https://doi.org/10.18800/iusetveritas.202401.005

Prueba informática: el problema de su fiabilidad(*)(**)

Computer Evidence: The Problem of its Reliability

Luis Alfaro Valverde(***)
Pontificia Universidad Católica del Perú (Lima, Perú)

Resumen: Los datos contenidos en dispositivos informáticos y tecnológicos, cada vez más, son utilizados como elementos de prueba en los procesos judiciales, siendo determinantes en las decisiones finales de los jueces. Se trata de la denominada prueba informática. A menudo estas suelen ser valoradas acríticamente como una mera prueba documental, sin que se considere, entre otras cosas, su naturaleza vulnerable y compleja. Entre los distintos problemas que existen sobre esta prueba, este estudio se centra específicamente en aquellos relacionados con su fiabilidad. Se examinan, en primer orden, los aspectos relacionados a la naturaleza de la prueba informática, así como su valoración racional. Luego, se revisa la cuestión central de su fiabilidad, relacionado con el riesgo de su manipulación y su repercusión en la misma. Por último, se analizan algunos instrumentos que permitan gestionar adecuadamente su fiabilidad, como es la pericia, la firma electrónica y la intermediación del notario en la certificación de la evidencia digital.

Palabras Clave: Prueba informática - Fiabilidad - Riesgo de manipulación - Derecho Procesal - Perú

Abstract: The data contained in computer and technological devices are increasingly used as evidence in judicial processes, being decisive in the final decisions of judges. This is the so-called computer test. These are often valued uncritically as mere documentary evidence, without considering, among other things, their vulnerable and complex nature. Among the different problems that exist about this test, this study focuses specifically on those related to its reliability. Firstly, the aspects related to the nature of the computer test are examined, as well as its rational assessment. Then, the central question of its reliability is reviewed, related to the risk of its manipulation and its impact on it. Finally, some instruments are analyzed that allow their reliability to be adequately managed, such as expertise, the electronic signature and the intermediation of the notary in the certification of digital evidence.

Keywords: Computer evidence - Reliability - Risk of manipulation - Procedural law - Peru

---

(*) Nota del Equipo Editorial: Este artículo fue recibido el 24 de marzo de 2024 y su publicación fue aprobada el 22 de junio de 2024.
(**) La presente investigación contó con el apoyo financiero del Centro de Investigación, Capacitación y Asesoría Jurídica (CICAJ) del Departamento Académico de Derecho de la Pontificia Universidad Católica del Perú.
(***) Abogado por la Universidad Privada San Pedro. Máster por la Universidad Complutense de Madrid. Doctorando en el Programa de Doctorat en Dret, Economia i Empresa de la Universidad de Girona. Profesor ordinario del Departamento Académico de Derecho de la Pontificia Universidad Católica del Perú, Lima (Perú). Miembro del Grupo de Investigación de Derecho Procesal Crítico y Constitución (GIDEPROC). Código ORCID: 0000-0001-8433-4099. Correo electrónico: lalfarov@pucp.edu.pe

1. Introducción

Desde la década de los 90, la tecnología ha irrumpido en la sociedad al punto de considerarse indispensable en todos los ámbitos (disrupción digital), incluso en lo jurídico, esta última, a consideración de algunos, es lo que fundamenta el denominado Derecho informático(1). El uso de las Tecnologías de la Información y la Comunicación (TIC) e Informática en el ámbito de la función judicial no es ajeno a este fenómeno social, principalmente, en el contexto de la pandemia por la COVID 19.

Por un lado, con la finalidad de garantizar la prestación del servicio de justicia, muchos Estados regularon y aplicaron nuevas disposiciones para el ejercicio de la función jurisdiccional. Es así como se dispuso el teletrabajo para los magistrados, servidores y auxiliares jurisdiccionales, también, se permitió la realización de audiencias virtuales mediante aplicativos como *Google Meet* o *Zoom* en reemplazo de las audiencias presenciales; además, se creó nuevas plataformas digitales para la presentación de escritos judiciales, entre otras medidas(2). Todo ello representó un aceleramiento mayor en el uso de las TIC en el ámbito judicial.

Por otro lado, en cuanto a la relación de las tecnologías con el Derecho probatorio, las TIC como medios para corroborar las afirmaciones sobre los hechos en juicio han incursionado con lentitud, a pesar de que hoy en día es usual utilizar los datos almacenados en soportes electrónicos (tales como SMS, *e-mail*, *WhatsApp*, *Facebook Messenger* o *Telegram*). Llama la atención que, cuando estas pruebas informáticas(3) son presentadas al proceso, su análisis y valoración no siempre es el esperado. Quizá esto se deba, entre otras razones, a cierto recelo sobre la veracidad de la información digital, mostrando con esto cierto sesgo de sobreconfianza (*overconfidence bias*), respecto de sus habilidades fundadas por la experiencia judicial en el manejo del proceso y su decisión final.

Existe la preocupación de contar con herramientas idóneas para verificar la autenticidad de la evidencia digital, puesto que, en atención a su naturaleza, el contenido de la prueba informática es muy vulnerable y, por lo tanto, menos confiable que las pruebas tradicionalmente empleadas. Por ejemplo, en el proceso civil, laboral o penal, se ha vuelto una práctica cotidiana que las partes capturas de pantallas (*screenshots*) sobre conversaciones entre los propios sujetos procesales o estos con terceros mediante redes sociales como *WhatsApp, Messenger, Telegram, Instagram,* por mencionar las más conocidas. Sin embargo, el temor surge cuando se aporten quiere determinar la validez de tales pruebas. Es decir, en el caso en concreto, para otorgar fiabilidad a dichas conversaciones, se necesita verificar, previamente, que su contenido sea verdadero, siendo una condición necesaria para que el juez pueda tomarlo en cuenta en el momento de la resolución de la controversia.

De ahí que, es oportuno preguntarse, si acaso esta nueva forma de probar supone una alteración en la comprensión y sentido actual del fenómeno probatorio. De hecho, el mayor desafío de este medio de prueba es cómo determinar su validez, ya que en la doctrina existe un gran debate sobre si se debe o no recurrir a una pericia, cuán útil sería el uso de la firma electrónica o quizá la intervención de un notario que acredite la veracidad de la evidencia digital, preliminarmente, a su presentación en soporte físico. Todas estas acciones son consideradas como posibilidades para una mejor comprensión de la prueba informática. De igual manera, se pone en cuestión que, si para diseñar un procedimiento probatorio adecuado es necesario determinar, por lo menos: ¿cómo obtener una prueba informática?, ¿cómo

(1) "La idea de un Derecho informático tiene como punto de referencia el pensamiento de Norbert Wiener en su obra *The human use of human beings: cybernetics and society"* (Téllez, 2003, p. 23). También se afirma que esta disciplina jurídica, aplicado a la ciencia procesal, ha dado inicio al Derecho Procesal Informático, definida, según Vicente (2016) como "un conjunto de actos provenientes del Estado que regulan las pruebas digitales que aportan las partes y terceros ajenos a juicio, a fin de demostrar los hechos controvertidos en él mismo" (p. 611).

(2) De acuerdo con Arellano et al. (2020), todas estas iniciativas realizadas por las autoridades competentes conllevaron a una reforma a gran escala del sistema de justicia, especialmente, en los diversos estados latinoamericanos, en donde se mostraba cierto rezago sobre el uso de las tecnologías en el sistema judicial en comparación a otros como Estados Unidos o los países europeos.

(3) En general, las palabras "electrónica" e "informática" se utilizan de manera análoga para referirse a los soportes tecnológicos presentados como pruebas en el proceso. Pero, se sabe que no todo lo electrónico es necesariamente informático o a la inversa, dado que no todo instrumento electrónico busca el procesamiento de información. En la actualidad, son cada vez más las tecnologías llamadas emergentes que no utilizan la electrónica, sobre todo en lo que respecta en la conservación de la información. Por estas razones, no existen objeciones fuertes sobre el uso de expresiones "prueba electrónica" o "prueba informática" o "prueba digital". No obstante, para los fines del presente estudio se utilizará preferentemente los términos "prueba informática".

introducirla al proceso?, vale decir, si acaso su aportación al proceso deba ser diferente a la utilizada por la prueba tradicional, y, por último, ¿cómo debe ser valorada por el juez?

Son varios los cuestiones que se realizan a esta prueba; sin embargo, este estudio únicamente interesa analizar y discutir las principales dificultades que existe con relación a su de fiabilidad. Esto debido a las particularidades (naturaleza) de la información y datos cognitivos que contiene esta prueba(4). Para ello, se iniciará con un breve análisis de los aspectos más relevantes de la prueba en la era digital: fuente, medio y hecho digital; concepto y naturaleza de la prueba informática; y valoración racional de la evidencia digital. Seguidamente, se revisará el problema de su fiabilidad, relacionado con el riesgo de manipulación de la evidencia digital y su repercusión en la misma. Finalmente, se reflexionará sobre algunos instrumentos para gestionar la fiabilidad de la prueba informática, como es la pericia, la firma electrónica y la intermediación del notario en la certificación de la evidencia digital.

2. La prueba en la era digital

El estudio del fenómeno probatorio es quizá uno de los temas que más ha sido afectado con tal intervención tecnológica, en especial las relaciones derivadas de la actividad probatoria con el internet (5). Estos medios digitales son utilizados como pruebas judiciales con las que se puede determinar, verbigracia: la marca; el modelo; el número de serie del USB conectado a una computadora; a qué hora y qué información copió; y cuándo desconectó el dispositivo electrónico(6). Esta vinculación entre las TIC y el fenómeno probatorio hace necesario repensar el entendimiento de cuestiones básicas de la prueba a la luz de los cambios que exigen las especificidades del nuevo contexto de la era digital. Por esto, a continuación, se analizarán algunos aspectos (fuente, medio, hecho digital, concepto, y una breve experiencia comparada) de la complejidad de la prueba informática como un nuevo tipo de prueba.

2.1. Prueba informática: trinomio probatorio digital

Una cuestión previa al estudio de la prueba informática es la discusión sobre la posible variación en la típica diferencia teórica de las categorías fuentes de prueba, medios de prueba y hechos en el contexto digital(7): *trinomio probatorio digital*. La confusión en sus significados es causante de problemas en la doctrina y en no pocos casos en la práctica judicial. Una distinción que más ha influenciado en la doctrina procesal es la planteada por Sentís Melendo (1979), quien afirma que, por un lado, las fuentes de prueba son aquellos elementos que existen en la realidad mientras que, por otro lado, los medios de prueba están conformados por la actividad para ingresarlos en el proceso (p. 141-142). De esto se desprende que estas categorías se encontrarían en dos dimensiones distintas. Así, mientras que la fuente de prueba se ubica en un contexto anterior y externo al proceso (extrajurídico), en cambio, los medios de prueba corresponden a un escenario procesal (judicial)(8).

Siguiendo esta explicación, vemos que la fuente se diferencia del medio de prueba por su ubicación extraprocesal y está compuesta por datos empíricos o elementos de la realidad con información fáctica que se suscitan de manera extraña al proceso. Por ejemplo, con respecto a la prueba documental, la fuente estaría compuesta por la información contenida en el objeto definido como "documento" o, en relación a la prueba testimonial, es el testimonio mismo que constituye la fuente de prueba. En cambio,

(4) Si bien se analizarán diversos problemas en torno a la prueba informática en el proceso judicial, no se tiene como objetivo hacer un estudio minucioso y detallado de cada uno de ellos, solo se hace mención de los escenarios en donde interviene también el problema de la fiabilidad.

(5) Es conocido que la expresión "prueba" es polisémica, bien se la puede concebir como actividad (regulada por el procedimiento probatorio en el que se establece la manera como debe producirse la prueba al interior del proceso); medio (elementos que emplea el juzgador para determinar los hechos del caso) y resultado (la conclusión en la que el juez resuelve que hipótesis de los hechos pueden darse por verificadas). Comparten estos sentidos de prueba: Ferrer, 2005, p. 27-29; Taruffo, 2002, p. 448-450; Gascón, 2010, p. 77-78 y Ubertis, 2017, p. 73 -74.

(6) Bueno De Mata (2014) explica que una dificultad que presenta la investigación y sanción de los ciberdelitos es que la mayoría de casos judiciales de este tipo tienen como único elemento probatorio a la prueba informática p. 140-141.

(7) Frecuentemente los sistemas procesales ponen mayor énfasis en los "medios de prueba", sin embargo, la doctrina procesal ha manifestado también la necesidad de distinguir "medio de prueba" y "fuente de prueba". Los teóricos que han estudiado tal distinción, entre otros, son: Bentham, 1825, p. 19-39; Carnelutti, 1955, en la doctrina clásica; Arazi, 1998, p. 123-126; Devis Echandía, 2002, p. 532-533; Falcón, 2003, p. 615-635; Montero Aroca, 2005, p. 133-137; Taruffo, 2002, p. 439-448, en la doctrina más reciente.

(8) Distinción que también ha seguido Montero Aroca (2005) al referirse a la fuente de prueba como lo que ya existe en la realidad y como medio de prueba la forma como se aporta al proceso (p. 133-137).

en el contexto digital, la fuente de la prueba se centra en toda la información o datos digitales[9] contenida o transmitida por los nuevos instrumentos o medios electrónicos desarrollados por las tecnologías de la información (así como: celulares, *smartphones*, computadoras, *tablets*, dispositivos USB, *CD-ROM*, reproductores de MP3 o MP4), que ofrecen una forma distinta de registrar la información. Ello a su vez representa un incremento de fuentes de prueba electrónica en donde puede encontrarse información de diversa naturaleza; por ejemplo, registro de acciones como los *logs*, bases de datos o comunicaciones digitales como los *e-mails* y SMS, mensajería instantánea (*WhatsApp*), redes sociales como *Facebook*, entre otros.

En lo que concierne a medio de prueba, Taruffo (2010) menciona que es cualquier elemento usado para determinar la verdad de los hechos. Aunque, intentando ser preciso, en el proceso, los hechos ingresan como enunciados (o conjunto de enunciados) que describen las situaciones que se dieron en el pasado y que son importantes para la solución de la controversia (p. 16). Consecuentemente, como refiere Gascón (2010), son los enunciados que versan sobre los hechos el objeto de la prueba y no los hechos mismos, ya que una vez ocurridos no se pueden probar sino constatar (p. 76)[10]. Con todo, la referencia a medio de prueba o "*evidence*"[11] lo ubica en la realidad del proceso judicial y da cuenta de la forma o manera como las fuentes de prueba son ingresados al contexto jurisdiccional. Así, cuando se habla de la prueba documental, el medio consiste en la manera por la que es incorporado al proceso, por ejemplo, adjuntando físicamente por si se trate de un documento impreso.

En el contexto informático, se hace mención a medio de prueba como la forma mediante la cual dicha información de naturaleza digital ingresa en el proceso judicial. La multiplicidad de fuentes probatorias, antes mencionadas, deben ingresar al proceso a través de alguno de los instrumentos de prueba legalmente previstos. Para Delgado (2017), esto abre la posibilidad de ingresar las fuentes de pruebas informáticas, sea usando las formas tradicionales como documento, prueba pericial e incluso mediante la prueba testifical o declaración de parte mediante las declaraciones o el testimonio del sujeto o individuo que ha tenido contacto con el aparato electrónico (párr. 5-6). Con relación a lo afirmado, aquello pone en discusión la naturaleza jurídica de la prueba informática y su descripción como un mero documento electrónico, cuestión que será materia de análisis en la siguiente sección sobre su naturaleza jurídica.

Luego, tanto fuente como medio de prueba son, en rigor, elementos empíricos que permiten el conocimiento de los hechos como resultado del contacto de las personas, a través de sus sentidos, con los acontecimientos. Hechos que suceden en la realidad y tienen relevancia jurídica. Según Meneses (2008), un ejemplo es el caso de la celebración de un acto jurídico en un tiempo pasado, que no puede ser registrado por la experiencia sensorial presente, el cual requiere de signos retenidos en el presente para constatar su realización en la realidad (p. 54-56). A su turno, la prueba informática también permite constatar hechos digitales, con la cualidad de que esta prueba determinará la veracidad de las afirmaciones sobre los hechos digitales. Hecho que puede ser definido como un suceso o acontecimiento de un entorno virtual[12]. No cabe duda de que en el mundo digital sobrevienen muchos hechos importantes para el derecho, no obstante, tal como refieren Oliva y Valero (2016), "solo habrán hechos jurídicas digitales cuando exista una voluntad humana consciente y libre, y no en actos automáticos que realizan los ordenadores ajenos al conocimiento de su usuario" (p. 29).

Con todo, se observa que las categorías probatorias analizadas (fuente, medio y hecho) parecen no haber sufrido mucha

(9) El Convenio de Budapest sobre Ciberdelincuencia define datos informáticos como "toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función" (Council Of Europe, 2001, p. 4).

(10) Asimismo, Ubertis (2017) sostiene que es inexacto y distorsionado hablar de "prueba de la verdad de los hechos", pues con ello se olvida que no existen "hechos verdaderos" o "hechos falsos", pues un hecho "es" o "no es", solamente su enunciación puede ser "verdadera" o "falsa". Siendo correcto hablar de "prueba de la verdad de la afirmación de existencia de un hecho" (p. 21).

(11) Conviene mencionar que, en la literatura inglesa para referirse a medio de prueba, en la mayoría de los casos, se utiliza la expresión *evidence*, la cual es entendida como aquello destinado a demostrar, o refutar, la existencia de algún u otro hecho afirmado por alguna persona. *Véase* "Rethinking Evidence. Exploratory Essays" de Twinig, 2006, p. 193.

(12) Según Delgado (2016), el entorno virtual, inferido con base en la STS 342/2013, 17 de abril de 2013, es entendido como "aquel conjunto de informaciones en formato digital que una persona genera con su actividad mediante dispositivos electrónicos, de manera consciente o inconsciente, con voluntariedad o sin ella" (p. 363).

alteración cuando se contrasta con las particularidades de la prueba informática, entendida como un elemento de la realidad sensible que, al igual que la prueba clásica, registra una serie de hechos del mundo a través de impulsos eléctricos que almacena y/o transmite información. En buena cuenta, la prueba informática lo que hace es ampliar el catálogo de datos empíricos que transitan en la realidad. Lo que no se puede negar es que los datos e información contenidos en este tipo de pruebas son de más difícil percepción por las personas. De esta forma, se exige el apoyo de dispositivos y programas informáticos adecuados para la lectura de la información; lo que provoca, entre otras cosas, problemas relacionados con la confiabilidad epistémica en los juzgadores, que es la principal preocupación de este estudio.

2.2. Concepto y naturaleza jurídica: ¿más que un documento electrónico?

Formas de comunicación totalmente desconocidas para el Derecho se han presentado en el ámbito probatorio como consecuencia del entorno digital. No obstante, con referencia a estos, los operadores jurídicos están incursionando en una menor medida de la que deberían; pero a todo esto ¿qué debemos entender por prueba informática? Los ordenamientos normativos en general no se han comprometido en establecer algún concepto legal, por ello los teóricos vienen proporcionando distintas nociones doctrinales. Pese a que la idea de prueba informática no es muy antigua, existen múltiples propuestas e intentos por definirla, aunque lo cierto es que pocas veces se emplean de manera estable y rigurosa. Pero subsiste la necesidad de comprender esta nueva forma de prueba mediante conceptos que al menos puedan ser aceptables, que, sin pretender terminar la cuestión, contribuya a los que trabajan con esta prueba en proporcionar algo de luz frente a un tema complejo y a veces ambiguo. Con este propósito, no sería pertinente plantear un concepto abstracto más de la prueba informática.

En cambio, puede resultar más útil aproximarse a la cuestión de manera descriptiva que trate de identificar los principales caracteres que normalmente se atribuyen a la prueba informática. De este modo, se pueden considerar los siguientes elementos: (i) toda clase de información o datos; (ii) producida, conservada o transmitida por dispositivos electrónicos o medio digital; y (iii) puede tener efectos para corroborar hechos digitales en la indagación de todo tipo de proceso. Estos caracteres no pretenden ser exhaustivos, pero pueden ser válidos para identificar al menos algunos de los aspectos particulares que se pueden desprender de los diversos conceptos encontrados en la doctrina[13].

A pesar de esta descripción, parece que la complejidad del problema no permite identificar con claridad qué se entiende por prueba informática, sobre todo cuando se intenta comparar o vincular con las características de las pruebas tradicionales y en especial con la prueba documental. Como respuesta a esta preocupación sobre su "naturaleza jurídica", se han planteado diversas tesis o teorías que explican tal relación o si acaso su distinción. Y es que analizar el concepto y la naturaleza de la prueba informática es útil para poder distinguirlo de los documentos electrónicos, que es la forma más usual en que se presenta en la práctica judicial. Sin embargo, no es el único motivo, sino también para permitir distinguirla de otras categorías procesales. Se debe aclarar que la noción descrita no tiene pretensión de ser estipulativa, sino descriptiva. Solo da cuenta de una idea general a partir de la identificación de ciertas características.

Así se tiene que una tesis señala que la prueba documental y la informática son de naturaleza equiparable (teoría analógica). Se afirma que las nuevas pruebas han superado el concepto estricto del documento como "escrito soporte papel" para alcanzar la noción de representación para cualquier tipo de soporte; es decir, tal como lo explica Pinto y Pujol (2017), estamos simplemente ante una actualización de los medios clásicos de prueba (p. 131). Comparte este parecer Téllez (2009), quien argumenta que muchos de los medios enunciados pueden interrelacionarse con las computadoras; pese a ello, en última instancia, la prueba documental tiene un vínculo más estrecho en cuanto a que el fundamento legal pueda constar como

(13) Para mayor información, *véase* Abel Lluch, 2012, p. 104-106; Sanchís, 2012, p. 713-903; Delgado, 2013, p. 1; Bueno De Mata, 2014, p. 103-104, entre otros.

(14) Por ejemplo, para Pinto y Pujol (2017), en el proceso civil español se aplican las mismas reglas para la aportación (artículos. 265 a 27 LEC) y el deber de exhibición documental (328 y ss LEC), aunque, se distingue respectos del valor probatorio, dado que la prueba electrónica se valora conforme a las reglas de la sana crítica mientras la prueba documental pública y privada cuya autenticidad no se ha impugnado se ajusta a un sistema de valoración tasada (artículos. 319 y 326 LEC) (p. 131). *Véase*. Abel Lluch, 2011, p. 109-110.

documento (p. 288). Conforme a esta perspectiva, algunos ordenamientos aplican de modo semejante el régimen legal de la prueba documental a la informática, como la de aportación o exhibición de documentos, aunque tienen diferentes tratamientos respecto de las reglas de valoración probatoria(14). Si bien todo hecho digital puede ingresar al proceso a través de la documental, no es impedimento para acreditar su existencia mediante una prueba pericial o testimonial, esto si tenemos en cuenta que responden al mismo objetivo: la adecuada determinación de los hechos en el proceso.

Al contrario, teniendo en cuenta la teoría autónoma, hay quienes afirman que estos nuevos medios de prueba tienen características propias e independientes de las pruebas tradicionales, las cuales no se pueden encuadrar en el conjunto de pruebas documentales. Diferencia que se proyecta en el distinto tratamiento que hacen algunos ordenamientos legales(15). Sin embargo, conviene tener presente que el concepto de prueba informática es más amplio que el de documento(16). En efecto, según Pinto y Pujol (2017), no es posible entenderlas como categorías equivalentes, entre otras causas, por las diferentes exigencias prácticas de reproducción de los datos del aparato electrónico que deberán ser examinados por un tribunal (p. 130-1031).

También existe la teoría de la equivalencia funcional, en virtud de la cual, de acuerdo con Pinto y Pujol (2017), la prueba informática y el documento (en soporte papel) pueden tener identidad en cuanto a sus efectos jurídicos (p. 131). La idea general es que la tecnología desempeña las mismas funciones que una determinada categoría, por lo que debe ser posible alcanzar similar consecuencia jurídica. Se pone mayor énfasis en la función que cumple la prueba informática y no tanto en el medio que se utilice para ingresar al proceso. A diferencia de la *teoría analógica*, no se trata de algún cambio del sentido del documento tradicional sino el modo en que este se constituye, cuyo objetivo es acreditar un hecho electrónico afirmado por los justiciables. Por estos motivos, para determinar la noción y la naturaleza jurídica de la prueba informática, sería aconsejable la aproximación y el fortalecimiento de la relación entre ingeniería informática y derecho.

Sin pretender profundizar en el análisis sobre la naturaleza jurídica de esta prueba, basta considerar que la teoría de la equivalencia funcional es la que explica mejor su relación con la prueba documental. El ofrecimiento de estas pruebas no tradicionales en el proceso tiene las mismas consecuencias jurídicas que los otros medios de prueba popularmente conocidos y utilizados (documento, pericia o testimonio). Lo que se busca, mediante la aportación de todos estos medios probatorios, incluyendo la novedosa evidencia informática, no es más que la acreditación o corroboración de los hechos objeto de la decisión judicial.

Más allá de la diferencia o similitud entre la prueba informática y documental, lo curioso es que, en el proceso judicial, a menudo las pruebas informáticas suelen presentarse como simples documentos impresos(17). Entonces, ¿cómo se puede hacer valer una prueba informática si, al fin y al cabo, es común que se presenten bajo una forma distinta a su naturaleza? Además, cabe recalcar que, según Carrasco (2016), "la impresión de una imagen, un correo o mensajes enviados por *Facebook Messenger*, para su aportación en el proceso, suponen la omisión de importantes datos de los que puede depender su valoración final" (p. 44). En otras palabras, se debe precisar que lo que se presenta es una simple representación de un medio digital, introducido en el proceso con la finalidad que el juez sepa de qué se trata(18). En ninguna circunstancia, la presentación de este documento impreso debe ser considerada como la prueba informática en sí misma.

2.3. Hacia una valoración racional de la prueba informática

A diferencia de lo que ocurría antes, en

(16) Para Sepúlveda (2008), erróneamente, un sector de la doctrina hace referencia a la prueba electrónica utilizando el concepto de documento electrónico, ya sea para afirmar en qué consiste, qué características tiene o simplemente para mencionar ejemplos de aquel, sin embargo, no significan lo mismo (p. 9).

(17) Taruffo (2008) sostiene que cada vez con más frecuencia las transacciones se estipulan y documentan por medio de ordenadores, y los registros informáticos y las copias impresas se suelen usar como prueba. Para el autor, la cuestión no parece ser problemática en algunos casos cuando, por ejemplo, se usa un ordenador simplemente como procesador de textos, en lugar de la máquina de escribir o cuando una copia impresa se usa como un texto que está firmado personalmente por las partes, el resultado final es un documento común y corriente que puede ser presentado como cualquier otro tipo de prueba escrita (p. 85-86).

(18) Por ejemplo, cuando una persona compra un automóvil, existen agencias que otorgan dos tipos de facturas: una por email y otra impresa. En un primer momento se puede interpretar que tengo dos tipos de facturas válidas, cuando la correcta es la factura digital. Ahí se demuestra que existe una falta de conocimientos cuando se piensa que el papel es el original ya que esta no es más que una representación gráfica del email.

la actualidad, de manera progresiva, se viene dando real importancia a la necesidad de una valoración de tipo racional de las pruebas sobre los hechos aportados al proceso. Según Ferrer (2007a), este tipo de valoración puede dividirse en dos elementos diferentes; en primer lugar, se pide que los instrumentos probatorios admitidos y actuados sean tomados en cuenta con el fin de justificar el fallo que se tome; y, en segundo lugar, se requiere que la valoración que recaiga sobre las pruebas, se adecue a las reglas de la racionalidad (p. 56-57). Aplicada al tema materia de análisis, el juzgador de los hechos debería otorgar valor probatorio a la evidencia informática con base al raciocinio, según las reglas de la lógica, la experiencia general y los conocimientos científicos.

Pese a que no es posible desarrollar aquí los diversos aspectos sobre la valoración racional de la prueba, es necesario referirnos, por lo menos, a aquellos aspectos que conectan con la confiabilidad epistémica de la prueba. Ante lo dicho, a pesar de que en muchos ordenamientos no existe una regulación muy clara sobre el procedimiento probatorio específico, la regla general debería ser su valoración racional. Sobre el particular Oliva (2016) refiere que:

> La prueba informática no es totalmente diferente a la prueba tradicional, ya que ambas pueden probar la ocurrencia de hechos físicos y electrónicos, por lo tanto, le serán aplicables muchas de las reglas procesales generales sobre actividad probatoria y resultado probatorio establecidos en la legislación (p. 58).

Sin embargo, durante la valoración, deberá tenerse en cuenta algunas particularidades en atención a los conocimiento científicos y tecnológicos por lo que se encuentra inmerso la prueba informática.

En el momento en que el juzgador lleva a cabo la valoración de este tipo de pruebas, de acuerdo con las reglas de la valoración racional, se deberá tener presente, sobre todo, dos particularidades: la autenticidad del origen y la integridad del contenido[19]. Para Delgado (2017), si existen incertidumbres sobre la autenticidad y/o integridad de los datos, será muy probable que el juez cuestione la fuerza o eficacia de la prueba informática (párr. 20-24). Por su parte, Ferrer (2022) señala que "la valoración individual de la prueba tiene por objeto determinar el grado de fiabilidad que tenga cada una de las pruebas aportadas al proceso" (p. 399). En otras palabras, el uso de este tipo de prueba para corroborar las alegaciones de las partes y, con ello, la solución del litigio por parte del juez, que, si bien dependerá de la valoración en conjunto de todos los medios de pruebas aportados, a este conjunto se incluirá la prueba informática, siempre y cuando se determine, previamente, tanto la autenticidad como la integridad de su contenido.

3. Sobre la fiabilidad de la prueba informática

3.1. Fiabilidad epistémica de la prueba

La fiabilidad, de acuerdo con el uso común, es la cualidad de confiable. Es decir, hace alusión a un sujeto o cosa digna de confianza o de lo que se puede uno defiar (Diccionario de la Real Academia Española, 2021). Ahora, el término "confianza" es una locución adjetiva dicho de una persona o, también, de una cosa que tiene las cualidades recomendadas para la finalidad a la que se destina (Diccionario de la Real Academia Española, 2021). De manera sucinta, se puede decir que la fiabilidad es la cualidad que posee un sujeto o cosa de poder defiar de sí misma para la finalidad a la que está predestinada. Sin embargo, profundizando un poco más en el sentido de la fiabilidad (*reliability),* es necesario tener en cuenta que existen diversas líneas de posiciones y teorías que estudian este fenómeno. Así, desde un análisis epistemológico, Becker señala que el fiabilismo (*reliabilism*) comprende varias teorías que buscan explicar el conocimiento o la justificación mediante una verdad propia del proceso, a través del cual un sujeto constituye una verdadera creencia[20]. Luego, Goldman

(19) La verificación por parte del juez de que las pruebas informáticas introducidas al proceso cumplen con los requisitos de autenticidad del origen e integridad del contenido se debe llevar a cabo previo ejercicio del contradictorio de la parte contraria a la que presenta dicha prueba. Es decir, la verificación del cumplimiento de los requisitos mencionados es una tarea en la que coparticipan tanto las partes como el juez, ya que, quien lo presenta deberá acreditar que el contenido de dichas pruebas es verídico, y si no, será la parte contraria quien, en su oportunidad, las impugnará, siendo el juez el que, al tener toda la información completa, deberá verificar si efectivamente el contenido es auténtico e íntegro. Así también, es necesario aclarar que esto no supone una afirmación de que es una cuestión en todo el sistema de valoración de la prueba, sino especialmente cuando se trata de un problema de prueba informática, en donde se deja un amplio margen al juzgador de determinar si confía o no de esta información y en su arbitrariedad, lo cual es contrario al sistema de valoración racional de la prueba.

(20) En efecto, en The Internet Encyclopedia of Philosophy (s/n) se refiere que "Reliabilism encompasses a broad range of epistemological theories that try to explain knowledge or justification in terms of the truth-conduciveness of the process by which an agent forms a true belief".

y Beddor (2021) refieren que, bajo este enfoque del fiabilismo, para que exista un relato adecuado, previamente, se debe indicar la confiabilidad del proceso responsable de la creencia. Dicho de otra forma, que el conocimiento necesita alguna forma de confiabilidad, pudiéndose entender de dos maneras: bien, en un sentido de frecuencia (que pertenece a lo que sucede en el mundo real) o en un sentido de propensión (que pertenece al mundo real como a otros mundos posibles).

Si bien no es el propósito de esta investigación explorar en los confines del fiabilismo y de sus teorías, es importante aprovechar estas ideas en torno a aquel tema para relacionarlo, y aplicarlo, a la comprensión de la prueba en general y la de tipo informática en particular. En este sentido, Zagzebski (2009) nos dice que, desde el ámbito de la epistemología, en muchas ocasiones, la confianza se da en los casos en donde nos falta algo que, en otras circunstancias, hubiéramos querido tener, como una prueba o un tipo de fuente de justificaciones (p. 39) [(21)]. A su vez, Vázquez (2017) refiere que la confiabilidad es normativa, dicho de otro modo, que está tolerado (en términos de justificación) confiar en quien parece ser confiable, llegando a representar la acción de "confiar" un aspecto cognitivo y otro motivacional (p. 178). De esa manera, por un lado, el aspecto cognitivo de la confiabilidad de los medios probatorios depende de que el juzgador cuente con toda la información necesaria sobre la clase de instrumento probatorio ofrecido en el proceso, con la finalidad de otorgarle validez a su contenido; por otro lado, el aspecto motivacional hace alusión a la necesidad de las partes que aportaron sus medios de prueba de tomar en consideración ese interés institucional de los órganos jurisdiccionales concerniente a la búsqueda de la verdad.

Por lo tanto, la confiabilidad epistémica de la prueba informática está relacionada con el grado de conocimiento judicial de que su contenido sea válido. Por ejemplo, que no exista manipulaciones de por medio, o que las partes lo hayan introducido al proceso con la intención de establecer la verdad sobre las afirmaciones de los hechos o sucesos controvertidos. Este aspecto, es de gran importancia si se pretende hablar de una adecuada valoración, pues no se puede desconocer el riesgo de que exista un exceso de confianza epistémica o por el contrario una posición extremadamente escéptica (no cognitiva) del juzgador. Este específico problema probatorio será abordado en la siguiente parte del estudio.

3.2. Statu quo: el riesgo de manipulación y su repercusión en la fiabilidad de la prueba informática

La interacción social por medio de soportes informáticos, como el uso de aplicaciones de mensajería instantánea contenidos en celulares, tablets, laptops o computadoras, genera datos electrónicos que pueden ser útiles para la corroboración de los hechos en el proceso. Esto convierte a las pruebas informáticas en instrumentos novedosos e innovadores. Sin embargo, la posibilidad de crear, modificar o eliminar dichos datos, pone al descubierto el riesgo de su manipulación, repercutiendo en la fiabilidad de la misma.

Tal como señalan Pérez-Tome y Sánchez (2016), "existen muchos procesos en los cuales estas pruebas han sido rechazadas, debido a que los contenidos no han sido reconocidos por el acusado ni se han practicado sobre aquella prueba pericial informática que acredite su autenticidad y envío" (p. 286). Asimismo, según el Estudio Europeo sobre la Admisibilidad de la Prueba Electrónica en la Corte, se percibe la creación de la prueba informática como una dificultad, a causa del desconocimiento sobre los procedimientos de manejo de datos y la interpretación de la ley respecto a este medio probatorio (Fredesvinda Insa, 2007, p. 286). Por otra parte, para De parada (2016), el temor a la prueba informática se centra en su alto grado de volatilidad propio de su naturaleza, terminando por valorar únicamente los medios probatorios tradicionales (p. 345).

A pesar que la prueba informática puede resultar relevante para la resolución de un caso concreto, su alto grado de volatilidad (que los datos contenidos en dichos soportes son temporales, por la facilidad de su manipulación) podría impedir el otorgamiento de un correcto valor probatorio. Es verdad que esta prueba se diferencia de las pruebas tradicionales, por ser intangible y volátil al encontrarse en formato electrónico, pudiendo ser modificada, lo que, para De Prada (2016), representa una dificultad al momento de diferenciar los originales de las copias, de este modo, será sustancial corroborar que la prueba ofrecida es la original, esto, mediante garantías y protocolos procesales con la intención de impedir que sea impugnada por

(21) En una investigación multidisciplinaria, las referencias a autores de confiabilidad epistémica resultan ser pertinentes para el esclarecimiento de este tema, ya que, hablar de confiabilidad epistémica requiere y exige que la fundamentación teórica esté relacionada con bibliografía de epistemología.

una supuesta inexactitud o falsedad (p. 345). La posibilidad de hacer uso de la información contenida en soportes electrónicos como medios probatorios debe ir de la mano con la garantía de que dichos instrumentos no hayan sido adulterados(22).

Si bien pueden existir diversos problemas sobre la fiabilidad de la prueba informática, eso no quiere decir que los jueces tengan una amplia discrecionalidad en sentido estricto de elegir indiscriminadamente en qué pruebas defiar y en cuáles no. Conviene tener presente que, conforme a una adecuada valoración racional de los medios probatorios, se deben analizar de manera individual cada uno de los medios de prueba. Aunque, en la prueba informática la información tiene una naturaleza volátil y son susceptibles de manipulación, eso no quiere decir que *a priori* se le debe restar fiabilidad. A través del uso de técnicas, procedimientos o la intervención de expertos se puede mejorar la autenticidad de los datos digitales y de este modo el juez puede otorgarle el valor probatorio que corresponda.

En la línea de lo sostenido, Alcaino (2014), afirma que la fiabilidad puede ser entendida como un estándar con el que se controla la calidad de las evidencias que son empleadas en el proceso judicial. En otras palabras, esto puede incentivar a las partes a presentar solo aquellas pruebas que cumplan con estándares mínimos de elaboración o producción. Esto garantiza que las probabilidades de errores se vean razonablemente disminuidas, aunque, al final, será el juez quien tendrá que valorar si dicho medio probatorio, en base a su apreciación racional, resulta creíble o no. Siendo así, en el caso de la prueba informática, los jueces deben ser conscientes de la trascendencia de estos nuevos medios probatorios y apoyarse en ellas para la resolución de las controversias. Además, deben verificar en la etapa de actuación, a través del debate probatorio en contradictorio, que estas pruebas introducidas al proceso se encuentren exentas de riesgos de manipulación; para que, posteriormente, se le pueda otorgar el valor que corresponda. Todas estas medidas, no parecen ser suficientes para mejorar el grado de fiabilidad de este tipo de pruebas en un proceso judicial.

3.3. ¿Cómo mejorar la fiabilidad de la prueba informática?

La prueba informática es un fenómeno reciente que presenta aspectos controvertidos, los cuales, algunos hasta el momento, no tienen una solución(23). Uno de los principales problemas gira en torno a la fiabilidad del contenido de los soportes electrónicos, pues, tal como señala Vázquez (2015), no controlar la validez y fiabilidad de los medios probatorios, podría acarrear el ingreso de información deficiente o datos incorrectos al proceso, lo que podría conllevar, a su vez, en graves errores judiciales (p. 14-15). Siendo esto así, resulta evidente que, en atención a la naturaleza especial, se debe tomar medidas para el procedimiento probatorio y que tengan como propósito garantizar que su contenido es válido y, por ende, fiable.

Por ejemplo, es una práctica habitual incorporar pruebas informáticas mediante su impresión en papel, lo que, evidentemente, pone en cuestionamiento su fiabilidad, siendo crucial que se presenten con la aplicación de algún instrumento que garantice la veracidad de su contenido. Es ahí donde el uso de ciertas herramientas para mejorar la fiabilidad en esta prueba será determinante si lo que se busca es establecer la verdad de las afirmaciones sobre los hechos, ya que, tal como señala Vázquez (2015), la fiabilidad probatoria se encuentra ligada a la cientificidad de la prueba (p. 87); es decir, una prueba será fiable, siempre y cuando, a través de alguna herramienta o técnica dotada de cientificidad, se ha determinado que su contenido es verídico o, mejor dicho, que se encuentra exento de modificaciones.

Por este motivo, en la doctrina especializada, se debate sobre el modo más adecuado para solucionar estos inconvenientes y mejorar su fiabilidad. Entre las principales herramientas, se propone el uso de la pericia informática, la aplicación de la firma electrónica, incluso, la intervención de un notario que verifique el contenido de estos tipos de pruebas. A continuación, estas serán materia de estudio.

(22) Tal como afirman Mason & Seng (2017) “Electronic evidence must also be authenticated, as for any other form of evidence. The authentication evidence for electronic evidence is even more critical,and can occasionally be challenging. (...). But if parties and investigative authorities choose to use the fruits of technology, they must also accept the need to prove the authenticity and integrity of the evidence produced by technology, even though the cost of such proof might be considered to be high. This is particularly the case where authentication evidence will shed light on the latent assumptions and hidden errors inherent in electronic evidence, which could affect the accuracy of the electronic evidence itself” (p. 48).

(23) Si bien el fenómeno jurídico en general de la confiabilidad de la prueba informática en particular se da en el contexto judicial y, por tanto, jurídico, esto no excluye la posibilidad de utilizar herramientas bibliográficas de otras áreas de conocimiento (por ejemplo, el campo de la filosofía.) que puedan hasta cierto punto ser útiles y necesarias para explicar mejor el fenómeno jurídico.

3.3.1. La pericia informática: justificación y riesgo de manipulación

Las pruebas que contienen información digital presentadas en una controversia judicial, como se ha afirmado anteriormente, pueden estar expuestas a manipulación[24], dificultad de escucha o visualización. Antes de ahondar más en el tema, primero se considera pertinente señalar que el estilo crítico que se aplica al demostrar las dificultades de la prueba informática que trae consigo el problema de fiabilidad, no busca incrementar las complicaciones, sino solo evidenciar que el estado de cosas no es pacífico y se merece ser consciente de ello, con el objetivo de mejorar. No se niega la trascendencia de la prueba informática para acreditar las afirmaciones sobre los hechos, por el contrario, resaltamos su importancia en la era actual, solo que se debe advertir de ciertas situaciones, respecto de las cuales se deberá ser cautos para garantizar su correcta actuación y valoración.

En efecto, según Oliva y Valero (2016), la prueba informática se representa mediante soportes electrónicos creados por las TIC, razón por la cual tiene de un carácter efímero y manipulable de mayor amplitud que el de las otras pruebas (p. 58). La variable de la evidencia es uno de los aspectos problemáticos de la prueba informática, pues parece no ser complicado manipular el contenido del material electrónico. Taruffo (2008) refiere que aun cuando esta clase de pruebas se impriman, los documentos resultantes no serán "escritos" en el sentido tradicional, por lo que el riesgo de falsificación, errores e incorrecto uso o abuso se da de forma especialmente frecuente y relevante, siendo su alcance, en alguna medida todavía desconocido (p. 86).

Una de las maneras para enfrentar estas dificultades probatorias, que requieren de información y conocimiento especializado, es utilizando la denominada pericia informática. Existe la necesidad de que dichas pruebas sean corroboradas por un informe pericial correspondiente, sólo así el juzgador podrá aceptar o no dicho medio de prueba. Por ello, tal como afirman Abel Lluch y Picó i Junoy (2009), la pericia supone la realización de un conjunto de actividades desplegadas por el experto (p. 25). En este caso, el especialista en Informática y en el uso de las TIC. Su labor inicia con la cadena de custodia de las pruebas informáticas, procedimiento general conformado por las subetapas de localización, fijación, recolección, embalaje y traslado al laboratorio correspondiente para su análisis, y culmina en el dictamen pericial, informe en el que se plasma la actividad del perito, compuesto por el estudio y descripción del objeto, la relación y explicación de las operaciones técnicas, y las conclusiones.

Mediante la pericia informática se puede tener una mejora del grado de fiabilidad de las pruebas informáticas, entre otros aspectos, porque es el resultado de un minucioso análisis forense digital ejecutado por el experto[25]. Por ejemplo, los usuarios de *WhatsApp* o *Facebook Messenger* pueden eliminar un determinado mensaje y luego sacar una captura de pantalla, alterando el contexto de la conversación y ocultando partes que podrían ser concluyentes[26]. En estos casos, para Oliva y Valero (2016), el perito informático debe intervenir lo más rápido posible, puesto que existe el temor o peligro de que ciertos elementos puedan desaparecer al ser eliminados por su autor original (p. 105). Y es que, cualquier tipo de evidencia informática debe ser analizada con mucha reserva y preocupación ante la gran facilidad de que haya sido manipulada por terceros, que puede darse tanto en la inserción de contenido falso o en la eliminación de una parte relevante del mismo, aparentando hechos que nunca ocurrieron y que puede tener una injerencia negativa en la resolución de las controversias judiciales.

3.3.2. Firma electrónica: una alternativa a la pericia informática

Otra de las salidas a las que menudo se acude, es el uso de la firma electrónica. De manera general, se puede decir que es una

(24) Es importante resaltar que, según Pulgar (2016), en la legislación procesal peruana (Código Procesal Civil, Código Procesal Penal, Ley Procesal del Trabajo, entre otros) no se han recogido reglas específicas para el tratamiento de la prueba informática que permitan a los jueces y abogados una actuación más célere y adecuada a los fines que esta exige (párr.10).

(25) Wilson et al (2021) afirman que "electronic evidence in particular needs to be validated if it is to have any probative value. Digital evidence professional will typically need to copy the contents from a number of disks or storage devices. To prove that the electronic evidence has not been altered from its source copy, it is necessary to put in place checks and balances to prove that the duplicate evidence is identical to its source" (p. 444).

(26) Por otra parte, ¿existen aplicaciones que pueden generar chats de *WhatsApp* falsos? La respuesta a esta interrogante es sí. En *Google Play Store* existen aplicaciones gratuitas como "*Whatsfake*" o "*Fake Chat Conversa*tions", las cuales son utilizadas para crear conversaciones falsas de aquella aplicación. Si bien, su propósito principal es usarlo para bromear entre los amigos, haciéndoles creer sobre la veracidad del contenido, no obstante, cuando se presentan dolosamente en un proceso judicial, el propósito ya no es el mismo.

herramienta tecnológica que garantiza la autoría e integridad de los documentos electrónicos. Siendo más precisos, es un mecanismo criptográfico que garantiza la integridad, autenticidad, confidencialidad e identidad de una persona con respecto a estos documentos, mediante el cual otorga su consentimiento. Cuando la prueba contiene una firma electrónica, ésta garantiza su integridad, produciendo los mismos efectos que las leyes procesales le otorgan a la prueba documental. Este instrumento surge debido a la incertidumbre que generaba la firma manuscrita en los documentos físico papel: ¿cómo verificar si la firma manuscrita es válida y, por ende, el documento no fue manipulado? De ahí que este tipo de firma es equivalente e incluso superior a la rúbrica tradicional(27), ya que utiliza procesos más complejos de seguridad y verificación. Esta se posiciona como el tipo de firma más segura y moderna en los últimos tiempos, pues reduce el riesgo de alteración de la información contenida en los soportes informáticos.

Sobre el procedimiento de creación de una firma electrónica, resulta ser una explicación amplia. Falcón (2009), lo describe a través de una serie de pasos; en primer orden, se debe solicitar a una autoridad de certificación los servicios para la firma de un documento electrónico generado a través de alguna aplicación; en segundo lugar, se crean dos claves: una pública y otra privada, esta última, por su naturaleza, debe ser mantenida en incógnito, ya que es la que permite firmar los documentos, así pues, mientras que la clave privada se almacena en el ordenador del usuario y es convocada por aquel cada vez que seleccione la opción "firmar", la otra es de conocimiento público para que el receptor del correo firmado pueda descifrarlo; en tercer lugar, cuando el emisor se dispone a firmar digitalmente el documento utiliza un software, el cual emplea un algoritmo llamado *hash*(28) sobre el documento a firmar, obteniendo un extracto del texto de longitud fija llamado digesto; por último, cuando es recibido el mensaje, se calcula nuevamente el extracto *hash*, comparándose con el bloque de caracteres obtenidos anteriormente, de esa manera, sí coinciden debidamente, se considera que el documento es auténtico, dicho de otro modo, que no ha sufrido manipulación desde que fue enviado por el emisor (p. 427-428).

La firma electrónica proporciona una mayor seguridad jurídica de la información y datos digitales que pueden contener ciertos documentos informáticos. Este alto grado de fiabilidad que proyecta se debe a que: (i) será posible identificar a la persona que emitió el documento, otorgándole seguridad jurídica; (ii) es una tecnología más segura que la firma manuscrita, por lo que suplantar una identidad resulta mucho más compleja; y (iii) otorga validez jurídica a los documentos electrónicos, al igual como una firma manuscrita, según su equivalencia funcional.

Por lo tanto, este instrumento cuenta con altos estándares de seguridad, lo que hace posible reconocer una mejor fiabilidad a dichos documentos electrónicos. No obstante, para garantizar la autenticidad de una prueba electrónica sin firma, se debe practicar un dictamen pericial, que se puede realizar ante el cuestionamiento de la autenticidad o integridad de la prueba o bien como dictamen autónomo. La exposición del informe pericial, el planteo de preguntas por las partes y/o juez, así como las explicaciones del perito serán importantes para que posteriormente sea valorada racionalmente dicha prueba.

3.3.3. ¿El notario puede certificar la prueba informática?

En la tarea por encontrar alternativas viables que mejoren la fiabilidad de las pruebas informáticas, se ha pensado en la posibilidad de la intervención del notario, pero ¿será pertinente su participación en estos tipos de casos? Para desarrollar esta interrogante, sería necesario iniciar por esclarecer ¿cuál es la función de un notario público? En general, se sabe que el notario tiene la competencia de otorgar fe pública y seguridad jurídica a determinados hechos y actos realizados ante él, siendo su intervención muy requerida e indispensable. No obstante, la incertidumbre se presenta cuando se quiere determinar si un notario, dentro de su competencia, puede certificar una prueba de naturaleza electrónica. Con relación a esto, surge ota incógnita: ¿es factible una relación entre el notario y las evidencias digitales?

(27) En los documentos-papel se requiere una firma para identificar al autor del contenido descrito en ellas, estableciéndose procedimientos especiales para "controlar" dicho aspecto. Es por ello que, respecto a los archivos informáticos, según Taruffo (200), se ha dado una solución ante la dificultad de poder firmarlos, reconociendo que la firma electrónica, creada según métodos tecnológicos y jurídicos determinantes, es similar a la firma manuscrita (p. 89).

(28) "Algoritmo matemático con el cual se puede calcular un valor resumen que permite calcular un valor resumen de los datos a ser firmados digitalmente. El resultado es un valor que identifica inequívocamente al documento" (Edelman, 2014, p. 81).

Hoy en día, hay quienes conciben erróneamente que, para acreditar ciertos tipos de prueba informática, por ejemplo, conversaciones por medio de aplicaciones de mensajería instantánea o fotos subidas a redes sociales, únicamente se necesita imprimirlas y llevarlas a certificar con un notario público. A lo mucho, el notario lo que puede hacer es dar fe de los hechos que observa en determinado dispositivo informático. Es decir, puede verificar si cierta información que aprecia en la pantalla coincide con el contenido del documento impreso, pero no podrá determinar, por la falta de conocimientos técnicos, con exactitud si aquella información fue sometida a modificaciones o cambios respecto del primer hecho digital original.

Por lo cual, ¿se puede afirmar que es incorrecto acreditar el valor probatorio de la prueba informática a través de un notario público? Según Llopis (2016), existe la posibilidad que los notarios aporten una prueba electrónica revestida de fe pública, si es que los notarios como los profesionales técnicos (peritos informáticos) confían en aplicaciones y programas, interpretando correctamente los datos que contiene la prueba electrónica (p.19)[29]. En otros términos, el notario podrá asegurar la fiabilidad de la prueba digital, siempre que reciba una capacitación sobre la materia[30].

En síntesis, la certificación del notario de alguna prueba informática únicamente podría dar fe de su apreciación extrínseca del objeto[31], pero no asegura cabalmente su veracidad intrínseca, siendo contraproducente para garantizar su fiabilidad. Sin los conocimientos necesarios, un notario no podrá determinar la validez de este tipo de pruebas. Por el contrario, la persona capacitada para certificar lo que se quiere probar en el proceso es, indudablemente, el experto en la materia, en este caso, el perito informático.

4. Conclusiones

Cada vez más se siguen presentando pruebas informáticas al proceso judicial. A menudo, estas son admitidas, practicadas y valoradas por los jueces sin la ayuda de ningún experto o la aplicación de herramientas tecnológicas que permita garantizar mejor su adecuado análisis. La incertidumbre sobre la autenticidad o falsedad de que su contenido, provoca que a veces sean rechazadas liminarmente o llegado el momento, simplemente sean dejadas de lado en la motivación de la decisión sobre los hechos.

En este estudio se ha puesto de relieve que uno de los aspectos problemáticos de este tipo de pruebas gira en torno a los inconvenientes relativos a la determinación de su fiabilidad. En efecto, debido a su naturaleza especial y alta volatilidad, existe el peligro latente que puedan ser objeto de manipulación, en el sentido de que se puedan modificar o suprimir una parte o el íntegro de su contenido.

La complejidad y vulnerabilidad de estas pruebas no parecen ser razones suficientes para minimizar su importancia o prescindir de su aporte en el acervo de elementos de juicio disponibles en el proceso. Conforme a una valoración racional de la prueba informática, su apreciación individual y conjunta con los demás medios de prueba resultan importantes para la determinación correcta de los hechos que permita justificar externamente una decisión judicial.

Es recomendable que los jueces cuenten con el apoyo de expertos en tal conocimiento especializado (peritos informáticos) o instrumentos idóneos que ayuden a gestionar mejor su grado de fiabilidad. Las pruebas informáticas que posean firmas electrónicas garantizan mejor la seguridad de los datos o información digital que contienen ciertos dispositivos informáticos. En cambio, la certificación otorgada por un notario *per se* es insuficiente para asegurar la autenticidad de su contenido, salvo que tengan la formación tecnológica especializada necesaria para desempeñar esta labor.

(29) De acuerdo con Llopis (2016), si el notario emplea medios informáticos seguros, que estén bajo su control y de su confianza, está en una situación equiparable a cualquier otra empresa generadora de pruebas digitales en cuanto a su admisibilidad, al menos como prueba documental siendo al menos discutible que lo pueda ser como pericial; y, luego, si lo que necesita el Juez es confianza en quien obtiene la prueba, es indudable que el Notario la genera y mucha (p. 24).

(30) Postura contradictoria acerca de la eficacia del notariado electrónico en Canut (2016, p.152-157).

(31) Cabe señalar que, en el Perú, además de la participación del notario en la certificación de las pruebas informáticas, dicha labor también puede ser realizada por los fedatarios juramentados con especialidad en informática, de acuerdo con el Decreto Legislativo 681- Dictan normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto a la elaborado en forma convencional cuanto la producida por procedimiento informáticos en computadoras, cuya certificación −de acuerdo con el artículo 2 de dicho texto normativo− genera efectos legales y mérito probatorio.

Referencias bibliográficas

Abel, X. (2011). La prueba electrónica, en Abel, X. & Picó I Junoy, J. (Direc.), *Serie estudios prácticos sobre los medios de prueba*, *Colección de Formación Continua de la Facultad de Derecho ESADE* (pp. 15-230). Bosch Editor.

Abel, X. & Picó I Junoy, J. (2009). *La prueba pericial*. Barcelona: Bosch Editor.

Alcaíno Arellano, E. (2014). La confiabilidad como estándar para evaluar la calidad de los reconocimientos de imputados. *Política criminal, 9*(8), 564-613.

Arazi, R. (1998). *La prueba en el proceso civil*. Ediciones La Rocca.

Arellano, J. et al (2020). *Estado de la Justicia en América Latina bajo el COVID-19. Medidas generales adoptadas y el uso de TICs en procesos judiciales*. CEJA.JSCA. https://scm.oas.org/pdfs/2020/CP42372TCEJACOVID19.pdf

Asencio, J. & Fernández, M. (Coord.) (2017). *Justicia penal y nuevas formas de delincuencia.* Tirant lo Blanch.

Bentham, J. (1825). *Tratado de las pruebas*. Bossange.

Bueno De Mata, F. (2014). *Prueba electrónica y proceso 2.* 0. Tirant Lo Blanch.

Bueno De Mata, F. (2017). *La prueba electrónica desde una perspectiva internacional*. Tirant Lo Blanch.

Canut, P. (2016). Validez y eficacia procesal de la prueba electrónica. En Oliva León, R. y Valero, S. (Coord.) *La prueba electrónica. Validez y eficacia procesal* (pp. 152-157). Juristas con Futuro.

Carnelutti, F. (1955). *La prueba civil*. Arayú.

Carrasco, S. (2016). La alegalidad o limbo legal de la prueba electrónica, en Oliva, R. y Valero, S. (Coord.) *La prueba electrónica. Validez y eficacia procesal* (pp. 40-49). Juristas con Futuro.

Consejo Consultivo De Jueces Europeos (2011). *Informe 14. Justicia y Tecnologías de Información (TI)*. https://www.poderjudicial.es/cgpj/es/Temas/Relaciones-internacionales/Relaciones-internacionales-institucionales/Europa/Consejo-Consultivo-de-Jueces-Europeos/

Convenio n°185 [Council Of Europe]. Convenio sobre la ciberdelincuencia. 23 de noviembre de 2001. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf.

Cruz, H. (2013). Algunos apuntes en torno a la prueba electrónica, a propósito del Código de Procedimiento Administrativo y Contencioso Administrativo. *Monitor estratégico*, (3), 74-81.

Delgado, J. (2013). La prueba electrónica en el proceso penal. *Diario La Ley* (8167).

Delgado, J. (2016). *Investigación tecnológica y prueba digital en todas las jurisdicciones.* Wolters Kluwer.

Delgado, J. (2016). La valoración de la prueba digital. Concepto, clases, aportación al proceso y valoración. En J. Delgado (Ed.), *Investigación tecnológica y prueba digital en todas las jurisdicciones*. Wolters Kluwer.

De Prada, M. (2016). La prueba digital: una realidad en el proceso civil. En M. Jimeno & J. Pérez (Coord.), *Nuevos Horizontes del Derecho Procesal: libro homenaje al Prof. Er*nesto Pedraz Penalva (pp. 341-357). Bosch Editor.

Devis, H. (2002). Teoría general de la prueba judicial. Temis.

Edelman, H. (2014). La firma electrónica. En C. Galindo (Coord.), Seguridad de la información (pp. 75-88). Universidad San Carlos de Guatemala.

Fairén, V. (1992). Teoría general del derecho procesal. UNAM.

Falcón, E. (2003). Tratado de la prueba. Astrea.

Ferrer, J. (2007). La valoración racional de la prueba. Colección Filosofía del Derecho. Marcial Pons.

Ferrer, J. (2022). La decisión probatoria. En J. Ferrer (Coord.), Manual de razonamiento probatorio (pp. 397-45). Suprema Corte de Justicia de la Nación

Fredesvinda, I. (2007). The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime-Results of a European Study. Journal of Digital Forensic Practice, 1(4), 285-289. https://doi.org/10.1080/15567280701418049

Gascón, M. (2010). Los hechos en el Derecho. Bases argumentales de la prueba. Marcial Pons.

Goldman, A. (1991). Epistemic Paternalism: Communication Control in Law and Society, Journal of Philosophy, 88(3), 113-131. https://doi.org/10.2307/2026984

Goldman, A. & Beddor, B. (2021). Reliabilist Epistemology. En E. Zalta (Ed.), The Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/archives/sum2021/entries/reliabilism

Gosálvez, P. (06 de julio de 2014). WhatsApp, dudoso testigo de cargo. EL PAÍS. https://elpais.com/sociedad/2014/06/27/actualidad/1403886630_918603.html

Instituto Nacional de Estadística e Informática (2018). Estadísticas de las Tecnologías de Información y Comunicación en los Hogares. https://n9.cl/mri7s.

Llopis, J. (2016). Prueba electrónica y notariado. En R. Oliva, S. Valero & A. Dolado (Coord.), La prueba electrónica. Validez y eficacia procesal (pp. 40-49). Juristas con Futuro.

Mason, S. & Seng, D. (Eds.) (2017). Electronic Evidence. University of London Press.

Meneses, C. (2008). Fuentes de prueba y medios de prueba en el proceso civil. Ius et Praxis, (2), pp. 43-86.

Montero, J. (2005). La prueba en el proceso civil, (4ª ed.). Thomson - Civitas.

Oliva, R. & Valero, S. (Coord.) (2016). La prueba electrónica. Validez y eficacia procesal. Juristas con futuro.

Oliva, R. (2016). La prueba electrónica envenenada. En R. Oliva, S. Valero & A. Dolado (Coord.), La prueba electrónica. Validez y eficacia procesal (pp. 50-68). Juristas con Futuro.

Pérez-Tome, S. & Sánchez, M. (2016). Cifrado de WhatsApp y aportación de prueba. En R. Oliva, S. Valero & A. Dolado (Coord.), La prueba electrónica. Validez y eficacia procesal (pp. 50-68). Juristas con Futuro.

Pinto, F. & Pujol, P. (2017). La prueba en la era digital. Marcial Pons.

Pulgar, A. (2016). Alcances generales de la prueba electrónica. Enfoque Derecho. https://www.enfoquederecho.com/2016/11/16/alcances-generales-de-la-prueba-electronica/

Real Academia Española. (s.f.). Confiabilidad. En Diccionario de la lengua española. Recuperado en 18 de junio de 2023, de https://dle.rae.es/confiabilidad?m=form

Real Academia Española. (s.f.). Confiable. En Diccionario de la lengua española. Recuperado en 18 de junio de 2023, de https://dle.rae.es/confiabilidad?m=form

Real Academia Española. (s.f.). Confianza. En Diccionario de la lengua española. Recuperado en 18 de junio de 2023, de https://dle.rae.es/confiabilidad?m=form

Sentís, S. (1979). La prueba. Los grandes temas del Derecho probatorio. Ejea.

Taruffo, M. (2002). La prueba de los hechos. Trotta.

Taruffo, M. (2008). La prueba. Marcial Pons.

Taruffo, M. (2010). Simplemente la verdad. El juez y la construcción de los hechos. Marcial Pons.

Téllez, J. (2008). Derecho Informático. Editorial McGraw Hill.

The Internet Encyclopedia of Philosophy. (s.f.). Reliabilism. Recuperado en 19 de junio de 2023, en https://iep.utm.edu/reliabilism/

Twining, W. (2006). Rethinking Evidence. Exploratory Essays. Cambridge University Press.

Ubertis, G. (2017). Elementos de epistemología del proceso judicial. Trotta.

Vázquez, C. (2015). De la prueba científica a la prueba pericial. Marcial Pons.

Vázquez, C. (2017). El perito de confianza de los jueces. Revista Jurídica Mario Alario D'Filippo, 9(18), 170-200.

Vicente, A. (2016). La prueba digital en la automatización de los procesos jurisdiccionales, en Gómez, C. y Briseño, M. (Coord.), Nuevos paradigmas del derecho procesal (pp. 609-624). UNAM.

Wiener, N. (1950). The human use of human beings. Cybernetics and society. Houghton Mifflin.

Wilson, N. et al. (2021). Proof: the technical collection and examination of electronic evidence en Mason, S y Seng, D. (Eds.), Electronic Evidence and Electronic Signatures (1-50). University of London Press. https://doi.org/10.14296/2108.9781911507246

Zagsebski, L. (2009). Confianza epistémica y conflicto epistémico. Diánoia, (62), 27–45..