga que pulsar unas pocas teclas para saber qué ha ocurrido. Es cierto que, en este caso, la investigación será mucho más rápida, pero no mucho más fiable. La velocidad puede ser un mérito del sistema, pero abrir la posibilidad de que se puedan hacer otras **"investigaciones no autorizadas"** quizás no compense.

Escenarios descentralizados y centralizados

Pongámonos en un escenario propio del espionaje industrial o no industrial; en un sistema de monitorización no centralizado y no agregado, el atacante necesitará infiltrar espías humanos que hagan la recolección de datos que hacía el investigador autorizado del ejemplo anterior. Esos espías tendrían que acceder a diferentes sistemas, contactar con distintos operadores y administradores, y todo ello con un coste superior, en tiempo y recursos, al de la investigación autorizada de los de "*asuntos internos*".

En el caso del sistema centralizado, automatizado e intensivamente monitorizado, los espías sólo tienen que entrar en el sistema central, preguntar lo que quieran a esa inmensa base de datos que representa la conciencia de todo el sistema, y enterarse de todo lo que ocurre incluso mejor que los propios dueños legítimos del sistema. Esto es así ya que **la "*inteligencia*" que se obtiene de una buena base de datos siempre está limitada por la "*inteligencia*" de la pregunta que se le haga.**

Sistemas dispersos y discretos

Una forma de combinar la ventaja de que existan registros de lo que ocurre en los sistemas informáticos y de información, y de que no haya el riesgo de montar un sistema central del que se puedan aprovechar también nuestros "enemigos", es utilizar **sistemas dispersos y discretos de un sistema compartimentalizado**. En ese escenario, los registros, los *logs*, se gestionan de forma independiente junto a la fuente de la que se nutren, y se procura con ahínco proteger su integridad, su autenticidad y controlar su acceso. Cuando sea necesario y esté adecuadamente autorizado, los agentes pertinentes, humanos o no, reunirán sólo la información que es precisa para proseguir una investigación en concreto. Así sólo se reúne y se genera la información sensible cuando es necesaria y en condiciones controladas.

Este inteligente proceder es el que se sigue para la manipulación de las sustancias más toxicas que jamás han existido[4]. Dado que los gases neurotóxicos de la guerra química son tan letales, su manipulación es realmente difícil y por ello, los ingenieros de armamento descubrieron que lo importante era fabricar, acumular y transportar por separado dos reactivos que, en el momento de la verdad, sintetizasen el agente letal poco antes de ser necesario[5].

Siguiendo tan sombrío ejemplo y aplicándolo a aquellos sistemas en los que haya que proteger la confidencialidad de procesos e informaciones, quizás debamos huir de las grandes bases de datos llenas de registros y trazas del sistema, y preocuparnos más de cómo conseguir que los registros que genera cada sub-sistema sean íntegros, auténticos y realmente verificables mediante un procedimiento público.

La mera y masiva acumulación de trazas sólo puede hacer la felicidad de espías, licenciadores de bases de datos y vendedores de equipos para correrlas, pero en sí, no siempre permiten llegar a descubrir qué es lo que realmente pasó y casi nunca llegan a probar quién lo causó si enfrente tenemos a un ser humano[6] adecuadamente entrenado.

El camino hacia una evidencia y prueba digital es largo y realmente no lo hemos iniciado. Por el momento, otros procedimientos de investigación más clásicos y menos digitales pueden cubrir las incipientes necesidades actuales, pero más temprano que tarde se quedarán cortos, si no lo son ya. Probar algo en el mundo digital será mucho más difícil que probar algo en el mundo físico que tan bien conocemos. ■

La mera y masiva acumulación de trazas sólo puede hacer la felicidad de espías, licenciadores de bases de datos y vendedores de equipos para correrlas, pero en sí, no siempre permiten llegar a descubrir qué es lo que realmente pasó y casi nunca llegan a probar quién lo causó si enfrente tenemos a un ser humano adecuadamente entrenado. Debemos preocuparnos más de cómo conseguir que los registros que genera cada subsistema sea íntegro, auténtico y realmente verificable mediante un procedimiento público.

[4] Tabun, Soman, Sarín, Ciclosarín, Agentes nerviosos VX y VR, los agentes de Novichok, etc.

[5] **Munición Química Binaria**: son armas químicas en las que el agente tóxico no está contenido en ellas en un estado activo, sino como dos precursores físicamente separados, que son mucho menos tóxicos que el agente que generan si se les mezcla. La reacción química de generación del agente letal se produce mientras el arma está en vuelo hacia su destino, y que se completa antes de ser dispersada como un aerosol mortal.

[6] ***Evidencia***, cuento o relato corto escrito por Isaac Asimov y publicado en septiembre de 1946 en la revista *Astounding Science Fiction* y luego reimpreso en las colecciones como Yo, Robot (1950), The Complete Robot (1982), y Visiones de Robot (1990).

Jorge Dávila Muro
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es