DOSSIER ESPECIAL

EL DESAFÍO DE LA PRUEBA ELECTRÓNICA EN EL PROCESO JUDICIAL

La inteligencia, la tecnología y la experiencia profesional necesarias para obtener respuestas confiables.

the answer company™
THOMSON REUTERS®

El futuro del Derecho es hoy, ya está definido por varios cambios sorprendentes en la rutina del Poder judicial y de la administración de los estudios jurídicos.

Ya es posible hablar de ellos con cierto aprendizaje y no como tendencias legales lejos de consolidarse: expediente electrónico, notificaciones procesales automáticas, smart contracts, data privacy, ciberseguridad y derecho Fintech, son solo algunos de los conceptos que los abogados ya deben incorporar a su rutina.

En este Dossier Especial, nos enfocaremos específicamente en la **prueba electrónica:** ¿Qué es la prueba electrónica? ¿Qué valor probatorio tiene? ¿Cómo se preserva? ¿Qué datos se deben consignar en la demanda? ¿Qué es una firma electrónica?, son algunas de los interrogantes que destacados especialistas analizan para dar respuesta a los desafíos diarios que asechan a los profesionales del Derecho, en un momento de transformaciones y avances tecnológicos en los que nadie puede quedar afuera.

Índice

LA EXTRACCIÓN DE PRUEBA ELECTRÓNICA DE TELÉFONOS CELULARES Y LA GARANTÍA DE DEFENSA EN JUICIO

Por Carla Paola Delle Donne(*)

I. Introducción. — **II.** Las leyes procesales y el secuestro de dispositivos electrónicos. — **III.** La cadena de custodia y la prueba digital. — **IV.** La extracción de la prueba digital y el hash: un acto definitivo e irreproducible para el Código Procesal Penal de la Nación. — **V.** Consideraciones sobre la resolución comentada. — **VI.** Conclusión.

I. Introducción(**)

El 20 de septiembre de 2019, la sala IV de la Cámara Nacional de Apelaciones en lo Criminal y Correccional resolvió confirmar la decisión del juez de instrucción que había rechazado el planteo de nulidad contra la medida que dispuso la copia forense de dos teléfonos celulares secuestrados sin que se notificara a las defensas. Según se señala en la resolución comentada, los agravios introducidos por el único apelante que mantuvo el recurso estuvieron dirigidos a cuestionar la validez de la "manipulación del teléfono sin intervención de la defensa". Durante la audiencia prevista en el art. 454 del Cód. Proc. Penal de la Nación, la defensa agregó que, al no poder asegurar la preservación de la cadena de custodia, la inmutabilidad de la evidencia digital no podía garantizarse y esa circunstancia permitía objetar su valor probatorio.

A los efectos de fundamentar la decisión, los magistrados que integran la sala IV entendieron, por una parte, que "la apertura de los teléfonos celulares es equivalente a la obtención de una copia de la información de los datos almacenados en el dispositivo mencionado". Por otro lado, expresaron que la copia forense de la información almacenada en los teléfonos celulares fue una "operación realizada por la Dirección de Inteligencia de la Policía de la Ciudad" que no constituyó un peritaje en los términos del art. 253 del Cód. Proc. Penal de la Nación — o de los arts. 167 y ss. del Cód. Proc. Penal Fed.(1) —, sino que se trató de una medida ordenada para preservar la prueba contenida en los teléfonos celulares secuestrados, según lo dispuesto en el art. 233 del Cód. Proc. Penal de la Nación, que faculta al juez a obtener copias o reproducciones de las cosas secuestradas a los efectos de preservar la cadena de custodia. En ese orden de ideas, consideraron que resultaba aplicable, como "pauta interpretativa", el art. 151 del Cód. Proc. Penal Fed., que autoriza la incautación de datos a través del registro de un sistema informático o de un medio de almacenamiento de datos informáticos o electrónicos.

Además, afirmaron que la validez del acto no se encuentra sujeta a la notificación de la defensa, ya sea que la copia digital de la prueba almacenada en los teléfonos celulares secuestrados implique el examen de documentos, de la copia o el examen de comunicaciones personales realizada por la policía en calidad de auxiliar de la justicia de acuerdo con el art. 236, párr. 2º, Cód. Proc. Penal de la Nación, que citó el juez de instrucción para fundamentar la medida, para luego argumentar que ese acto procesal no afectó garantía constitucional alguna, toda vez que la actuación policial respondió a una orden del juez natural de la causa llevada a cabo en virtud de lo dispuesto en el art. 184, inc. 4º del Cód. Proc. Penal de la Nación, que establece que las fuerzas de seguridad tendrán atribuciones, en cuanto aquí interesa, para rea-

lizar exámenes técnicos siempre que hubiera peligro de que cualquier demora comprometa el éxito de la investigación, y en el art. 233 del Cód. Proc. Penal de la Nación, que dispone que el juez puede ordenar copias o reproducciones de las cosas secuestradas cuando aquellas puedan desaparecer, alterarse, sean de difícil custodia o convenga a la instrucción.

Con relación al planteo que efectuó la defensa sobre el valor probatorio de la prueba, los magistrados sostuvieron que la "eventual alteración de los datos incorporados constituye una mera conjetura" y que los dispositivos podían ser peritados para establecer si se habían modificado los datos originales.

Por otro lado, agregaron que se activó el modo avión de los teléfonos celulares a fin de que no recibieran o emitieran datos y que, luego, fueron conectados a un ordenador para duplicar el contenido a través del software UFED 4PC. Por ese motivo, los jueces entendieron que no existió irregularidad alguna en la manipulación de los dispositivos electrónicos.

Para concluir, afirmaron que el planteo de la defensa introducía una nulidad por la nulidad misma, ya que no había demostrado un perjuicio real y concreto; que no se afectó el derecho de defensa y que "los planteos de las partes se vinculan a cuestiones de entidad probatoria que escapan al análisis de la validez de los actos procesales, que solo procede en caso de que no pueda ser ponderada otra interpretación posible que armonice con las garantías fundamentales".

Ahora bien, la resolución que se comenta refleja un tema de vital actualidad que requiere de especial atención, porque la motivación desarrollada desatiende conceptos fundamentales sobre la extracción y preservación de la prueba digital[(2)]. La arbitrariedad en la que incurren los magistrados al fundamentar la decisión a través de argumentos aparentes y la inobservancia de las normas procesales aplicables al caso convocan a la reflexión acerca de la necesidad de respetar las formalidades procesales a los fines de garantizar el pleno ejercicio del derecho de defensa cuando la prueba del caso involucra la recolección, extracción y preservación de evidencia digital.

Antes de efectuar mis apreciaciones sobre la decisión, estimo ineludible establecer los parámetros normativos y conceptuales que sustentarán mis reflexiones acerca de la resolución y las conclusiones a las que arribo. Entonces, en primer lugar, reseñaré las normas procesales vigentes y aplicables del Código Procesal Penal de la Nación y del Código Procesal Penal Federal para extracción de prueba digital de teléfonos celulares secuestrados en casos en trámite ante la justicia penal nacional y federal. En segundo lugar, haré referencia a las definiciones conceptuales que son imprescindibles a los efectos de comprender las particularidades que reviste la recolección, la extracción y la preservación de la prueba digital. En particular, analizaré el concepto de cadena de custodia de la prueba digital y las características de ese tipo de evidencia para, luego, examinar las definiciones de hash o valor hash y los motivos por los cuales la extracción de prueba digital es un acto definitivo e irreproducible. Sentadas esas bases, el estudio de la resolución será una tarea más sencilla, puesto que las conclusiones se desprenderán naturalmente de la conjunción de la ley procesal aplicable y de los conceptos explicados.

II. Las leyes procesales y el secuestro de dispositivos electrónicos

El Código Procesal Penal de la Nación no establece medidas de prueba especiales para el secuestro de dispositivos electrónicos, la extracción de la prueba digital allí almacenada y la preservación de la cadena de custodia que debe comenzar en el mismo momento de la incautación. Sin embargo, frente a las inocultables consecuencias que apareja la revolución tecnológica que, en materia de investigación penal, se traduce en la necesidad de incorporar prueba digital al proceso, pueden invocarse dos soluciones previstas en las reglas procesales vigentes que no plantean objeciones constitucionales o de validez de la prueba.

El Código Procesal Penal de la Nación establece el principio de libertad probatoria en el art. 206. Ese principio, que el legislador optó por restringir únicamente en materia de prueba del estado civil de las personas, implica que, a los efectos de la investigación, puede ordenarse toda medida de prueba que resulte conducente y que guarde relación directa con el objeto procesal de la pesquisa.

A su vez, el mismo cuerpo normativo establece un catálogo de medios de prueba que no constituyen una enumeración taxativa, sino que pueden ser ampliados en la medida en que resulten adecuados para determinar la verdad jurídica objetiva de un hecho delictivo. La aplicación analógica de las reglas procesales sobre secuestro de cosas relacionadas con el delito, las sujetas a decomiso o aquellas que puedan servir como medios de prueba permite válidamente incorporar ese tipo de prueba al proceso penal y asegurar su cadena de custodia (art. 231 y ss. del Cód. Proc. Penal de la Nación).

La posibilidad de aplicar analógicamente disposiciones procesales y su discutible constitucionalidad escapan del objeto del presente comentario. No obstante esa observación, considero plenamente aplicables las leyes procesales vigentes a la recolección de un tipo de prueba que no existía como tal en la época en la que se sancionó el Código Procesal Penal de la Nación. Es por esa razón que, como punto de partida del estudio del tema propuesto, resulta inevitable la adecuación

normativa de las disposiciones sobre secuestro de cosas para el secuestro de dispositivos electrónicos y la preservación de la cadena de custodia de prueba digital con el alcance que autoriza el art. 206 del Cód. Proc. Penal de la Nación.

Distintas son las disposiciones del Código Procesal Penal Federal vigente en las jurisdicciones de Salta, Jujuy, Mendoza y Santa Fe[3] y parcialmente vigente para la justicia penal federal del resto del país y de la justicia nacional de la Ciudad de Buenos Aires[4], que el tribunal invoca como "pauta interpretativa" del Código Procesal Penal de la Nación. Así, pues, el Código Procesal Penal Federal —aunque no es todo lo innovador que podría haber sido en materia de prueba informática e investigación por medios informáticos[5]— establece normas específicas y concretas para el secuestro de prueba informática. En efecto, el art. 151 del Cód. Proc. Penal Fed., prevé la incautación de datos que solo procede por orden judicial a pedido de parte. El registro de un sistema informático, de una parte de este o de un medio de almacenamiento de datos informáticos o electrónicos que puede involucrar el secuestro del dispositivo o de partes del dispositivo, así como la copia de datos o elementos de interés para la investigación, en los términos establecidos en esa disposición, deben llevarse a cabo de acuerdo con las reglas previstas en el art. 136 del Cód. Proc. Penal Fed., que, en cuanto aquí interesa, disponen que la diligencia deberá documentarse en un acta firmada por dos testigos. Será luego tarea del fiscal proceder a la apertura y el examen de los objetos secuestrados (art. 152 en función del art. 151 del Cód. Proc. Penal Fed.).

Sentados los parámetros normativos aplicables al secuestro de dispositivos electrónicos, resta efectuar algunas precisiones más técnicas relativas a la cadena de custodia de la prueba digital, para luego analizar de la resolución comentada.

III. La cadena de custodia y la prueba digital

La cadena de custodia es el procedimiento que permite garantizar que la prueba recogida es la misma que será objeto de examen pericial y que luego se presentará como elemento de prueba en el juicio. Preservar la cadena de custodia en el proceso penal es esencial, porque permite demostrar que la evidencia digital recolectada, extraída, preservada y analizada se mantuvo inalterada en todas esas etapas, es decir, que la prueba es siempre la misma. Además, permite identificar a los oficiales de las fuerzas de seguridad que intervinieron en el secuestro, las herramientas informáticas que se utilizaron para extraer la prueba digital del dispositivo electrónico en el caso que no se hubiera podido secuestrar el dispositivo o que la extracción de la prueba se realice después del secuestro y antes del peritaje —tal como sucedió en el caso comentado—, el método utilizado a esos efectos, así como también permite identificar a los peritos que la analizaron.

La cadena de custodia es esencial en todo proceso penal porque hace a la confiabilidad, autenticidad, identidad e integridad de la prueba. Asegurar la cadena de custodia implica, en esos términos, que la prueba es válida, que su valor probatorio no puede ser cuestionado y que tampoco puede ser eliminada por aplicación de las reglas genéricas de exclusión probatoria por encontrarse viciada de nulidad, al menos en lo que al secuestro, la extracción y la preservación se refiere.

Entonces, ¿cómo se aplican estas reglas genéricas de preservación de la prueba a la prueba digital?

La prueba digital es todo dato o información generada por un sistema informático que se encuentra almacenada en dispositivos informáticos. La prueba digital, que puede categorizarse como prueba documental, se obtiene y se preserva de un modo diferente a todo otro tipo de evidencia porque está almacenada en un soporte electrónico. Esa circunstancia implica que la prueba electrónica tiene características particulares que exigen que las fuerzas de seguridad que intervenga en la extracción de la prueba digital cuenten con los conocimientos especiales para no contaminarla y las herramientas forenses necesarias a los fines de asegurar la recolección pertinente, la extracción correcta y la preservación adecuada.

Para comprender la relevancia del primer acto de extracción de la prueba digital, debe considerarse que la prueba informática tiene características propias. La prueba digital es volátil, alterable o modificable y fácilmente duplicable.

La volatilidad es una de las características más relevantes de la evidencia electrónica y debe interpretarse en términos de inestabilidad de la prueba. La evidencia digital tiene una capacidad amplia y fácil de transformarse y si no se toman los recaudos necesarios, puede eliminarse total e inmediatamente. La posibilidad de que eso suceda significarían que la prueba pierda valor probatorio o que desaparezca por complemento como evidencia de un hecho delictivo.

Esa característica lleva ínsita otras dos características: la prueba digital también es fácilmente alterable y hasta eliminable, ya que puede modificarse o borrarse con una sola operación y solo se puede recuperar a través de herramientas forenses adecuadas y el conocimiento especial.

Asimismo, la prueba digital es también de fácil reproducción o copiado y, aunque esa característica puede ser una ventaja a los fines probatorios porque se pueden efectuar tantas copias como resulte necesario, el personal de las fuerzas de

seguridad encargado del secuestro debe contar con los conocimientos informáticos suficientes para no adulterar o contaminar la información digital. Además, esa ventaja puede poner en riesgo la autenticidad y la integridad de la prueba. Es que si en el primer acto de extracción no se obtuvo el valor hash o hash —concepto al que haré referencia en el acápite siguiente—, la validez de la extracción de la prueba digital se pone en juego si no se puede asegurar que la prueba extraída no se adulteró, es decir, si no se puede garantizar que la prueba extraída es la misma que se encontraba almacenada en el dispositivo electrónico que se secuestró o al que se accedió en el procedimiento. Y si no puede corroborarse que la prueba extraída es toda la información original que existía almacenada en el dispositivo electrónico o que es toda la prueba obtenida durante el allanamiento, no puede garantizarse su integridad y autenticidad. La prueba así obtenida pierde su confiabilidad y, en consecuencia, no solo podría cuestionarse su valor probatorio sino también su validez.

Los distintos dispositivos electrónicos existentes a la fecha y la capacidad de almacenar prueba, por ejemplo, en la nube —o servidores de almacenamiento de datos electrónicos y programas que se accede a través de internet— plantean escenarios diversos que impiden hacer generalizaciones sobre las buenas prácticas aplicables en el secuestro de prueba digital. No es lo mismo incautar un teléfono móvil que secuestrar los racks de sistemas informáticos de una empresa privada o de un organismo del Estado y luego extraer la prueba. La posibilidad de incautar grandes volúmenes de información electrónica no requiere de la misma planificación que la extracción de información de una computadora personal o de un teléfono. Es por ese motivo que las investigaciones que involucran la incautación de prueba digital exigen una planificación previa que permita determinar, por ejemplo, qué herramientas informáticas serán necesarias, qué tipo de información se buscará, cómo se realizará esa búsqueda, si se secuestran los dispositivos electrónicos o si se realizara al extracción de la prueba digital en el lugar y, en ese caso, si se realizan imágenes forenses de toda la información digital o se realiza un digital forensic triage o selección de la prueba digital por muestreo forense, así como también será necesario contar con personal de las fuerzas de seguridad especializado en la materia y operadores de justicia que tengan conocimientos suficientes para tomar esas decisiones.

Esos distintos escenarios de extracción de la prueba que presentan diversos niveles de complejidad comparten el mismo requisito para identificar la evidencia extraída en la primera extracción: **el hash o huella digital.**

IV. La extracción de la prueba digital y el hash: un acto definitivo e irreproducible para el Código Procesal Penal de la Nación

El secuestro de teléfonos celulares debe documentarse en el acta correspondiente y requiere la presencia de dos testigos, según lo establecen el art. 138 del Cód. Proc. Penal de la Nación y el art. 110 del Cód. Proc. Penal Fed. Por lo general, o en la práctica así debería realizarse, el personal de las fuerzas de seguridad no puede acceder a la información almacenada en el dispositivo electrónico durante el secuestro efectuado como consecuencia de un allanamiento o de una requisa personal debidamente fundamentados[(6)]. La información allí almacenada solo puede ser extraída mediante la orden judicial pertinente que así lo disponga. La extracción de la información permitirá el análisis de la prueba incautada para, luego, incorporar solo aquella que resulte pertinente al objeto procesal de la investigación[(7)].

En el caso de secuestro de teléfonos móviles la evidencia física es el teléfono y la evidencia digital es la información allí contenida que debe extraerse para peritarse. En la práctica, por lo general, se extrae la totalidad de la información allí almacenada y se preserva en un dispositivo portátil de almacenamiento de datos (p. ej., discos rígidos extraíbles, discos de memoria USB conocidos, en nuestro país, como pendrive). La obtención de la prueba electrónica se realiza mediante la utilización de herramientas forenses adecuadas que preserven la autenticidad y la integridad de la prueba almacenada en un dispositivo electrónico, denominadas bloqueadores de escritura.

En el caso que se comenta, la Dirección de Inteligencia de la Policía de la Ciudad utilizó UFED 4PC[(8)] para realizar el clonado de la información digital almacenada en el teléfono celular secuestrado. UFED 4PC es una herramienta informática para la extracción segura de información almacenada en dispositivos móviles o teléfonos celulares y no solamente un software. Sencillamente explicado, se trata de una herramienta forense que se coloca entre el puerto del dispositivo secuestrado y el puerto del ordenador que, a través de un software, se encargará de extraer la prueba sin alterarla y permitirá almacenarla en el soporte en el que se copiará.

A través de ese tipo de herramientas forenses se realiza el clonado de la prueba. Clonar un dispositivo electrónico implica efectuar una imagen en espejo o mirror image, es decir, realizar una copia que duplica la información bit a bit. El clonado es, entonces, la reproducción o copia de la totalidad de la información original almacenada en el dispositivo electrónico.

En la etapa de extracción de la prueba surge uno de los conceptos más relevantes en materia de prueba digital: el valor hash. El valor hash o, simplemente, hash, es la cadena de caracteres de longitud fija que resulta del procesamien-

to de un archivo digital representada en un algoritmo que crea un valor único[9]. Ese algoritmo permite identificar, de manera indudable, que la prueba extraída es exactamente la misma que se encontraba almacenada. Entonces, si esa prueba se modifica cambian los bits de los archivos originales, cambia el cálculo del hash y, en consecuencia, la cadena o algoritmo no es la misma.

En otras palabras, el hash es la huella digital de la información electrónica que permite comprobar que no se alteró la prueba original y que, en consecuencia, asegura la autenticidad e integridad de la prueba digital. El hash constituye el rastro principal que identifica a la prueba y que posibilita verificar que esa evidencia contenida en el dispositivo secuestrado es la misma que se encontraba almacenada en el momento del secuestro y que es exactamente la misma que se extrajo y que, luego, se examinará. Es por ese motivo que el hash debe mantenerse inalterado desde el primer momento de identificación de la prueba hasta su presentación en el juicio.

Para que la extracción de la prueba sea un acto procesal válido, debe registrarse el primer hash obtenido. La documentación del primer hash es un acto de gran trascendencia a los efectos de la identificación de la prueba, porque, si bien es cierto que la extracción de la prueba se puede repetir indefinidamente mediante la utilización de las herramientas forenses que impidan que se modifique la prueba, no menos cierto es que si las partes no fueron notificadas de la realización de ese acto nunca podrán controlar que el primer acceso al dispositivo secuestrado se efectuó siguiendo las buenas prácticas sobre extracción de la evidencia digital, no podrán corroborar que el hash obtenido corresponde al valor que tenía la prueba en el momento del secuestro, así como tampoco podrán verificar que la prueba no fue contaminada. Es decir, si las partes del proceso no fueron notificadas de la medida de extracción de información digital de un teléfono celular secuestrado podrían no solo cuestionar su valor probatorio, sino también plantear la nulidad del acto porque, aunque la extracción se repita, no tendrían forma de corroborar que el primer hash corresponde a una extracción no viciada. Solo podrían confirmar que el hash de una nueva y posterior extracción coincide con el primer hash, pero eso no asegura que ese primer hash sea el valor que arrojó la primera extracción.

Lo expuesto anteriormente demuestra que la extracción de la información de todo dispositivo electrónico, en los términos del Código Procesal Penal de la Nación, es una medida única e irreproducible y que la forma de documentar el acto varía según el momento en que se realice: si se efectúa durante el procedimiento se realizará en presencia de testigos y si se lleva a cabo en un momento posterior deberá realizarse en presencia de la defensa.

En otras palabras, el acto procesal bien podría formalizarse mediante acta si la extracción de la evidencia digital la realizan funcionarios de la policía o de las fuerzas de seguridad con la presencia de dos testigos (art. 138 del Cód. Proc. Penal de la Nación y art. 110 del Cód. Proc. Penal Fed.), pero la práctica informa que, en el caso de secuestros de teléfonos celulares, la extracción de la prueba se realiza en una etapa posterior. Por lo tanto, en ese caso corresponde aplicar las reglas establecidas en el art. 200 del Cód. Proc. Penal de la Nación, que establece que los defensores de las partes tendrán derecho a asistir a todos los actos que por su naturaleza y sus características se deban considerar definitivos e irreproducibles y, en las jurisdicciones en las que se encuentra vigente, resulta aplicable el art. 151 del Cód. Proc. Penal Fed., que establece reglas específicas sobre incautación de datos informáticos o electrónicos. Los términos del nuevo ordenamiento procesal federal son más precisos a pesar de que la redacción del art. 151 exige la remisión a las disposiciones relativas a las inspecciones (art. 136 del Cód. Proc. Penal Fed.), la requisa (art. 137 del Cód. Proc. Penal Fed.), el secuestro de documentos (art. 148 del Cód. Proc. Penal Fed., que a su vez dispone que en ese caso se aplican las reglas para la requisa y el registro), y a la apertura y examen de correspondencia (art. 152 del Cód. Proc. Penal Fed.). En cuanto aquí interesa, el art. 151 del Cód. Proc. Penal Fed. establece que, cuando existiera motivo suficiente y fundado para presumir que se encontrarán elementos útiles para la investigación, se puede ordenar el registro de un sistema informático, de una parte de este o de un medio de almacenamiento de datos informáticos o electrónicos. Esa medida tiene como objeto secuestrar los dispositivos electrónicos y sus componentes periféricos, copiar los datos o preservarlos, tareas que deben documentarse mediante actas en la presencia de dos testigos que no pertenezcan a las fuerzas de seguridad que llevó a cabo el procedimiento y, adicionalmente, por otro medio idóneo que garantice su inalterabilidad y fidelidad (art. 136 del Cód. Proc. Penal Fed., requisitos que también disponen el art. 137 y art. 148 del Cód. Proc. Penal Fed.).

El Código Procesal Penal Federal resuelve con mayor claridad la incautación de datos informáticos y la copia de toda la información electrónica extraída de los dispositivos incautados en cuanto establece que esos actos deben documentarse en actas y deben realizarse ante dos testigos. Distintas son las disposiciones del Código Procesal Penal de la Nación, que autoriza la obtención de copias o reproducciones de las cosas secuestradas cuando éstas puedan desaparecer, alterarse, sean de difícil custodia o convenga así a la instrucción (art. 233 del Cód. Proc. Penal de la Nación). Sin embargo, esa facultad que puede ejercer el juez de instrucción para preservar la cadena de custodia debe contemplar el derecho de la defensa de asistir a todo acto definitivo e irreproducible (art. 200 del Cód. Proc. Penal de la Nación). Las formas que prevé el Código Procesal Penal de la Nación son claramente diferentes a las establecidas en el nuevo Código Procesal

Penal Federal. El código de rito que será reemplazado en los próximos años, todavía exige que se notifique a la defensa la realización de todo acto definitivo e irreproducible (art. 200 del Cód. Proc. Penal de la Nación) y la primera extracción de la prueba digital de un dispositivo electrónica reviste ese carácter.

V. Consideraciones sobre la resolución comentada

Las reglas procesales y las definiciones conceptuales anteriormente expuestas son indispensables para comentar la resolución porque ofrecen el marco teórico en el que se enmarca el agravio de la defensa y la respuesta jurisdiccional. Estimé oportuno efectuar esas apreciaciones ya que, tal como anticipara, entiendo que la decisión comentada no se asienta en la normativa procesal aplicable al caso, desatiende las características especiales de la prueba digital y su extracción de dispositivos electrónicos y, en consecuencia, afecta el derecho de defensa en juicio que invocó el apelante en su recurso y en la audiencia.

En efecto, la errónea aplicación de la ley procesal en la que incurren los magistrados al dictar la resolución comentada es consecuencia de desentender la relevancia que tiene el momento en el que se extrae prueba digital de un dispositivo electrónico y, en definitiva, de desconocer que se trata de un acto irreproducible. Desde ese punto en adelante, todos los argumentos desarrollados en la resolución son fundamentos aparentes que resultan opuestos al real ejercicio del derecho de defensa cuyo cumplimiento reclamaba la defensa en sus agravios.

En primer lugar, cabe señalar que los argumentos de la decisión comentada requerían de la interpretación armónica de los arts. 200 y 206 y el art. 233 del Cód. Proc. Penal de la Nación único vigente y aplicable al caso. La libertad probatoria prevista en el art. 206 del Cód. Proc. Penal de la Nación, sumada a la aplicación analógica de las reglas procesales previstas para el secuestro de objetos y la preservación de la cadena de custodia para el secuestro de dispositivos electrónicos en los términos establecidos en el art. 233 del Cód. Proc. Penal de la Nación, en este caso, de teléfonos celulares y la posterior extracción de prueba digital, exigen, al mismo tiempo, el cumplimiento de restantes disposiciones de ese ordenamiento a los efectos de asegurar el debido ejercicio del derecho de defensa. La interpretación armónica del ordenamiento procesal vigente y, en definitiva, insisto, el que resultaba aplicable al caso —me refiero al Cód. Proc. Penal de la Nación— requería notificar a la defensa para que tuviera la opción de asistir a un acto definitivo e irreproducible en los términos previstos en el art. 200 del Cód. Proc. Penal de la Nación.

Por otro lado, no parece acertada la invocación del art. 151 del Cód. Proc. Penal Fed. como "pauta interpretativa" porque genera confusiones argumentativas. El Código Procesal Penal Federal no es un código vigente para la jurisdicción y, aun si quisiera afirmarse lo contrario, esa disposición resulta perjudicial para la defensa[10] en tanto exige que la obtención de datos electrónicos se realice en presencia de dos testigos ajenos a la fuerza de seguridad, es decir, no concede a la defensa el derecho a asistir a un acto definitivo e irreproducible. Además, si pudiera aplicarse de manera analógica el Código Procesal Penal Federal, ese requisito —la presencia de dos testigos— no se plasmó en ningún pasaje de la decisión. Entonces, pareciera que el art. 151 del Cód. Proc. Penal Fed., solo se citó de manera fragmentada a los efectos de demostrar que el nuevo ordenamiento procesal federal prevé la incautación de datos informáticos sin que se hiciera referencia al cumplimiento de formalidad alguna para la realización del acto procesal que también contempla esa norma.

La resolución comentada cita otras dos disposiciones: el art. 161 y ss. del Cód. Proc. Penal Fed. y el art. 236 del Cód. Proc. Penal de la Nación. El único acierto que se desprende de la decisión comentada es que la extracción de la prueba digital de un teléfono celular no es un peritaje. Y no es un peritaje porque no constituye un examen de la prueba sino la obtención de la prueba. Claro que, tal como sostuve anteriormente, no correspondía citar el art. 161 del Cód. Proc. Penal Fed., sino que era suficiente con la referencia al art. 253 y ss. del Cód. Proc. Penal de la Nación que es la única ley procesal aplicable al caso. En relación con el art. 236 del Cód. Proc. Penal de la Nación aparece un nuevo yerro en la decisión. Esa disposición regula las intervenciones telefónicas que ni siquiera por analogía resultan equivalentes a la extracción de información digital de un teléfono celular.

Las disposiciones del Código Procesal Penal de la Nación eran suficientes para resolver el caso. Utilizar como "pauta interpretativa" las normas relativas al secuestro de datos informáticos del Código Procesal Penal Federal plantea un doble problema; por un lado, echa mano a normas no vigentes para la justicia nacional de la Ciudad de Buenos Aires y, en consecuencia, no aplicables al caso. Por otro lado, y aun de considerarse posible la convalidación de una nulidad a la luz de las disposiciones del Código Procesal Penal Federal sobre incautación de datos informáticos, la resolución nada expresa en relación con el reemplazo de la notificación a la defensa por la presencia de dos testigos que refrendaron el acta que documentó la extracción de la prueba digital. Justificar la extracción de la prueba digital de los teléfonos de ese modo, quizás, se hubiese acercado más a la motivación de la resolución que exige el art. 123 del Cód. Proc. Penal de la Nación para considerarla un acto jurisdiccional válido. Sin embargo, como señalé anteriormente, confirmar la validez

de un acto procesal con reglas procesales sin fuerza de ley no parece un camino que respete la garantía constitucional de defensa en juicio.

La ley procesal aplicable al caso hubiese sido más sencilla de invocar si no se hubiese omitido otorgar la real significación que efectivamente reviste la primera extracción de información digital de un teléfono celular. En ese primer acceso, la posibilidad de contaminar la prueba, lejos de constituir una conjetura de la defensa, es una realidad técnica que fácilmente puede suceder. Sumado a lo expuesto, nos encontramos con el hash que arroja la primera copia de la prueba electrónica que es único e irrepetible. El argumento que desarrollan los magistrados con relación a la posibilidad que tendrán más adelante las defensas de cuestionar el valor probatorio de la prueba extraída no considera que era pertinente no solo cuestionar el valor probatorio, sino que era oportuno plantear la nulidad por no haber podido ejercer su derecho a asistir —o contar con la opción de no asistir— al primer acceso del dispositivo electrónico, tal como lo expresa el tribunal, que implica el clonado de la prueba y la obtención del primer hash.

Sin embargo, los magistrados insisten en señalar que la posible contaminación de la prueba es un argumento "de índole probatorio y conjetural". Y si bien es cierto que podría ser conjetural una posible afectación de la cadena de custodia y que cualquier modificación podría, eventualmente, verificarse mediante un peritaje posterior, cabe preguntarse si es necesario realizar un peritaje para acreditar que la prueba extraída no se alteró, cuando la investigación debería estar dirigida a peritar la información válidamente obtenida. Siempre, claro está, que la prueba fuera obtenida válidamente, y ese es el problema inicial de este caso. Es decir, cómo podría la defensa cuestionar en otra etapa procesal el valor probatorio de una prueba que no lo tiene porque es nula desde el mismo momento de la extracción. Es que lo que no se considera en la resolución comentada es que la autenticidad y la integridad de la prueba no se encuentran únicamente relacionadas con la utilización de las buenas prácticas en la recolección de prueba digital que informan que es indispensable la utilización de herramientas forenses adecuadas, tal como UFED 4PC, para asegurar la cadena de custodia y, por lo tanto, la confiabilidad de la evidencia. Es necesario, a la luz de las reglas previstas en el Código Procesal Penal de la Nación, notificar a la defensa del acto en el que se accederá por primera vez a toda la información almacenada en el teléfono celular.

El valor hash se obtiene la primera vez que se extrae la prueba electrónica. Ese acto de vital importancia es el primer acceso al dispositivo en el que se encuentra almacenada la prueba y es en ese momento en el que se obtendrá el hash o la huella digital de la información electrónica. La obtención del hash es determinante para comprobar que la prueba almacenada no se alteró y que, en consecuencia, su autenticidad e integridad no pueden cuestionarse. Entonces, mal podía convalidarse el acto cuando la defensa no tuvo la oportunidad de elegir si asistía o no a un acto eminentemente irreproducible. Es que, si bien es cierto que, tal como se señaló, ese acto podría volver a reproducirse innumerable cantidad de veces, no menos cierto es que si en el primer acto en el que se accede por primera vez a la información digital —que, una vez examinada, puede transformase en prueba de cargo o de descargo— no estuvo presente la defensa, el acto procesal de extracción de la prueba digital de los teléfonos celulares no es un acto válido. Solo si la defensa decide no asistir, encontrándose debidamente notificada, tendrá posibilidad de cuestionar el valor probatorio de la prueba, p. ej., argumentando que no se adoptaron las buenas prácticas en materia de prueba digital o que no se preservó la cadena de custodia y que, por esos motivos, la prueba no es confiable como tal porque podría haberse alterado o eliminado.

Por otra parte, considero que los magistrados no tuvieron en cuenta que la extracción de la información almacenada en el teléfono celular implica no solo acceder a posibles elementos de prueba relacionada con el delito, sino que también involucra la posibilidad de conocer toda la vida de una persona. En la actualidad los teléfonos celulares son pequeñas computadoras que sirven para comunicarse telefónicamente y permiten almacenar gran cantidad de información personal privada. Esas consideraciones fueron claramente analizadas en dos precedentes resueltos por la Corte Suprema de los Estados Unidos: "Riley vs. California"[(11)] y "US vs. Wurie"[(12)] (2014), en los que se analizaron los límites a la injerencia estatal cuando se arresta a una persona a la que se le secuestra su teléfono celular. El holding del caso no coindice con el planteo medular de la resolución comentada puesto que en esos casos se analizó si es necesaria una orden judicial para acceder a la información almacenada en el teléfono celular incautado a una persona arrestada, y en el caso comentado existió una orden judicial para acceder a los dispositivos electrónicos. Sin embargo, el examen que allí se realiza con relación al equilibrio que debe existir entre el poder de policía del Estado y el derecho a la privacidad por la cantidad de información almacenada en los teléfonos celulares es aplicable a la decisión comentada a fin de comprender por qué es necesaria la notificación a la defensa de la extracción de la prueba digital de los teléfonos celulares (que también debería haberse contemplado en el art. 151 del Cód. Proc. Penal Fed., que solo exige la presencia de dos testigos).

En los fallos de la Corte Suprema de Estados Unidos, el voto que lidera el acuerdo introduce el tema con una descripción de la realidad risueña en la que se sostiene que los teléfonos celulares *"en la actualidad, son hasta tal punto una parte omnipresente e insistente de nuestra vida diaria que un visitante proverbial proveniente de Marte podría concluir que*

son una característica importante de la anatomía humana". Agrega que "antes de los teléfonos celulares, la requisa de una persona estaba limitada a realidades físicas y tendían a constituir únicamente a una limitada intromisión de la privacidad como un tema general" y que "antes de la vida digital, las personas no llevaban consigo una provisión de datos personales sensibles mientras andaban por allí en su día". Y destaca que la información que pueden revelar los teléfonos celulares es mucho mayor que la que puede obtenerse de la prueba documental, física porque allí se puede almacenar en el mismo lugar todo tipo de información personal: notas, recetas médicas, fotos, videos, archivos, cuentas bancarias, cuentas de correo electrónico, aplicaciones de mensajería y redes sociales que permitirían reconstruir la vida de una persona a través de imágenes y videos que indican fechas, lugares y descripciones que se remontan a fechas aun anteriores a la adquisición del teléfono.

En consideración del avance a la esfera de la privacidad de la persona que implica obtener información almacenada en un teléfono celular para luego utilizarla como prueba, aunada a la posibilidad que existe de alterar esa información, parecería razonable que la defensa, a los efectos asegurar el cumplimiento de las garantías constitucionales de debido proceso y defensa en juicio, hubiese contado con la opción de asistir o no a la extracción de la prueba del teléfono celular tras recibir la notificación de la realización de un acto procesal notoriamente irreproducible.

VI. Conclusión

La autenticidad y la integridad de la evidencia electrónica son características esenciales que debe preservar la prueba a lo largo de todo el proceso penal. Esas características indican que la información no se adulteró en ninguna de sus particularidades y propiedades y que, en consecuencia, se mantiene en el estado original en el que se encontraba cuando se secuestró. Para que la evidencia digital tenga eficacia probatoria y permita que a través de su valoración los jueces elaboren su convencimiento acerca de la comisión o no de un hecho delictivo, debe asegurarse la cadena de custodia. La preservación de la prueba a través de la cadena de custodia asegura que la prueba es la misma que se secuestró y que no se alteró durante la extracción, en el examen pericial o en ninguna etapa de la instrucción del caso hasta su presentación en el juicio. Ese objetivo se alcanza a través de la aplicación de las buenas prácticas en la recolección de evidencia digital que requiere que tanto el personal de las fuerzas de seguridad como los peritos intervinientes cuenten con el conocimiento suficiente y utilicen las herramientas informáticas forenses apropiadas.

Sin embargo, esos recaudos no son suficientes a fin de resguardar la garantía constitucional de defensa en juicio. En efecto, para asegurar el pleno ejercicio del derecho de defensa del imputado, a la luz de las disposiciones previstas en el Código Procesal Penal de la Nación, es necesario que se notifique a la defensa de la realización de la medida de prueba en la que se extraerá la prueba digital y se obtendrá el hash que permitirá asegurar que a lo largo del proceso que la prueba será siempre la misma, tal y como debe realizarse con todo acto único e irreproducible de la investigación.

En la resolución comentada, no resultaba aplicable el Código Procesal Penal Federal; si ese hubiese sido el caso, los magistrados tenían que verificar únicamente que la extracción de la prueba digital se llevó a cabo en presencia de dos testigos. Las reglas de ese ordenamiento procesal son claras y, más allá de la inconveniente remisión a cuatro disposiciones distintas, el texto del art. 151 del Cód. Proc. Penal Fed. es preciso sobre el modo en el que debe realizarse la incautación de datos informáticos. Tan claras como son las reglas procesales del Código Procesal Penal de la Nación que, en este caso no se cumplieron porque, insisto, se omitió considerar el primer acto de extracción de prueba digital como un acto irreproducible, que trajo como consecuencia necesaria la errónea aplicación del Código Procesal Penal de la Nación, en particular, de los arts. 200 y 233, que torna la decisión en un acto jurisdiccional inválido en abierta afectación al ejercicio del derecho de defensa en juicio.

La conclusión a la que arribo, lejos de ser rigorista, implica adecuar la perspectiva de la investigación al escenario digital actual, que tiene características propias que deben ser conocidas por las fuerzas de seguridad y por empleados, funcionarios y magistrados judiciales. Esa pareciera ser la única forma de asegurar el pleno ejercicio del derecho de defensa.

Este artículo se encuentra publicado en LA LEY 12/02/2020, 12/02/2020, 8. **Cita Online:** AR/DOC/89/2020

(*) Abogada de la Universidad de Buenos Aires; especialista en Derecho Penal y Ciencias Penales de la Universidad del Salvador; Master of Laws (LL.M) in International Crime and Justice que la Universidad de Torino dictada junto con United Nations Interregional Crime and Justice Research Institute (UNICRI); secretaria en la Procuraduría de Crímenes Económicos y Lavado de Activos.

(**) "... la idea de justicia impone que el derecho de la sociedad a defenderse contra el delito sea conjugado con el del individuo sometido a proceso, en forma que ninguno de ellos sea sacrificado en aras del otro, procurando de esa manera conciliar el derecho del individuo a no sufrir persecución injusta con el interés general de no facilitar la impunidad del delincuente" (CS, Fallos 272:188; 311:652; 322:2683; 341:207).

(1) Para no confundir al lector en relación con la versión del Código Procesal Penal que se encuentra vigente, se citan los artículos a los que se intentó hacer referencia en la resolución y que corresponden al texto de la norma según las modificaciones introducidas por las leyes 27.272 y 27.482; el dec. 118/2019. La resolución cita el art. 144 y el art. 161 y ss. del Cód. Proc. Penal Fed. según la redacción de la ley 27.063, que no es la versión del código procesal que se encuentra vigente ni que resultaba aplicable a la fecha en la que se dictó la resolución que se comenta.

(2) A lo largo de este comentario me referiré, de manera indistinta, a la prueba digital como prueba o evidencia electrónica o informática.

(3) La implementación del Cód. Proc. Penal Fed., comenzó en Salta y Jujuy el 10/06/2019 (res. 1/2019 de la Comisión Bicameral de Monitoreo e Implementación del Código Procesal Penal Federal (BO 03/06/2019) y en Mendoza y Santa Fe en noviembre de 2019, según lo dispuesto en el art. 2º de la res. 2/2019 de la Comisión Bicameral de Monitoreo e Implementación del Código Procesal Penal Federal, BO 13/11/2019.

(4) La Res. 2/2019 de la Comisión Bicameral de Monitoreo e Implementación del Código Procesal Penal Federal, BO 13/11/2019, estableció la implementación de los arts. 19, 21, 22, 31, 34, 54, 80, 81, 210, 221 y 222 del Cód. Proc. Penal Fed., para la justicia federal y nacional.

(5) El Cód. Proc. Penal Fed., incorpora reglas específicas sobre prueba digital y zanja así el vacío legal del Cód. Proc. Penal de la Nación, y si bien autoriza que la comunicación por medios electrónicos de una orden de allanamiento en casos graves y urgente (art. 144, tercer párrafo del Cód. Proc. Penal Fed.) y la interceptación de comunicaciones electrónicas (art. 150 del Cód. Proc. Penal Fed.), no es pionero como otros códigos procesales provinciales, por ejemplo el Código Procesal Penal del Neuquén, que también dispone como medida de prueba el acceso remoto en el art. 153.

(6) Señalo esa circunstancia porque las facultades de las fuerzas de seguridad para, p. ej., solicitar los códigos de desbloqueo de los teléfonos celulares y acceder a la información almacenada plantea otros interrogantes relacionados con la posible afectación a la garantía constitucional que prohíbe la autoincriminación que no se aborda en este comentario.

(7) Los alcances del examen de la prueba extraída de un dispositivo electrónico deben estar establecidos en los puntos de peritaje si fuera que la prueba será relevada por personal técnico especializado, o si el examen lo realizan los empleados, funcionarios o magistrados judiciales la búsqueda debe quedar limitada a la información que se traduzca en prueba —de cargo o de descargo— relacionada con el hecho que motivó el secuestro de la prueba física. Lo expuesto plantea otro debate que excede el objeto de este comentario, pero que cabe mínimamente mencionar: ¿qué temperamento corresponde adoptar en el caso en que durante el examen de la prueba digital se adviertan elementos probatorios de otra posible conducta delictiva? ¿Podría en ese caso aplicarse la conocida doctrina del plain view, acuñada por la Corte Suprema de los Estados Unidos en los precedentes "Harris vs. United States", 390 US 234 (1968) y "Coolidge vs. New Hampshire" 403 US 443; (1971), receptada en el art. 224 in fine del Cód. Proc. Penal de la Nación y art. 146 del Cód. Proc. Penal Fed. y convalidada por la CFed. Cas. Penal, sala II, 19/11/2013, "Skrypnik, Ramón s/recurso de casación", causa 15609, reg. 2047.13.2; sala IV, 24/06/2014, "Ceballos, Aníbal S. y otros s/recurso de casación", causa 221/13, reg. 1269.14.4., y 01/09/2015, "Redsant López, Julio L. s/recurso de casación", causa FCR 94000170/2012/TO1/CFC1, reg. 1651.15.4., entre otros, para dar origen a una investigación distinta?

(8) Las distintas operaciones que pueden realizarse con UFED 4 PC pueden consultarse en http://www.complexbiz.com/wp-content/uploads/2014/05/UFED-4PC-Brochure_AL_ES_web.pdf, último acceso 10/12/2019.

(9) "Guidelines on Digital Forensic Procedures for European Anti-Fraud Office Staff (OLAF)", 15/02/2016, https://ec.europa.eu/anti-fraud/sites/antifraud/files/guidelines_en.pdf.

(10) Resulta oportuno volver a señalar que la res. 2/2019 de la Comisión Bicameral de Monitoreo e Implementación del Código Procesal Penal Federal, BO 13/11/2019, estableció únicamente la implementación de los arts. 19, 21, 22, 31, 34, 54, 80, 81, 210, 221 y 222 del Cód. Proc. Penal Fed., para la justicia federal (art. 1º, primer párrafo) y las mismas disposiciones para la justicia nacional excepto el art. 54 (art. 1º, segundo párrafo), porque resultan disposiciones más benignas para los imputados.

(11) "Riley vs. California", 134 S. Ct. 2473 (2014).

(12) "US vs. Wurie Riley", 134 S. Ct. at 2495 (2014).

IMPUGNACIÓN DE PRUEBA ELECTRÓNICA. UN NOVEDOSO, DINÁMICO Y FLUCTUANTE ESCENARIO DE LA ACTIVIDAD PROBATORIA MODERNA

Por Carlos Ordóñez(*)

I. Introducción

Atento el enorme potencial de las fuentes probatorias de origen electrónico, saber cuándo y cómo cuestionar la misma constituye sin lugar a dudas un tesoro preciado en la faena defensiva moderna[1].

La prueba electrónica nos invita a replantearnos las estrategias procesales tradicionales y a prestar un especial énfasis a cómo estos registros informáticos trasladan su influencia sobre la posición que asumen las partes en el proceso, especialmente cuando procuran fortalecer o desprestigiar este poderoso material convictivo.

Nos encontramos ante una temática tan importante que una desafortunada maniobra en este sentido podría conducirnos a falsas expectativas sobre el posible resultado de la contienda o, inclusive, a consecuencias no deseadas.

En este entuerto, existen ribetes especiales que deben ser analizados en detenimiento, dadas las ostensibles diferencias entre un documento en soporte papel (con o sin firma) y un documento electrónico, que además de poseer —o no— firma (electrónica o digital), puede exhibir características técnicas de toda índole, lo que a todas luces incidirá sobre el contenido o la entidad de los planteos que efectúen los litigantes.

Estos instrumentos telemáticos son una fuente inmensa de información y como tales, se han convertido en las estrellas más relumbrantes de la prueba electrónica, pues en su adquisición, representación, conservación, introducción, exploración y adecuada complementación, reconocimiento, negación e impugnación, reside el éxito de las contiendas modernas.Para comprender este fenómeno debemos saber que el concepto de documento electrónico es tan amplio y abarcativo que dentro del mismo quedan englobados una gran variedad de supuestos que hacen a la prueba electrónica propiamente dicha.

Un documento electrónico es un documento cuyo soporte material es algún tipo de dispositivo electrónico o magnético y cuyo contenido esta codificado. Para su lectura, para su reproducción o para su interpretación, necesitaremos también el auxilio de la tecnología disponible[2].

Molina Quiroga prefiere hablar de documento digital, definiéndolo como aquel que es conservado en formato digital en la memoria central del ordenador o en las memorias de masa y que no puede ser leído o conocido por el hombre sino como consecuencia de un proceso de traducción que hace perceptible y comprensible el código de señales digitales. Técnicamente, el documento digital es un conjunto de impulsos eléctricos que recaen en un soporte de computadora que, sometidos a un proceso, permiten su traducción al lenguaje natural a través de una pantalla, una impresora u otro periférico que genere un resultado equivalente[3].

De esta manera, cuando un juez valora bajo estas premisas una filmación, un mensaje de WhatsApp, una publicación de Facebook o Twitter, una página web, un mail, una fotografía, un audio, los registros existentes en un software, una firma electrónica, entre otros, técnicamente lo que está apreciando es un documento electrónico, con las derivaciones legales que ello implica. Esto no quiere decir que sea lo mismo un archivo de imagen que un archivo de video o de audio; o un documento no firmado que un documento signado con tecnología de firma digital o firma electrónica; o un mensaje enviado por una red local que un correo electrónico o un mensaje multimedia, etc.[4], existiendo distintas variables de estos instrumentos y no todas gozando de las mismas propiedades.

A lo largo del presente trabajo, haremos un repaso general del instituto para después sumergirnos de lleno en las situaciones más usuales con las que nos podemos encontrar y que ameritan un esfuerzo impugnativo extra o adicional del interesado para no sucumbir en el complejo entramado de información que almacenan estas fuentes probatorias.

II. La prueba electrónica. Aproximaciones

Quadri ya ha sostenido que la prueba es un medio de verificación de las proposiciones que los litigantes formulan en el juicio o, en el caso en que la ley lo autoriza (ej. arts. 163, inc. 6°, p. 2, Cód. Proc. Civ. y Com.; arts. 200 y 201, CPC Córdoba), de acreditación de los hechos conducentes para la solución del litigio; mientras tanto, si pasamos a su análisis en el marco de un proceso concreto, prueba será —vista desde el enfoque del resultado— todo motivo o razón aportados al proceso para llevar al juez el convencimiento o la certeza sobre los hechos. Probar será, entonces, la acción de aportar tales razones y motivos, en orden a dejar verificada alguna de las proposiciones formuladas en juicio; y la actividad probatoria será aquella encaminada a probar (por cierto, con un resultado contingente, pues podrá —o no— lograr su objetivo)[5].

Y coincidimos con el citado autor en que la prueba electrónica no es, en esencia, diferente a cualquier prueba en general, conforme ingresa dentro del campo más amplio de la prueba; es decir, y valga la redundancia, la prueba electrónica no es más que prueba.

En el derecho comparado español, ya el maestro Lluch ha sostenido que la expresión prueba electrónica puede definirse como la información obtenida a partir de un dispositivo electrónico o medio digital, el cual sirve para adquirir convencimiento de la certeza de un hecho o, con mayor precisión doctrinal, la información obtenida a partir de un dispositivo electrónico o medio digital, el cual sirve para formar la convicción en torno a una afirmación relevante para el proceso [6].

Siguiendo esa senda, nosotros definimos a la prueba electrónica como aquella prueba cimentada en la información o datos, con valor probatorio, que se encuentran insertos dentro de un dispositivo electrónico o que hubiera sido transmitida por un medio afín, a través de la cual se adquiere el conocimiento sobre la ocurrencia o no de hechos que las partes hayan afirmado como fundamento de sus derechos, o cuestionados, y que deban ser invocados dentro de un proceso judicial[7].

Ahora bien, agregamos que técnicamente está constituida por campos magnéticos y pulsos electrónicos, susceptibles de ser recolectados, acreditados, analizados y valorados por aquellos individuos que posean los conocimientos necesarios a dichos fines[8].

Y, en el marco de un proceso judicial, la prueba electrónica tiene por objeto cualquier registro que pueda ser generado dentro de un sistema informático, entendiendo por este a todo dispositivo físico (computadoras, smartphones, tablets, CDs, DVD, pen drives, etc.) o lógico, empleado para crear, generar, enviar, recibir, procesar, remitir o guardar a dichos registros que, producto de la intervención humana u otra semejante, han sido extraídos de un medio informático[9].

En este sentido, lo distintivo de la prueba electrónica es que está esencialmente vinculada a hechos o actos jurídicos ocurridos o realizados a través de medios informáticos. Es decir, resulta determinante que los hechos asuman una configuración informática. Entonces, una fotografía, un video, una página web, un correo electrónico, una base de datos, una contabilidad en un programa de cálculo Excel —por citar algunos ejemplos—, en cualquier soporte (digital, magnético o informático), constituyen una «prueba electrónica» o «documento electrónico», aun cuando su reproducción e impugnación puedan ser diferentes [10].

III. Impugnación. Generalidades

La capital relevancia de la prueba electrónica en el pleito encuentra su razón de ser en el enorme cúmulo de información que almacenan sus registros, la cual debidamente explorada y/o robustecida permite formar convencimiento en el juez sobre la veracidad de los hechos o actos que documentan.

Este gigantesco potencial de la probática digital, como contrapartida, obliga a prestar un especial énfasis a la faz defensiva, cuyo debido abordaje asume un rol preponderante para los litigantes.

Ante todo, debemos incorporar, comprender y conocer los aspectos técnicos indispensables que caracterizan a las mismas y cómo juegan aquellos en la mayor o menor eficacia probatoria de estas modernas fuentes[11].

No se requiere que los profesionales se conviertan en expertos en ingeniería informática para poder trabajar con este tipo de probanzas, aunque si deberán internalizar el conocimiento necesario que les permita ejercer la tarea de forma eficiente, ya sea procurándose la asistencia necesaria o absorbiendo los contenidos mínimos ineludibles a tales fines.

En el ejercicio actual del derecho, cada vez es más frecuente que los letrados litigantes sean consultados sobre la ocurrencia de hechos o actos jurídicos que de alguna manera se encuentran mediados por elementos relativos a la evidencia electrónica. Ergo, para poder exponerlos adecuadamente en el marco de una acción judicial y, luego, probarlos de un modo jurídicamente relevante y, eventualmente, defenderse de este tipo de evidencia, es fundamental que los abogados posean un conocimiento acabado del medio informático que les permita explicarlo y ofrecer la prueba necesaria para fundar su posición.

Asimismo, resulta trascendental saber cuáles son los mecanismos que nos proporciona el orden ritual o que mejor se ajustan al mismo para desvirtuar o restar eficacia probatoria a estas modernas fuentes.

El reconocimiento o la negación de un documento electrónico es uno de ellos, disponiendo el art. 356 del Cód. Proc. Civ. y Com. que al demandado le incumbe la carga de: *"...reconocer o negar categóricamente cada uno de los hechos expuestos en la demanda, la autenticidad de los documentos acompañados que se le atribuyeren y la recepción de las cartas y telegramas a él dirigidos cuyas copias se acompañen. Su silencio, sus respuestas evasivas, o la negativa meramente general podrán estimarse como reconocimiento de la verdad de los hechos pertinentes y lícitos a que se refieran. En cuanto a los documentos se los tendrá por reconocidos o recibidos, según el caso..."*. Igual peso recae sobre la contraparte en caso de que existiera reconvención o de que se le diere traslado de nuevos documentos (art. 358 Cód. Proc. Civ. y Com.).

Aunque en muchas ocasiones no es suficiente el mero desconocimiento de la prueba electrónica, sino que asimismo deviene imprescindible realizar una actividad procesal de mayor envergadura, más compleja e incluso acompañada de un debido respaldo probatorio.

Estamos hablando específicamente de la "impugnación".

Rojas efectúa un lúcido análisis de las implicancias del término "impugnación" en el plano probatorio, resaltando que no es privativo del ámbito recursivo, y así nos brinda numerosos ejemplos de su utilización práctica (impugnación de la prueba pericial o testimonial, entre otros)[12].

Asimismo, el autor citado reflexiona que se impugna para atacar, para quitarle eficacia, para restarle validez, esto es, para privar de efectos jurídicos a aquello que se está atacando, por eso es importante tener en cuenta dos aspectos básicos: por un lado, el sentido de la voz "documento" y, por otro, el sentido de la voz "impugnación", pues sobre ellos se deberá construir la elaboración necesaria a los efectos de poder demostrar en el proceso aquello que se persigue, es decir, la privación de los efectos jurídicos de aquello que se ha impugnado.

Enfocándonos en el plano de la prueba documental, vemos que el orden procesal presta un especial énfasis a la impugnación de los instrumentos públicos, reglada en el art. 395 del Cód. Proc. Civ. y Com. y nada dice de los instrumentos privados, que se encuentran huérfanos de regulación.

La aparición de los documentos electrónicos en el ámbito jurídico y su ascendiente crecimiento en la escena probatoria tornó mucho más evidente este vacío normativo, en razón de las diferentes aristas que ofrecen tales archivos, lo que trae aparejado un desarrollo peculiar y especializado de la labor impugnativa, totalmente distinto a lo que ocurría con los clásicos documentos en soporte papel.

En esta compleja empresa, debemos comprender que la fortaleza de todos los instrumentos telemáticos gira alrededor de tres ejes basilares, que son: autoría, integridad y licitud.

La autoría sirve para desdeñar quién es el autor del documento electrónico, vale decir, de quién emanó el mismo para así producir consecuencias legales de diverso tenor. La integridad apunta a descartar o eventualmente restar eficacia probatoria a aquellos documentos telemáticos que hayan sido objeto de modificaciones o adulteraciones o que carezcan de aptitud para trasmitir confianza técnica. La licitud busca confinar cualquier medio probatorio obtenido o producido en violación al orden jurídico en su conjunto, independientemente de que se trate de una norma adjetiva, sustancial o supra legal (Constitución Nacional y Tratados Internacionales de igual jerarquía)[13].

En la mayoría de los casos, en la conjunción de estos tres pilares fundantes residirá la fuerza probatoria de los mismos, de lo cual se coligen tres conclusiones de gran valor: la primera, que estamos ante tres conceptos independientes entre sí; la segunda, que podremos atacar cualquiera de ellos, sin tener necesidad de impugnar todos, para restarle eficacia probatoria al documento; y la tercera constituye una derivación de aquellas y consiste en que, en algunas ocasiones, bastará con desvirtuar solo uno para echar por tierra la prueba (v.gr. licitud).

Uno de los inconvenientes más frecuentes en la generalidad de estos instrumentos radica en que los mismos no permiten per se una efectiva identificación del remitente (autoría), sino que, eventualmente, solo proporcionan los datos del dispositivo donde se ha generado y remitido.

Entonces, para enervar la eficacia probatoria de una firma electrónica que se atribuya a determinada persona, la clave de la impugnación va a estar dada por controvertir la confiabilidad de los soportes y procedimientos técnicos utilizados para asociar al mismo a un usuario determinado.

Por el lado de la integridad, un aspecto a tener en consideración en una eventual impugnación es la volatilidad del formato, atento que no se requieren grandes conocimientos o habilidades para su manipulación, ni mucho menos instrumental complejo. No todos los documentos digitales poseen las mismas propiedades técnicas. Existe una gran diversidad y grados de seguridad al respecto, por lo que tendremos que ser cuidadosos en su debida individualización y cuestionamiento. No es lo mismo atacar un documento con o sin firma digital, o uno con o sin firma electrónica.

Yendo al plano de la licitud, la regla sentada por el art. 378 del Cód. Proc. Civ. y Com. permite impugnar cualquier medio probatorio que afecte a la moral, la libertad personal de los litigantes o de terceros, o que estén expresamente prohibidos para el caso.

Todo lo dicho no hace más que poner sobre la mesa las diversas complicaciones que ofrecen los documentos electrónicos y que incluso varían en cada instrumento en particular, lo que hace que un cuestionamiento difícilmente sea similar a otro.

Tal vez los documentos electrónicos con firma digital sean el mejor ejemplo de este atolladero. Dada la fortaleza legal que gozan los mismos al contar con las presunciones de autoría e integridad, conllevan un esfuerzo defensivo complejo más similar a la impugnación de instrumento público que al ataque de un instrumento privado.

No obstante, existen muchísimos otros supuestos que también demandan una ardua labor en ese sentido.

Lo que queremos significar es que los documentos electrónicos en muchos casos requerirán un cuestionamiento específico, más allá que el orden procesal únicamente nos constriña a negar o reconocer tales instrumentos y nada más, pues una debida impugnación de los mismos, acompañada de un andamiaje probatorio adecuado, será la única manera de restarle eficacia a estas fuentes tan poderosas.

En cuanto al momento procesal oportuno para efectuar este tipo de cuestionamientos de mayor complejidad, ante el desamparo adjetivo habrá que estarse a cada caso en particular y a las previsiones rituales referidas al cuestionamiento de prueba documental.

A modo de ejemplo, tratándose de documentos electrónicos anexados al escrito de demanda o a la contestación de la misma, no caben dudas que la etapa y el plazo pertinente para impugnar aquellos será el reglado por los arts. 356 y 358 del Cód. Proc. Civ. y Com., respectivamente.

IV. Supuestos especiales

a) Falsedades:

Todo documento electrónico —por diseño— es modificable dado que puede ser objeto de agregados, reformas, adulteraciones o manipulaciones de todo tipo y tenor, presentando un contexto más que delicado en el ámbito judicial al tiempo de analizar la confiabilidad del material probatorio de esta naturaleza.

Mediante una impugnación de falsedad buscaremos atacar la "integridad de la prueba" (obviamente en los casos que ello correspondiere), con el objetivo de mostrarle al juez que se encuentra frente a una fuente probatoria corrompida y que, por ende, carente de toda eficacia.

Antes de activar este andamiaje, los abogados deberán llevar a cabo tareas de investigación forense menores, tendientes a detectar posibles irregularidades técnicas en este material de probatorio.

A modo de ejemplo, podremos estudiar las propiedades del documento electrónico que tengamos en nuestro poder y así, con tan sólo hacer clic en el botón derecho del mouse, sabremos la fecha de creación del archivo, lo cual arrojará in-

formación muy útil para verificar su correspondencia con los hechos; a través de la utilización de WhatsApp Web podremos corroborar que los mensajes instantáneos que tenemos a la vista en un celular no han sido adulterados; analizando el código fuente de la página web que surge de un acta de constatación notarial chequearemos su equivalencia con el dominio original; verificando la línea móvil involucrada mediante una consulta en la web del ENACOM sabremos quién es el titular de la misma; entre otros.

En cuanto al momento oportuno para deducir este tipo de impugnaciones, habrá que estarse a cada caso en particular, por regla general, tratándose de cuestionamientos de documentos electrónicos anexados al escrito de demanda o a la contestación de la misma, no caben dudas que la etapa y el plazo pertinente para impugnar aquellos será el reglado por los arts. 356 y 358 del Cód. Proc. Civ. y Com., respectivamente.

Lo que no quita que puedan darse otros supuestos, por ejemplo, el previsto por el art. 365 del Cód. Proc. Civ. y Com. (hechos nuevos), o los establecidos por los arts. 388 (documentación en poder de una de las partes) o 389 (documentación en poder de terceros) del Cód. Proc. Civ. y Com., entre otros, que darán inicio al cómputo de un nuevo plazo impugnativo.

b) Firma digital:

Un documento electrónico rubricado con firma digital válida, es decir, emitida de conformidad a las disposiciones legales y reglamentarias vigentes, presupone que dicha operatoria fue efectuada por el titular del certificado (autoría) y que el instrumento no ha sido modificado desde el momento de su rúbrica (integridad).

Ergo, si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento telemático es verdadero, estas presunciones legales garantizan el no repudio por parte del firmante, tanto de la rúbrica como del contenido del instrumento.

Estas características del documento con firma digital, que respetan estándares internacionales, lo convierten en un muro probatorio prácticamente infranqueable, a prueba de cuestionamientos que dejan la faena impugnativa de los litigantes muy limitada, reducida a supuestos específicos y con consecuencias procesales —en la generalidad de los casos— bastante atenuadas.

Dentro de ellos, sobresalen todas aquellas cuestiones que hagan al ataque de validez de la firma digital y cuyos requisitos especialmente se encuentran reglados en el art. 9° de la ley 25.506[(14)].

Así, una firma digital podrá ser impugnada por falta de emisión durante su periodo de vigencia, por no poder ser verificable y por carecer de un certificado emitido por un certificador licenciado, y para ello deberá desplegarse una actividad probatoria en ese sentido.

Sin embargo, en caso de prosperar ese tipo de ataques no producirán per se la desestimación de la prueba, sino muy por el contrario, la misma continuará siendo válida, aunque con las limitaciones propias de la firma electrónica, tal como prevé el art. 5° de la Ley de Firma Digital.

Todo lo expuesto pone sobre el tapete la enorme eficacia probatoria de esta fuente, cuya impugnación —en la mayoría de los supuestos— difícilmente pueda ser capitalizada satisfactoriamente por el impugnante. Al respecto, la doctrina ha dicho que la firma digital está revestida de una serie de formalidades que le permiten contar con una presunción, asimilándola a la certificación de firma por escribano, pero con un condimento menor: la presunción es iuris tantum y no se debe recurrir —necesariamente— a la redargución de falsedad para su impugnación[(15)].

Respecto al momento pertinente para atacar estos tipos de documentos, tratándose de prueba documental, resultan aplicables los mismos conceptos que venimos viendo precedentemente.

c) Ilicitudes:

Hoy en día nos encontramos ante un escenario probatorio muy particular, caracterizado por la facilidad con que los litigantes recolectan y documentan información de la realidad que los rodea, al punto tal de preconstituir prueba por sus propios medios en todo momento y lugar, sin contralor alguno del guardián de la función judicial.

Y hay que tener muchísimo cuidado con esta realidad, el procedimiento no puede convertirse en un gerenciador de datos informáticos (prueba) mal habidos y en un instigador de conductas probatorias irregulares.

En ese afán, cumple un rol significativo la actividad impugnativa desplegada por las partes, ya que la misma pondrá en evidencia el desapego legal o el agravio constitucional que motive la exclusión de la prueba y, asimismo, importará el ejercicio de una garantía que el orden normativo pone en cabeza de su titular, para que este la utilice —o no— cuando lo estime menester. Respecto al momento procesal oportuno para deducir la misma, tratándose de prueba documental, resultan aplicables los mismos conceptos que venimos viendo "ut supra", y en torno a otros medios probatorios, habrá que estarse a cada caso en particular.

Una mención especial merece la prueba obtenida a través de un reconocimiento judicial web. Si se realiza con carácter anticipado, antes de trabarse la litis, el plazo para impugnar la prueba comenzará a correr desde que se tomó conocimiento formal de la prueba, no obsta ello la presencia de la defensora oficial en el acto. Si se lleva a cabo con carácter anticipado, pero después de trabada la litis y con la presencia del demandado, deberá ser impugnado al contestar el escrito de inicio. Idéntica oportunidad será aplicable cuando se desarrolle la prueba en la etapa pertinente.

d) Actas de constatación:

Una modalidad muy usual son las actas notariales de constatación de contenido digital pasadas ante un escribano público, a fin de que el mismo de fe de la información que aprecian sus ojos y que luego será reflejada en el protocolo pertinente.

Idéntica función cumplen los reconocimientos judiciales virtuales que, si bien poseen una naturaleza totalmente distinta, en definitiva, comparten la misma esencia.

La fortaleza de estos tipos de documentos públicos reside en que los funcionarios intervinientes (v.gr. escribano o secretario), por imperio del art. 296 del Cód. Civ. y Com., darán plena fe de:

a. En cuanto a que se ha realizado el acto, la fecha, el lugar y los hechos que el oficial público enuncia como cumplidos por él o ante él hasta que sea declarado falso en juicio civil o criminal;

b. En cuanto al contenido de las declaraciones sobre convenciones, disposiciones, pagos, reconocimientos y enunciaciones de hechos directamente relacionados con el objeto principal del acto instrumentado, hasta que se produzca prueba en contrario.

Observarán el distingo que efectúa la norma, elevando a rango de instrumento público únicamente el primer supuesto contemplado y solo podrá ser atacada mediante una redargución de falsedad, y no así el segundo, que al no poseer tales características bastará la mera impugnación.

Sin embargo, es interesante agregar que el Código Civil y Comercial de la Nación contiene una regulación específica de las actas notariales, que viene a complementar el régimen general expuesto.

Luego de regular los requisitos de la misma en el art. 311 del Cód. Civ. Y Com.,[16] el legislador se ocupa de aclarar, en el art. 312 del Cód. Civ. Y Com., que el valor probatorio de las actas se circunscribe a los hechos que el notario tiene a la vista, a la verificación de su existencia y su estado. En cuanto a las personas, se circunscribe a su identificación si existe y debe dejarse constancia de las declaraciones y juicios que emiten.

Queda claro entonces que el escribano solo da fe de lo que tiene a la vista, cuyo conocimiento adquiere sensorialmente, ya sea de la existencia de un documento electrónico, o de la identidad de los partícipes y no así de lo que no puede apreciar con sus propios sentidos. Siguiendo ese razonamiento, en el caso de que quisiéramos impugnar lo que el notario o el funcionario interviniente tuvo a la vista, indefectiblemente la única vía pertinente será el incidente de redargución de falsedad.

A su respecto, el art. 395 del Cód. Proc. Civ. y Com. dispone que *"La redargución de falsedad de un instrumento público tramitará por incidente que deberá promoverse dentro del plazo de DIEZ (10) días de realizada la impugnación, bajo apercibimiento de tenerla por desistida. Será inadmisible si no se indican los elementos y no se ofrecen las pruebas tendientes a demostrar la falsedad. Admitido el requerimiento, el juez suspenderá el pronunciamiento de la sentencia, para resolver el incidente juntamente con ésta. Será parte el oficial público que extendió el instrumento"*.

Acá, a los fines del cómputo de los plazos, habrá que efectuarse un distingo según se trate de un acta de constatación efectuada ante un notario, que deberá ser presentada en las oportunamente fijadas al efecto (arts. 333, 334 y 365 del Cód. Proc. Civ. y Com.), o de un reconocimiento judicial.

En cuanto a la actividad probatoria que deberá llevarse a cabo en el incidente, la jurisprudencia ha dicho que la prueba tendiente a demostrar la falsedad de un instrumento público debe examinarse con criterio restrictivo y tener una entidad tal que produzca la convicción necesaria para revertir la presunción de legitimidad y veracidad que emana de tal instrumento,[17] no bastando para ello las meras inferencias o indicios[18].

e) Hackeo de cuenta:

Vivimos en una época de plena ebullición y masificación de las redes sociales, existe una gran variedad de ofertas en el mercado, para todas las edades y gustos, gratuitos o pagas, según las preferencias de contenido del usuario.

Quién no escuchó alguna vez en un programa de chimentos a algún famoso exculpándose de un posteo en una red social, con la justificación *"me hackearon la cuenta"*. Aunque, lejos está de ser algo ficticio, místico o cosas de "hackers", sino, muy por el contrario, es mucho más fácil de lo que parece y solo bastará manipular los programas adecuados.

Dicho ello, puede ocurrir que a uno de los litigantes le "hackeen" la cuenta de una red social y aprovechen la misma para presconstituir elementos probatorios que después sean usados en su contra en un pleito judicial. Por más alocado que suene, es al menos probable.

Ante esta posibilidad, supongamos que somos citados a un juicio y a poco que revisamos la documentación existente, nos encontramos con contenido de esta naturaleza.

¿Qué debemos hacer en esos casos? y ¿qué recaudos tenemos que tomar?

Primeramente, ante todo impugnar, obviamente dentro de los plazos legales previstos al efecto, como si se tratare de un documento más, que dicho sea de paso lo es.

En segundo término, debemos hacer la denuncia penal correspondiente y saber que el éxito de la impugnación dependerá exclusivamente del resultado de la misma, pues el juez penal es el único con competencia para averiguar si existió —o no— el ilícito.

La Corte Suprema de Justicia de la Nación, en la causa "C.G.L. s/ denuncia violación de correspondencia", con fecha 25/04/17, entendió que el acceso ilegítimo a una "comunicación electrónica" o "dato informático de acceso restringido" constituye un delito de violación de correspondencia en los términos de los arts. 153 y 153 bis del Cód. Penal[19] .

No es la primera vez que el Máximo Tribunal entiende que el acceso ilegal a un medio de comunicación electrónico configura una violación de correspondencia como si fuese un correo postal tradicional. En "Díaz, Sergio Darío s/ violación correspondencia" (24/06/2014) y "N.N. s/ violación sistema informático art. 153 bis 1° párrafo" (23/06/2015), la Corte ya había establecido que "el acceso ilegítimo a una "comunicación electrónica" o a un "dato informático de acceso restringido", a los que solo es posible ingresar a través de un medio que, por sus características propias, se encuentra dentro de los servicios de telecomunicaciones que son de interés de la Nación" y deben ser investigados por la justicia federal[20].

f) Certificaciones de terceros de confianza:

Las certificaciones extendidas por terceros de confianza se caracterizan por poseer un sellado o marca de tiempo o timestamp, una cadena de caracteres o información codificada que identifica cuándo ocurrió un evento determinado, consolidando de forma exacta y específica la fecha y la hora del día en que sucedió[21].

Nos encontramos frente a un verdadero depositario "virtual", un custodio fiable del documento electrónico que alguna de las partes haya colocado bajo su órbita, en atención a determinados estándares de seguridad, con el objeto de procurar una mayor certeza (confianza) sobre el mismo, pero, aclaramos, no controla la legalidad de los contenidos que aloja.

Entonces, esta posibilidad de que pueda impugnarse el contenido de este documento "certificado", ya que la plataforma únicamente se encarga de dar certeza respecto de la existencia de un documento en tal día, hora y eventualmente, lugar.

Así, en una certificación extendida por un tercero de confianza sobre la existencia de una fotografía, por ejemplo, en una red social, la parte no podrá cuestionar la existencia de la misma, que se tendrá por probada, aunque si podrá cuestionar que la misma refiere a un perfil no fidedigno, vale decir, apócrifo.

Las enormes medidas de seguridad que poseen este tipo de plataformas, ya que la gran mayoría de los servicios disponibles en el mercado cumplen con estándares internacionales, colocan al pretenso impugnante en una situación muy similar a lo que ocurre con un documento con firma digital, pues si bien las mismas se valen del uso de tecnología de firma electrónica para materializar el sellado de tiempo, tal modalidad, siempre que se respeten los protocolos de rigor, será más que suficiente para producir el fin perseguido.

En última instancia, la prueba pericial informática nos brindará mayores detalles sobre los procedimientos técnicos empleados por la plataforma certificante y la seguridad de los mismos.

V. Reflexiones finales

Del recontó efectuado a lo largo del presente queda claro que debemos prestar una especial atención a la tarea impugnativa de la prueba electrónica. Habrá casos sencillos en los que bastará una mera negativa de los documentos electrónicos acompañados al proceso por la parte contraria, pero en muchos casos será necesario desplegar una actividad impugnativa de mayor complejidad, fundada no solo en aspectos legales, sino también en cuestiones técnicas, cuyo debido conocimiento cumple un rol fundamental en la litigación moderna.

La prueba electrónica es una realidad de los procesos actuales, siendo sumamente importante conocer sus principales aristas y cómo interactúan las mismas con el orden jurídico vigente.

Impugnación de prueba electrónica. Un novedoso, dinámico y fluctuante escenario de la actividad probatoria moderna

Por Carlos Ordóñez

La litigación actual demanda conocimientos específicos en materia de prueba electrónica, los cuales escapan a la formación de la mayoría de los profesionales y que, a su vez, todavía no cuentan con un respaldo normativo adecuado, aumentando exponencialmente la complejidad de la tarea.

Este artículo se encuentra publicado en **Sup. Esp. LegalTechII 2019 (noviembre), 11/01/2019, 21. Cita Online:** AR/DOC/3571/2019

(*) Abogado egresado de la Facultad de Derecho de la Universidad Nacional de Mar del Plata. Mediador. Doctorando en derecho. Secretario del Tribunal del Trabajo Nº 4 de Mar del Plata. Vicepresidente del Instituto Argentino de Derecho Procesal Informático.

(1) A los efectos de ahondar aún más sobre la incorporación al proceso y correspondiente valoración de las más diversas fuentes probatorias electrónicas utilizadas habitualmente por los litigantes (nos referimos a contenidos existentes en páginas web, correos electrónicos, WhatsApp, Facebook, Twitter, Instagram, YouTube, archivos locales, entre otros), recomendamos profundizar en Bielli, Gastón E. — Ordoñez, Carlos J., La prueba electrónica. Teoría y práctica, Thomson Reuters - La Ley, 2019.

(2) Tanco, María Cecilia, "Actos procesales electrónicos" en Camps, Carlos E. (dir), Tratado de Derecho Procesal Electrónico, Editorial AbeledoPerrot, Buenos Aires, 2015, t. II, p. 209.

(3) Molina Quiroga, Eduardo, "Ley de expedientes digitales y notificaciones electrónicas judiciales", LA LEY 22/06/2011, 1 — LA LEY2011-C, 1224 — Enfoques 2012 (enero), 02/01/2012, 70.

(4) Ordoñez, Carlos J., "La prueba electrónica y su valoración en sede laboral", en Granero, H. R. (Dir.), E-Mails, chats, WhatsApp, SMS, Facebook, filmaciones con teléfonos móviles y otras tecnologías. Validez probatoria en el proceso civil, comercial, penal y laboral, Buenos Aires, 2019, p. 289.

(5) Quadri, Gabriel H., La prueba en el proceso civil y comercial, t. I, Abeledo-Perrot, Buenos Aires, 2011, p. 17.

(6) Lluch, Xavier A., Derecho probatorio, Editorial Bosch, Barcelona, 2012, p. 1109.

(7) Bielli, Gastón E. - Ordoñez, Carlos J., La prueba electrónica. Teoría y práctica, La Ley, Buenos Aires, 2019.

(8) Bielli, Gastón E. - Ordoñez, Carlos J., cit.

(9) Vaninetti, Hugo A., "Preservación y valoración de la prueba informática e identificación de IP", LL 2013-C-374.

(10) Lluch, Xavier A., Derecho probatorio, cit.

(11) Para una mayor profundización sobre cada uno de estos aspectos véase Bielli, Gastón E. - Ordoñez, Carlos J., La prueba electrónica. Teoria y práctica, cit.

(12) Rojas, Jorge A., "Prueba documental: Redargución y adveración", en Revista de Derecho Procesal, 2005-2, Prueba — II, Rubinzal - Culzoni Editores, Santa fe, 2005, ps. 45-46.

(13) Para una mayor profundización sobre cada uno de estos aspectos véase Bielli, Gastón E. - Ordoñez, Carlos J., La prueba electrónica. Teoría y práctica, cit.

(14) Art. 9° (Ley 25.506): "Una firma digital es válida si cumple con los siguientes requisitos: a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante; b) Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente; c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado".

(15) Izquierdo, Carlos, G., "Recibo de sueldo digital", DT 2011 (abril), 806, IMP 2011-5, 249, Cita Online: AR/DOC/765/2011.

(16) Art. 311 (CCyCN): "Las actas están sujetas a los requisitos de las escrituras públicas, con las siguientes modificaciones: a) se debe hacer constar el requerimiento que motiva la intervención del notario y, en su caso, la manifestación del requirente respecto al interés propio o de terceros con que actúa; b) no es necesaria la acreditación de personería ni la del interés de terceros que alega el requirente; c) no es necesario que el notario conozca o identifique a las personas con quienes trata a los efectos de realizar las notificaciones, requerimientos y otras diligencias; d) las personas requeridas o notificadas, en la medida en que el objeto de la comprobación así lo permita, deben ser previamente informadas del carácter en que interviene el notario y, en su caso, del derecho a no responder o de contestar; en este último supuesto se deben hacer constar en el documento las manifestaciones que se hagan; e) el notario puede practicar las diligencias sin la concurrencia del requirente cuando por su objeto no sea necesario; f) no requieren unidad de acto ni de redacción; pueden extenderse simultáneamente o con posterioridad a los hechos que se narran, pero en el mismo día, y pueden separarse en dos o más partes o diligencias, siguiendo el orden cronológico; g) pueden autorizarse aun cuando alguno de los interesados rehúse firmar, de lo cual debe dejarse constancia".

(17) CNCIV., SALA D, 4.9.73, LL 156-3; CNCIV, SALA K, 23.8.94, ED 160-553.

(18) CNCom, Sala E, "Grabovieski Víctor c/ Serebrinsky, Daniel H. s/ sumario, 14.12.2001.

(19) Art. 153 (CP): "Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida. En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido...". Art. 153 bis (CP): "Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido".

(20) Delfi´n, Alejandra, "El hackeo de una cuenta Facebook configura un 'delito de violación de correspondencia', confirma la Corte Suprema", RDA 2017-112, 04/08/2017, 596, Cita Online: AP/DOC/622/2017.

(21) Bielli, Gastón E., "Terceros de confianza y certificación de prueba electrónica. Una nueva frontera en materia de probática", LA LEY 03/06/2019, 1, Cita Online: AR/DOC/1629/2019.

MEDIDAS DE PRUEBA ANTICIPADA EN LA DOCUMENTACIÓN ELECTRÓNICA

Por Diego Fernández

Las medidas de prueba anticipada tendientes a asegurar la producción de documentos electrónicos constituyen medidas cautelares y, como tales, serán procedentes en la medida en que la parte requirente pruebe la existencia de verosimilitud en el derecho, el peligro en la demora y otorgue suficiente contracautela. El peticionante de la medida deberá explicar al tribunal de forma clara y concreta cuáles son las razones que hacen a la medida solicitada el único o más efectivo medio probatorio para resguardar los documentos electrónicos.

I. Introducción

El uso de computadoras y dispositivos móviles es cada día más necesario. Todos ellos permiten reproducir, acceder y guardar información y distinto tipo de documentos. Muchos de esos documentos únicamente se encuentran en formato electrónico, es decir, no existen en papel. En algunos otros casos, cada vez menos, queda de estos documentos una copia en versión papel. No hay dudas de que la tendencia es que con el correr de los años cada vez más información y documentos estarán almacenados de forma electrónica.

El hecho de que la mayoría de estos documentos esté almacenado únicamente en forma electrónica hace que el acceso al dispositivo en el que se encuentran almacenados sea de vital importancia para poder utilizarlos como medios de prueba en el caso de un conflicto.

En general, con la ayuda de profesionales versados en la materia, los documentos electrónicos pueden ser fácilmente alterados o borrados sin dejar un rastro claro sobre su alteración o eliminación. Es cierto que lo mismo puede suceder con los documentos en versión papel, y de hecho ha sucedido seguramente un sinnúmero de veces, pero la informática ha hecho que la alteración y eliminación de documentos electrónicos sea más fácil y abarcativa, entendida como la posibilidad de borrar una gran cantidad de documentos en segundos. Eliminar por completo varios cientos de hojas de papel lleva mucho tiempo y pueda dejar distintos rastros que permitan llegar a conocer su eliminación. Ese no es el caso de los documentos electrónicos.

Es por esta posibilidad cierta de extravío, pérdida, alteración o eliminación, que a menudo se los solicita a los tribunales el dictado de diligencias preliminares, particularmente el dictado de una medida de prueba anticipada, a fin de constatar la existencia de ciertos documentos electrónicos y de resguardar una copia de los mismos para el momento procesal oportuno.

El objetivo principal de estas medidas es el de evitar el extravío, pérdida, alteración o eliminación de la prueba antes de que pueda ser utilizada en un juicio.

Medidas de prueba anticipada en la documentación electrónica

Por Diego Fernández

El principal temor de la parte que requiere la medida es que el demandado intente obstaculizar el acceso a los documentos a resguardar una vez anoticiado de la medida. En este aspecto los tribunales suelen considerar cuál ha sido la conducta de las partes en lo previo al pedido de la medida o incluso cuál ha sido su conducta en casos anteriores[1].

Por otro lado, dado el cada vez mayor acceso no autorizado a distintos sistemas y servidores, también existe cierto temor de que los documentos electrónicos pudieran extraviarse o perderse por distintos motivos, aún motivos ajenos a la parte que tiene a su cargo el control de acceso a los mismos.

Así lo ha reconocido la jurisprudencia al sostener que *"(...) aparece verosímil la motivación del demandante sobre la necesidad de obtener una medida como la de la especie con el claro propósito de aventar el ulterior ocultamiento, modificación, destrucción, alteración o pérdida en el objeto probatorio (...) donde la vulnerabilidad y fragilidad que los registros informáticos ofrecen, permiten presuponer el peligro en la demora, ya que pueden desaparecer o resultar afectados por algún virus"*[2].

En un sentido similar, los tribunales han considerado que la propia naturaleza de los documentos electrónicos hace a éstos modificables por la mera voluntad de quién tiene el control sobre ellos lo que aconseja inclinarse a favor de la concesión de medidas tendientes a su resguardo para hacerlos valer en la etapa procesal oportuna. Asimismo, los tribunales se han mostrado más proclives a conceder medidas de prueba anticipada cuando sobre los documentos electrónicos a resguardar no exista una obligación legal de conservarlos, lo que permitiría su eliminación en cualquier momento sin que existe una sanción legal por haberlo hecho. Respecto de ambas cuestiones, se ha dicho que *"(...) se considera atendible el requerimiento en análisis, pues la información que se pretende obtener y resguardar de la base de datos de la demandada, por su naturaleza, es modificable y/o destruible por la sola voluntad de su poseedor o, incluso, desaparecer por tornarse inútil a los fines empresariales (...) [lo que se deriva] de la propia naturaleza y vulnerabilidad de los registros informáticos y de que se trata de una documentación que, como principio, no existe obligación legal de conservar"*[3].

En igual sentido, también se ha dicho que *"[l]a doctrina y la jurisprudencia admitieron la intervención del Representante del Ministerio Público en aquellos casos en los que juzgó improcedente notificar la medida a la parte afectada 'porque su anticipación en el conocimiento puede permitir, que a través de maniobras de diverso tipo, oculte, modifique, destruya o cambie el objeto probatorio a adquirir'"*[4].

Es por ello que resulta de vital importancia poder asegurar la producción de dicha prueba con anterioridad a anoticiar al demandado sobre la existencia del reclamo. Claro está, que estamos hablando del supuesto en el que los documentos electrónicos están en poder del demandado o de un tercero sobre el que la parte actora no ejerce ningún control[5].

Sobre esta particular problemática existen fallos recientes en los que se analiza la procedencia de medidas de prueba anticipada tendiente a resguardar documentos electrónicos.

Si bien es cierto que en algunos de estos casos pudiera existir alguna falencia de la parte requirente a fin de convencer al tribunal sobre el cumplimiento de los requisitos objetivos para su procedencia, también es cierto que no en todos los casos se llega a comprender la importancia de asegurar los documentos electrónicos de forma previa al inicio de un reclamo.

En particular, el art. 326 del CPCCN regula la prueba anticipada y dispone lo siguiente:

"[l]os que sean o vayan a ser parte en un proceso de conocimiento y tuvieren motivos justificados para temer que la producción de sus pruebas pudiera resultar imposible o muy dificultosa en el período de prueba, podrán solicitar que se produzcan anticipadamente las siguientes:

1) (...);

4) La exhibición, resguardo o secuestro de documentos concernientes al objeto de la pretensión, conforme lo dispuesto por el artículo 325 (...)" (el resaltado no se encuentra en el original).

En ese sentido, se ha dicho que el art. 326 *"(...) contempla un modo excepcional de producción de prueba ante tempus, que depende de la urgencia y circunstancias particulares que esgrima el requirente"* y que *"(...) la prueba anticipada sólo puede ser admitida, si se comprueba que la parte que la propone está expuesta a perderla o pudiere resultar imposible o muy dificultosa su producción (...)"*[6].

En ese mismo orden de ideas, no debemos perder de vista que si bien la concesión de medidas de prueba anticipada implica una excepción al principio general de producción de la prueba, también debe considerarse que están en juego, desde la perspectiva de la parte requirente, las garantías de acceso a la jurisdicción y la tutela judicial efectiva, ambas de raigambre constitucional[7].

Por otro lado, en cuanto a la naturaleza de las medidas de prueba anticipada también se ha dicho que con este tipo de diligencias *"(...) se cumplen medidas cautelares tendientes a recoger pruebas útiles para un proceso futuro o en trámite. No*

se trata de asegurar el cumplimiento futuro de la sentencia (...) sino de posibilitar su solución conservando pruebas (...) Sólo si se comprueba que la parte que la propone está expuesta a perder la prueba o que ésta pueda resultar imposible o muy dificultosa en el período de prueba, se admitirá la producción anticipada"[8].

Es decir, las medidas de prueba anticipada tendientes a asegurar la producción de documentos electrónicos constituyen medidas cautelares y, como tales, serán procedentes en la medida en que la parte requirente pruebe la existencia de verosimilitud en el derecho, el peligro en la demora y otorgue suficiente contracautela.

Sin embargo, es útil resaltar que a diferencia de los documentos que existen de forma física y se encuentran por ejemplo impresos en papel, para asegurar la producción de documentos electrónicos no es necesario realizar su secuestro sino que es posible tan sólo realizar una copia digital de seguridad o una copia de back up. Una copia que será idéntica a su original. En tales casos, en principio[9], no será necesario el secuestro de los documentos ni de los servidores en los que los documentos se encuentren almacenados.

En ese sentido, y haciendo referencia al resguardo de documentos electrónicos contenidos en dispositivos del demandado, se ha dicho que *"(...) el secuestro, normalmente, procede en forma complementaria a un embargo, cuando éste, por sí solo, no asegura el derecho del solicitante. Por lo tanto, es obvio que, para que resulte admisible un secuestro de bienes (...) es necesario que se encuentren reunidos y acreditados los presupuestos que habilitarían el dictado de una medida de embargo"*[10].

Como hemos dicho, ni el embargo ni el secuestro de los documentos electrónicos resulta necesario para asegurar la prueba, aunque en algunos supuestos si lo será.

Basta con que el juez o secretario del tribunal verifiquen ellos mismos la existencia de los documentos electrónicos, dando fe de su existencia y contenido, o con que se nombre un experto informático para que realice una copia de los documentos requeridos y los acompañe al tribunal a fin de que puedan ser consultados por los interesados en el momento que sea oportuno. Así lo han decidido los tribunales al ordenar el nombramiento de un perito ingeniero en sistemas para que *"(...) compulse los sistemas informáticos de la demandada (...) [a partir de los cuales deberá] realizar un 'back up' de todos los correos electrónicos que tengan al actor (...) por remitente o destinatario (...) que quedará reservado en el juzgado para que en la etapa de producción de la prueba se realice (...) la pericia correspondiente (...)"*[11].

La consecuencia práctica de esta diferencia, que implica que el demandado también quede en posesión de los documentos electrónicos y los dispositivos de almacenamiento, debiera ser que la interpretación de los requisitos de admisibilidad de la medida preliminar debiera ser morigerada y, en caso de duda, de acuerdo con la importancia que tales documentos tengan para la resolución del conflicto, estarse a favor de su admisibilidad.

Para el supuesto en que sea necesario proceder al secuestro de los equipos, como podría ser el caso de un servidor, una computadora o un teléfono celular -que en la mayoría de los supuestos serán bienes muebles de propiedad del demandado que éste utilizará en el ejercicio de su actividad económica y que se encuentran amparados por el derecho de propiedad-, sería conveniente solicitarle al tribunal la realización de una pericia informática sobre los equipos a fin de evitar *"(...) correrse el riesgo que la eventual dilación del proceso conlleve a privar a la accionada no sólo del uso y goce de bienes de su propiedad sino que, incluso, podría afectarse su valor e importancia por el mero transcurso del tiempo"*[12].

También resulta necesario marcar otra diferencia de importancia al considerar un pedido de medida de prueba anticipada. Tal como lo ha reconocido la jurisprudencia, en aquellos supuestos en los que la parte requirente se limita a solicitar el resguardo de documentos electrónicos mediante una copia de seguridad o back up, el requirente *"(...) no pretende la producción de la prueba pericial informática (...) lo concreto es que su solicitud se dirige a asegurar la obtención de elementos de información necesarios para la posterior producción de tal medio probatorio"*[13].

Por otro lado, sobre la base de distintos precedentes[14], también deberá el peticionante explicar al tribunal las razones por las cuales la medida intentada es el único o más efectivo medio probatorio para resguardar los documentos electrónicos a fin de evitar su extravío, pérdida, alteración o eliminación antes de que puedan ser utilizados en un juicio.

De lo contrario, existen casos en los que los tribunales han rechazado medidas de prueba anticipada argumentando que *"(...) existen otros medios, que puede utilizar la parte actora para procurar la realización de dicha prueba, incluso en el transcurso del trámite del expediente, durante la etapa de conocimiento"*[15]. En ese caso, el tribunal tuvo en cuenta que parte de los documentos e información que se intentaba resguardar por medio de la medida solicitada estaban en poder de la propia requirente o eran registros públicos de NIC Argentina[16], motivo por el cual consideró que existían otros medios de prueba para acceder a los documentos electrónicos.

En algunos casos, los menos, los tribunales han hecho mención a cuáles otros serían los medios probatorios al alcance de la parte requirente. Lamentablemente, en otros, los tribunales no han sido claros en cuanto a cuales medios proba-

torios, con excepción de intentar idéntica medida en la etapa de prueba, serían medios de prueba alternativos y eficaces para cumplir idéntico fin.

Por último, el hecho de que la parte requirente solicite que la medida de prueba anticipada sea ordenada inaudita parte no debiera presentar ninguna dificultad desde un punto de vista del derecho de defensa del destinatario de la medida. Tampoco desde lo prescripto por el art. 327 del CPCCN en tanto dispone que si hubiere de practicarse la prueba se citará a la contraria, salvo cuando resultare imposible por razón de urgencia, en cuyo caso intervendrá el defensor oficial.

Con fundamento en la importancia del factor sorpresa los tribunales han ordenado las medidas de forma inaudita, estimando que el hecho de que la medida deba realizarse en el domicilio del demandado es una circunstancia suficiente para tener por cumplido lo establecido por el art. 327 del CPCCN.

En ese sentido, se ha dicho que *"(...) teniendo en cuenta que la medida se realizará en el domicilio de la empresa demandada y que por tanto tomará en dicha ocasión conocimiento directo de la medida decretada y podrá fiscalizar la diligencia ordenada, dicha circunstancia permite tener por cumplido el recaudo exigido (...) tornándose innecesaria la intervención del Ministerio Público de la Defensa (...)"*[17].

A todo evento, si existiera alguna duda, y a fin de asegurar que la medida sea ejecutada de la forma más efectiva posible, pareciera una mejor opción citar al Defensor Oficial y no a la parte demandada. Así lo entendió un tribunal comercial al sostener que *"[c]omo la citación previa de la contraria, de acuerdo a las características que presenta el caso, podría entorpecer la concreción de la medida dispuesta, deberá el juez de grado citar al Defensor Oficial de acuerdo lo previsto por el CPr: 327"*[18].

En este primer capítulo nos hemos referido a algunas consideraciones generales respecto de las medidas de prueba anticipada sobre el resguardo de documentos electrónicos.

A continuación analizaremos algunos casos judiciales recientes concentrando nuestra atención en los motivos por los cuales los tribunales conceden o rechazan este tipo de medidas.

II. Fallos recientes

a) "Bueti Rosana Cristina c. EYG Medical System SRL" [19]
La parte actora solicitó, como medida de prueba anticipada, el nombramiento de un experto en sistemas para realizar un reconocimiento judicial y una pericia sobre una serie de correos electrónicos[20] que fueron también acompañados como copia simple.

El tribunal de primera instancia rechazó el pedido lo que fue más tarde confirmado por la Cámara Laboral.

En particular, la Cámara sostuvo que la procedencia de este tipo de requerimientos se encuentra condicionada por la ley adjetiva a la existencia de motivos justificados respecto de la pérdida del material probatorio en cuanto a su producción con anterioridad a la etapa de prueba (art. 326 del CPCCN).

En tal sentido, sostuvo que la parte actora no explicitó de modo concreto y circunstanciado (cuál es o) cuáles son los motivos objetivos que justificarían la producción anticipada, sosteniendo que constituye una mera conjetura la afirmación de "presumir" que la demandada, una vez notificada de la acción, *"seguramente intentará destruir, modificar o mutilar la afirmación contenida en los correos electrónicos (...)"*.

En decir, el tribunal puso en cabeza de la parte actora el probar que el destinatario de la medida intentará alterar o eliminar los documentos electrónicos que podrían eventualmente desmejorar su posición en un litigio.

Por esta razón, la ausencia de fundamentos válidos para temer que los documentos electrónicos pudieran verse alterados o eliminados antes de la etapa de prueba, confirmó lo decidido en primera instancia.

b) "Muñoz Leonardo Ariel c. ARCOR S.A."[21]
En este segundo caso la parte actora solicitó el dictado de una medida de prueba anticipada tendiente a realizar una pericia informática sobre ciertos documentos electrónicos en poder de la demandada.

El tribunal de primera instancia rechazó el pedido lo que fue más tarde confirmado en apelación por la Cámara Laboral.

Para así decidir, y luego de recordar que el art. 326 del CPCCN contempla un modo excepcional de producción de prueba -que depende de la urgencia y circunstancias particulares de cada caso-, y que este tipo de medidas solo procede si quien propone la prueba que está expuesta a perderla o que su producción en tiempo oportuno pudiera resultar imposible o de muy difícil concreción, la Cámara concluyó que la parte actora no invocó y menos probó la real existencia de peligro en la demora que justifique su dictado, por lo que confirmó la decisión de primera instancia.

Al igual que en el caso anterior, la Sala II de la Cámara Laboral rechaza la medida de prueba anticipada por no haberse probado el peligro en la demora necesario para el dictado de este tipo de medidas.

c) "Levin Ricardo c. Taraborelli Automobile"[22]

En lo que aquí interesa el actor solicitó como medida de prueba anticipada la designación de un perito ingeniero en sistemas a fin de que teniendo acceso a ciertos documentos electrónicos almacenados en servidores ubicados en las oficinas de la parte demandada se expidiera sobre ciertos puntos de pericia.

La medida solicitada fue rechazada en ambas instancias.

En particular, la Cámara Laboral concluyó que la requirente no individualizó de modo alguno las circunstancias de excepción que habilitarían un apartamiento de las etapas normales del proceso y de la bilateralidad, como así tampoco, *"(...) el concreto riesgo de que se alteren los elementos probatorios o que no existan otros medios probatorios al alcance del accionante"*.

En este caso, la medida de prueba anticipada fue rechazada por no haberse acreditado el peligro en la demora y por no haber el actor indicado de forma concreta cuales eran las circunstancias específicas del caso que aconsejaban apartarse de las etapas normales del proceso.

De todos modos, como hemos analizado en la introducción, el mero hecho de solicitar una copia de seguridad o back up -sin solicitar la producción de una prueba pericial sobre dichos documentos electrónicos- no debiera interpretarse como un apartamiento de las etapas normales del proceso porque el requirente en esos casos no pretende la producción de la prueba pericial sino asegurar la obtención de los documentos electrónicos que permitirán su producción en la etapa correspondiente[23].

d) "Powell Hugo Francisco c. Willis Corredores de Reaseguros"[24]

A fin de probar su relación laboral con la parte demandada y que ésta última estaría cometiendo fraude a la ley laboral, la parte actora solicitó el nombramiento de un experto en sistemas para realizar una copia de back up de distintos correos electrónicos almacenados en los sistemas informáticos de la demandada.

Le medida fue chazada por el tribunal de primera instancia. La Sala X de la Cámara Laboral revocó la decisión de primera instancia e hizo lugar al pedido de la parte actora aunque con un alcance más limitado del solicitado.

Para así decidir, tuvo por acreditado el temor de la parte actora sobre la dificultad de producir la prueba en la etapa procesal oportuna en el hecho de que la información contenida en los servidores de correo electrónico podría modificarse o destruirse, lo que justificaba el dictado de la medida solicitada.

Asimismo, consideró que los documentos individualizados por la parte actora podrían ser de fundamental importancia para acreditar el pago de salarios no registrados y realizados por la empresa a su favor en el exterior, en fraude a la ley laboral argentina. Es decir, le dio una especial trascendencia a la importancia que tales documentos podrían tener para la resolución del posible conflicto.

Por esas razones ordenó al tribunal de primera instancia nombrar un perito ingeniero en sistemas para que realice una copia de back up de determinados correos electrónicos y luego deposite dicha copia en el tribunal para oportunamente realizar una pericia sobre los mismos.

Este precedente resulta de importancia al reconocer que los documentos electrónicos, dada su propia naturaleza, son susceptibles de sufrir modificaciones o destruirse, circunstancia que aconseja acceder a su resguardo por medio de una medida de prueba anticipada en tanto que, como también se reconoce en el fallo, su resguardo sea de importancia a los fines de la resolución del conflicto.

e) "García Porcel de Peralta c. The Walt Disney Company"[25]

En este caso, y frente al temor de que ciertos documentos electrónicos en poder de la demandada pudieran destruirse, extraviarse o perderse, la parte actora solicitó el dictado de una medida de prueba anticipada tendiente a resguardar tales documentos.

El pedido fue rechazado en primera instancia y concedido por la Cámara en apelación.

En particular, la medida tenía por fin resguardar una serie de correos electrónicos que según la peticionante acreditarían la jornada laboral realizada y el acoso laboral sufrido.

Para así decidir, la Cámara Laboral tuvo especial consideración a la naturaleza de la relación que se invocó, la índole del trato persecutorio al que se refería la parte actora y conductas que le atribuyó a la demandada, las peculiares caracte-

rísticas de los elementos probatorios que se pretende resguardar, como así también la raigambre de las garantías de acceso a la jurisdicción y tutela judicial efectiva.

Por último, toda vez que la medida decretada debía practicarse en el domicilio de la parte demandada -momento en el cual tomaría noticia y podría fiscalizarla la medida de forma efectiva-, tuvo por cumplido los recaudos del art. 327 CPCCN en tanto establece la necesidad de citar al demandado.

En este caso, al igual que en el que comentamos en el punto anterior, se hace especial hincapié en las especiales características de los documentos electrónicos. Y si bien no se lo menciona de forma expresa, la forma en la que se decide permite inferir que el tribunal se refiere -como en otros precedentes- a la posibilidad cierta de que los documentos electrónicos pudieran verse alterados, modificados o eliminados con cierta facilidad, lo que resulta una circunstancia válida para tener por acreditado el peligro en la demora necesario para conceder una medida de prueba anticipada.

f) "Softmind Sistema c. Cardoso Cristian Hugo"[26]

La parte actora solicitó el dictado de una medida de prueba anticipada a fin de obtener una copia de toda la información contenida en los discos rígidos de las computadoras de uno de los demandados con el fin de resguardar tales documentos electrónicas y realizar una pericia informática en la etapa de prueba. La parte actora argumentó que esos documentos probarían las maniobras de mala fe que imputaba a los demandados.

El pedido fue rechazado en primera instancia y concedido por la Cámara Comercial en apelación.

En particular, la Cámara sostuvo que con fundamento en las circunstancias expuestas por el actor al expresar agravios se *"(...) torna razonable entender el temor de que los demandados realicen cambios o alteraciones en sus registros informáticos una vez conocida la existencia del juicio y antes de la etapa probatoria", concluyendo que resulta "(...) prudente, ante el claro riesgo de poder frustrarse la producción de las pruebas periciales ofrecidas, admitir la obtención de una copia o back up de toda la información contenida o almacenada en los discos rígidos (...)"* de Mindsap Consulting SRL con la intervención de un perito en informática y acompañado del oficinal de justicia.

Por último, sostuvo que atento a que la notificación de la medida al demandado podría entorpecer su concreción, el tribunal de primera instancia debería citar al Defensor Oficial.

En este caso también, el temor fundado de que los documentos electrónicos a resguardar pudieran verse alterados por los demandados antes de la etapa de prueba resultó un motivo suficiente para acceder a su resguardo mediante la obtención de una copia de seguridad o back up.

g) "Aguilar y Asociados SRL c. Native Software"[27]

En este último caso, la parte actora solicitó una medida de prueba anticipada tendiente a obtener una copia de seguridad de los sistemas informáticos de la demandada.

En el entendimiento de que la mera invocación de la posibilidad de adulteración de la prueba a resguardar no era suficiente para justificar el dictado de la medida solicitada, el tribunal de primera instancia la rechazó. Asimismo, tuvo en consideración que el proceso de mediación previa obligatoria había concluido por voluntad de las partes un año antes del pedido de la parte actora, lo que a su entender demostraba la ausencia de urgencia o peligro en la demora.

En apelación, la Cámara Comercial resaltó que la parte actora no había solicitado la producción de una prueba pericial informática sino el resguardo de aquellos documentos electrónicos que oportunamente permitirían realizar una pericia. Sobre esa base, entendió que el pedido de la parte actora aparecía verosímil ante la *"(...) necesidad de obtener una medida como la de la especie con el claro propósito de aventar el ulterior ocultamiento, modificación, destrucción, alteración o pérdida (...)" de tales documentos, sobre todo en esta particular temática "(...) donde la vulnerabilidad y fragilidad que los registros informáticos permiten presuponer el peligro en la demora (...)".*

En consecuencia, hizo lugar a la medida solicitada ordenado citar al Defensor Oficial ya que la citación al demandado podría posibilitar la alteración o modificación de la prueba.

La importancia de este precedente radica, por un lado, en el hecho de reconocer la diferencia que existe entre solicitar la producción de una prueba pericial informática como medida de prueba anticipada y requerir únicamente el resguardo de documentos electrónicos que permitirán realizar una pericia en la etapa procesal oportuna. En el segundo supuesto la finalidad es asegurar documentos electrónicos que podrían ser ocultados, modificados, destruidos, alterados o perdidos, con anterioridad a la etapa de prueba. Por otro lado, el fallo reconoce que la propia naturaleza de los documentos electrónicos los torna vulnerables y frágiles, lo que autoriza a presuponer la existencia del peligro en la demora necesario para el dictado de una medida de prueba anticipada.

En este segundo capítulo hemos analizado distintos precedentes que rechazan o hacen lugar a medidas de prueba anticipada con el fin de asegurar ciertos documentos electrónicos y utilizarlos como prueba en la etapa de prueba.

De estos precedentes surge que el criterio de los tribunales para analizar estos pedidos no resulta uniforme y en algunos casos pareciera no comprenderse el importante rol que las medidas de prueba anticipada juegan frente al resguardo de los documentos electrónicos dada su propia naturaleza.

III. Conclusión

Como hemos visto existe un uso cada vez mayor de distintos tipos de computadoras y dispositivos móviles y la tendencia es que este uso se incremente exponencialmente con el paso del tiempo. Estos equipos permiten generar un sinnúmero de documentos electrónicos.

Estos documentos, por su propia naturaleza, son susceptibles de sufrir modificaciones o destruirse. Dada su cada vez mayor importancia en juicio, el hecho de que puedan modificarse o eliminarse antes de ser utilizados como prueba, aconseja acceder a su resguardo por medio de una medida de prueba anticipada en la medida en que, como lo reconoce la jurisprudencia, su resguardo sea de importancia a los fines de la resolución de un conflicto. (28)

Estas medidas de prueba anticipada tienen como objetivo principal evitar el extravío, pérdida, alteración o eliminación de la prueba antes de que pueda ser utilizada en un juicio.

El principal temor de quién la solicita es que el demandado o destinatario de la medida intente obstaculizar el acceso a los documentos una vez anoticiado de la medida, lo que en la práctica ha significado que el demandado tome conocimiento de la medida en el momento de su ejecución[29].

Asimismo, existe un temor cierto de que los documentos electrónicos pudieran extraviarse o perderse dada la vulnerabilidad y fragilidad de los registros informáticos, lo que ha permitido presuponer la existencia del peligro en la demora necesario para conceder una medida de prueba anticipada[30]. En otros casos, la ausencia de prueba sobre la posibilidad de que los documentos pudieran verse alterados ha sido suficiente para rechazar la medida[31].

Por otro lado, los tribunales han hecho hincapié en que las medidas de prueba anticipada son un modo excepcional de producción de prueba antes de la etapa oportuna y que solo deben ser admitidas si el requirente prueba que los documentos a resguardar están expuestos a perderse o pudiere resultar imposible o muy dificultosa su producción[32].

Relacionado con esto último los tribunales también han reconocido que a través de las medidas de prueba anticipada se cumplen medidas cautelares que tienen por fin conservar pruebas[33] y respecto de las cuales la parte requirente debe probar la existencia de verosimilitud en el derecho, el peligro en la demora y otorgar suficiente contracautela.

No obstante ello, los tribunales también han marcado la diferencia que existe entre solicitar la producción de una prueba pericial informática como medida de prueba anticipada y requerir únicamente el resguardo de documentos electrónicos que permitirán realizar una pericia en la etapa procesal oportuna[34]. En este segundo supuesto no se trataría de la producción de prueba anticipada per se sino del resguardo de ciertos documentos electrónicos para poder hacerlos valer en la etapa de prueba. Esta diferencia debiera ser fundamento válido para morigerar la interpretación de los requisitos de admisibilidad de la medida preliminar[35].

Asimismo, resulta útil recordar que el peticionante de la medida deberá explicar al tribunal de forma clara y concreta cuales son las razones que hacen a la medida solicitada el único o más efectivo medio probatorio para resguardar los documentos electrónicos[36].

Como hemos analizado, que los tribunales hagan lugar o rechacen una medida de prueba anticipada tendiente a resguardar documentos electrónicos dependerá en gran medida de las circunstancias adjetivas de cada caso en particular, siendo las más relevantes la importancia que tales documentos tengan para la eventual resolución de un conflicto y el peligro de que ellos pudieran verse alterados o eliminados antes de la etapa de prueba.

Mientras no exista jurisprudencia más uniforme sobre su tratamiento confiamos en que los tribunales harán sus mejores esfuerzos para comprender el importante rol que las medidas de prueba anticipada juegan respecto de los documentos electrónicos.

Este artículo se encuentra publicado en LA LEY 31/07/2014, 31/07/2014, 1 - LA LEY2014-D, 998. **Cita Online:** AR/DOC/475/2014

(1) En ese sentido, se ha tenido especial consideración en las "(...) conductas que se le atribuyen a la demandada (...)" (CNTrab., Sala IX, Expte. No. 1422/2013, "García Porcel de Peralta María Cecilia c. The Walt Disney Company Argentina S.A. s/despido", sentencia del 20/09/2013).

(2) CNCom., Sala F, Expte No. 38813/2011, "Aguilar y Asociados SRL c. Native Software SRL s/ordinario", sentencia del 17/04/2012.

(3) CNCom., Sala B, Expte. No. 45341/2010, "Coppola Juan Carlos c. Okal S.A. y otros s/incidente de apelación art. 250 CPROC.", sentencia del 13/12/2010; con cita a CNCOM, Sala C, "Nieto Eduardo Arturo c. Editorial La Razón SA y otro s/ diligencia preliminar", sentencia del 24/02/2006 y CNCOM, Sala de Feria, "DVA Agro GMBH c. Ciagro SRL s/diligencia preliminar", sentencia del 28/01/2009.

(4) CNCom., Sala D, Expte. 37198/2010, "Silk Line SRL c. Visa Argentina S.A. y otro s/diligencia preliminar", sentencia del 17/11/2010 -aunque en este caso se rechazó la medida de prueba anticipada sobre la base de que la medida debía realizarse en las oficinas de parte actora, motivo por el cual no se advertía de qué manera la parte demandada podía entorpecer su ejecución una vez notificada; con cita a FALCÓN, Enrique M., Código Procesal Civil y Comercial de la Nación, Abeledo Perrot, T. I, p. 538, cit. por CNCiv., Sala J, "Asociación de Beach Soccer Argentina c. Asociación del Fútbol Argentino", sentencia del 17/05/2007; KIELMANOVICH, Jorge L., Código Procesal Civil y Comercial de la Nación, comentado y anotado, Buenos Aires, 2005, T. I, p. 563 y jurisp. cit. en nota n° 2110; CNCom., Sala B, "Doña Asunción S.A. c. Berry Group S.A. y otros", sentencia del 26/11/2009; CNCiv., Sala J, "Pardo, Rubén Ricardo c. Fernández, Juan Carlos s/medidas precautorias, sentencia del 15/08/2006.

(5) Distinto es el caso en el que los documentos están alojados en servidores pertenecientes a la parte actora o a un tercero respecto del cual en principio no existen razones para suponer que el demandado pudiera tener acceso y control como para ocultar, modificar, destruir, alterar o hacer perder los documentos electrónicos.

(6) CNTrab., Sala II, Expte. No. 47737/2013, "Muñoz Leonardo Ariel c. ARCOR S.A. s/diligencia preliminar", sentencia del 24/10/2013.

(7) CNTrab., Sala IX, Expte. No. 1422/2013, "García Porcel de Peralta María Cecilia c. The Walt Disney Company Argentina S.A. s/despido", sentencia del 20/09/2013.

(8) FASSI, Santiago C. y MAURINO Alberto L., Código Procesal Civil y Comercial, Comentado, Anotado y Concordado, tomo 3, pp. 84 y 85, Ed. Astrea, Bs. As., 2002.

(9) Decimos en principio porque podría darse el caso en el que los documentos a asegurar sean tantos o su almacenamiento precise de un dispositivo de tanta capacidad, que no sea posible su copia y se deba considerar la posibilidad del secuestro del servidor en el que los documentos se encuentran alojados.

(10) CNTrab., Sala II, Expte. No. 47737/2013, "Muñoz Leonardo Ariel c. ARCOR S.A. s/diligencia preliminar", sentencia del 24/10/2013.

(11) CNTrab., Sala X, Expte. No. 17258/2012, "Powell Hugo Francisco c. Willis Corredores de Reaseguros S.A. y otro s/diligencias preliminares", sentencia del 28/06/2012.

(12) CNTrab., Sala III, Expte. No. 28418/2010, "Palavecino Favio Néstor c. Carl Zeiss Argentina S.A. s/diligencia preliminar", sentencia del 29/10/2012.

(13) CNCom., Sala F, Expte No. 38813/2011, "Aguilar y Asociados SRL c. Native Software SRL s/ordinario", sentencia del 17/04/2012.

(14) CNTrab., Sala IX, Expte. No. 158/2012, "Levin Ricardo Javier c. Taraborelli Automobile S.A. s/diligencia preliminar", sentencia del 24/05/2012; y CNTrab., Sala VII, Causa No. 23539/2011, "Heberle Karina Soledad c. Caktus S.A. s/diligencia preliminar", sentencia del 30/9/2011.

(15) CNTrab., Sala VII, Causa No. 23539/2011, "Heberle Karina Soledad c. Caktus S.A. s/diligencia preliminar", sentencia del 30/9/2011.

(16) Nombre con el cual se conoce a la entidad encargada de registrar los nombres de dominio de código país .AR.

(17) CNTrab., Sala IX, Expte. No. 1422/2013, "García Porcel de Peralta María Cecilia c. The Walt Disney Company Argentina S.A. s/despido", sentencia del 20/09/2013; en igual sentido CNTrab., Sala X, "Matos Carlos Alberto c. Azertia Tecnologías de la Información S.A. s/despido", sentencia del 26/03/2010.

(18) CNCom., Sala E, Expte. No. 22439/2011, "Softmind Sistema S.A. c. Cardoso Cristian Hugo y otros s/diligencia preliminar", sentencia del 17/11/2011; en igual sentido CNCom., Sala F, Expte No. 38813/2011, "Aguilar y Asociados SRL c. Native Software SRL s/ordinario", sentencia del 17/04/2012. En sentido contrario ver CNCom., Sala A, Expte. No. 34776/2010, "Royal Vending S.A. c. Cablevisión S.A. y otro s/ordinario", sentencia del 17/02/2011.

(19) CNTrab., Sala X, Expte. No. 16857/2013, "Bueti Rosana Cristina c. EYG Medical System SRL y otro s/diligencia preliminar", sentencia del 26/08/2013.

(20) La problemática sobre el acceso a correos electrónicos en tanto equiparados a la correspondencia epistolar protegida por la Constitución Nacional escapa al alcance de este trabajo.

(21) CNTrab., Sala II, 47737/2013, "Muñoz Leonardo Ariel c. ARCOR S.A. s/diligencia preliminar", sentencia del 24/10/2013.

(22) CNTrab., Sala IX, Expte. No. 158/2012, "Levin Ricardo Javier c. Taraborelli Automobile S.A. s/diligencia preliminar", sentencia del 24/05/2012.

(23) CNCom., Sala F, Expte. No. 38813/2011, "Aguilar y Asociados SRL c. Native Software SRL s/ordinario", sentencia del 17/04/2012.

(24) CNTrab., Sala X, Expte. No. 17258/2012, "Powell Hugo Francisco c. Willis Corredores de Reaseguros S.A. y otro s/diligencias preliminares", sentencia del 28/06/2012.

(25) CNTrab., Sala IX, Expte. No. 1422/2013, "García Porcel de Peralta María Cecilia c. The Walt Disney Company Argentina S.A. s/despido", sentencia del 20/09/2013.

(26) CNCom., Sala E, Expte. No. 22439/2011, "Softmind Sistema S.A. c. Cardoso Cristian Hugo y otros s/diligencia preliminar", sentencia del 17/11/2011.

(27) CNCom., Sala F, Expte No. 38813/11, "Aguilar y Asociados SRL c. Native Software SRL s/ordinario", sentencia del 17/04/2012.

(28) CNTrab., Sala X, Expte. No. 17258/2012, "Powell Hugo Francisco c. Willis Corredores de Reaseguros S.A. y otro s/diligencias preliminares", sentencia del 28/06/2012.

(29) CNCom., Sala E, Expte. No. 22439/2011, "Softmind Sistema S.A. c. Cardoso Cristian Hugo y otros s/diligencia preliminar", sentencia del 17/11/2011; y CNCom., Sala F, Expte. No. 38813/11, "Aguilar y Asociados SRL c. Native Software SRL s/ordinario", sentencia del 17/04/2012.

(30) CNCom., Sala F, Expte No. 38813/2011, "Aguilar y Asociados SRL c. Native Software SRL s/ordinario", sentencia del 17/04/2012.

(31) CNTrab., Sala II, 47737/2013, "Muñoz Leonardo Ariel c. ARCOR S.A. s/diligencia preliminar", sentencia del 24/10/2013; y CNTrab., Sala X, Expte. No. 16857/2013, "Bueti Rosana Cristina c. EYG Medical System SRL y otro s/diligencia preliminar", sentencia del 26/08/2013.

(32) CNTrab., Sala II, Expte. No. 47737/2013, "Muñoz Leonardo Ariel c. ARCOR S.A. s/diligencia preliminar", sentencia del 24/10/2013.

(33) FASSI, Santiago C. y MAURINO Alberto L., Código Procesal Civil y Comercial, Comentado, Anotado y Concordado, tomo 3, pp. 84 y 85, Ed. Astrea, Bs. As., 2002.

(34) CNCom., Sala F, Expte. No. 38813/11, "Aguilar y Asociados SRL c. Native Software SRL s/ordinario", sentencia del 17/04/2012; y CNTrab., Sala IX, Expte. No. 158/2012, "Levin Ricardo Javier c. Taraborelli Automobile S.A. s/diligencia preliminar", sentencia del 24/05/2012.

(35) CNCom., Sala F, Expte No. 38813/2011, "Aguilar y Asociados SRL c. Native Software SRL s/ordinario", sentencia del 17/04/2012.

(36) CNTrab., Sala IX, Expte. No. 158/2012, "Levin Ricardo Javier c. Taraborelli Automobile S.A. s/diligencia preliminar", sentencia del 24/05/2012; y CNTrab., Sala VII, Causa No. 23539/2011, "Heberle Karina Soledad c. Caktus S.A. s/diligencia preliminar", sentencia del 30/9/2011.

EL CORREO ELECTRÓNICO COMO PRUEBA EN LA JURISPRUDENCIA Y EN EL PROYECTO DE CÓDIGO CIVIL Y COMERCIAL DE LA NACIÓN

Por Agustín Bender

I. Documento electrónico y correo electrónico. — **II.** Firma electrónica. — **III.** Firma digital. — **IV.** Documentos no firmados. — **V.** Documentos con firma electrónica reconocida. — **VI.** Efectos de la firma electrónica reconocida o validada. — **VII.** Prueba anticipada. — **VIII.** Necesidad de acompañar una copia de los correos. — **IX.** Necesidad de probar la recepción. — **X.** La prueba. — **XI.** Inferencias y sana crítica. — **XII.** Teoría de los propios actos. — **XIII.** Informativa. — **XIV.** Testimonial. — **XV.** Pericial sobre sistema propio. — **XVI.** Pericias sobre sistema de la contraparte. — **XVII.** Control de la casilla. — **XVIII.** Conclusiones.

I. Documento electrónico y correo electrónico

La ley de Firma Digital (en adelante LDFD), en su artículo 6to., define al documento electrónico como la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. La ley habla de documento digital y no de documento electrónico pero el decreto reglamentario Nro. 2628/2002 en el punto 3 del glosario y en sus arts. 4, 16 y 42, define y utiliza ambos términos como sinónimos.

De acuerdo al contexto en que se lo mencione, podría entenderse como correo electrónico, en sentido amplio, cualquier sistema de mensajería electrónica como los mensajes enviados a través de las redes Facebook, BlackBerry Messenger, Whatsapp, SMS, etc.

Sin embargo, a los efectos de este trabajo, se hace referencia al correo electrónico como el sistema de mensajería electrónica más utilizado actualmente para transacciones comerciales, y que habitualmente se denomina e-mail o correo electrónico a secas, que es el que utiliza el "Simple Mail Transfer Protocol" o protocolo SMTP definido actualmente por la Internet Engineering Task Force (ietf.org) en el estándar RFC 5321[1] de octubre de 2008 que evolucionó a partir del el estándar RFC 821 escrito por Jonathan B. Postel en Agosto de 1982, para la red ARPANET.

El correo electrónico es un medio de comunicación y como tal permite el envío de documentos (electrónicos) que pueden instrumentar actos y hechos jurídicos. Estos documentos, al ser electrónicos, satisfacen el requerimiento legal de escritura, como lo señala el art. 6 in fine de la LDFD, y por lo general, están firmados electrónicamente al indicar el nombre y/o el nombre de usuario del autor.

Sin embargo, la firma electrónica no puede ser validada con las mismas técnicas con que se validan los documentos en soporte papel ya que en el soporte electrónico se carece de trazos personales de escritura para cotejar la autoría y que la existencia de múltiples ejemplares en poder del emisor y receptor, no garantiza integridad por cuanto se puede agregar, modificar y borrar información del documento sin dejar rastros.

En consecuencia, deberá evaluarse la confiabilidad de los soportes utilizados y de los procedimientos técnicos aplicados para determinar si razonablemente permiten acreditar la autoría, integridad y recepción de los documentos, tal como ahora lo sostiene el Proyecto de Código Civil y Comercial de la Nación[2].

II. Firma electrónica

La ley de firma digital define la firma electrónica como el *"...conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital..." y establece que "En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez."* (Art. 5 LDFD).

El concepto de firma electrónica es muy amplio e incluye cualquier dato que utilice el emisor para identificarse, como su nombre al pié del correo, un membrete en el cuerpo del mensaje, un nombre de usuario, su firma ológrafa escaneada o simplemente el nombre de su casilla de correo[3].

Por ello, si la firma electrónica es técnicamente insegura, podrá acudirse a todo tipo de medios de prueba para acreditar su validez.

Siempre que el signatario haya asociado algún dato al mensaje que esté destinado inequívocamente a identificarlo, puede ser considerado firma electrónica en los términos del art. 5 LDFD, siempre y cuando, o bien sea reconocida por el signatario, o bien quién la alega consiga acreditar su validez.

En este sentido, en los autos **"Bieniauskas, Carlos c. Banco de la Ciudad de Buenos Aires"** se ha considerado como firma electrónica, la contraseña utilizada en un cajero automático ("No está de más recordar que tal clave -numérica en el caso-, ostenta la calidad de firma electrónica, a la luz de lo dispuesto por la ley 25.506 -artículo 5-. Si bien no tiene los mismos efectos de la firma digital -art. 3 de la norma citada-, no puede ignorarse que tal clave tiene amplio uso en nuestra vida diaria amén de tener por finalidad, bien que no única, la identificación del cliente, como ocurre con la firma ológrafa. De hecho, esta clave personal o firma electrónica es constantemente utilizada para múltiples actividades, muchas de ellas de claro contenido económico. Uso que se ha generalizado a partir de la llamada "bancarización". No sólo permite realizar múltiples transacciones a través del cajero automático, sino compras o pagos de servicios mediante su combinación con la tarjeta de débito o de crédito, la conexión "on line" con el Banco para realizar transacciones remotas -home banking-, acceso a bases de datos por vía de Internet, etc. En rigor, hasta la clave que utilizamos para ingresar en una red local y así operar el sistema de gestión aplicado a una determinada tarea, ora en la función pública ora en la empresa privada, es una firma electrónica con los alcances ya indicados, en tanto nos identifica como usuarios del sistema y nos habilita para operar, con cierto nivel de seguridad, el sistema al que accedemos. También permite que, frente a una auditoria, pueda ser atribuida responsabilidad al usuario que infringió normas internas o utilizó el recurso para finalidades impropias" -CNCom. Sala D, autos: "Bieniauskas, Carlos c. Banco de la Ciudad de Buenos Aires", LA LEY 21/07/2008, 3, con nota de Juan Manuel Prevot-).

III. Firma digital

Sin perjuicio de la definición que brinda la LDFD[4], podríamos sintetizar el concepto de Firma Digital como una implementación técnica de firma electrónica reglada por el Estado, que permite verificar la autoría e integridad de los documentos con un altísimo grado de fiabilidad, de forma tal que la ley invierte la carga probatoria y quién pretende desconocer la autoría o integridad del documento debe probarlo.

Los requisitos que impone el Estado para considerar una firma electrónica como firma digital son complejos, burocráticos y costosos por lo cual la firma digital entre privados no se ha extendido en nuestro país.

Si estuviese más difundido, la prueba en juicio de los documentos electrónicos firmados digitalmente (sean enviados por correo electrónico o no) sería muy sencilla ya que las tecnologías involucradas son muy seguras.

La seguridad que brindan es reconocida por la Ley de Firma Digital (en adelante LDFD) estableciendo en sus arts. 7 y 8, la presunción legal citada, de que las firmas digitales que pasan el proceso de verificación (que es muy sencillo), pertenecen al titular y que el documento no ha sido modificado.

En este sentido, en los autos **"Bunker Diseños SA c/IBM Argentina SA s/ordinario"** se sostuvo que *"...en el valor probatorio del correo electrónico, ocupan un lugar preeminente a partir de la vigencia de la Ley 25506, los documentos con firma digital, en tanto su valor probatorio es equiparable al de los instrumentos privados, y se presume la autoría e integridad del*

mensaje, correspondiendo a la otra parte destruir tales presunciones..." (cfr. Hocsman, H., "Negociosen Internet", cap. II, nro.63.b., pgs. 162/164, ed. 2005 cit. por CNCom. Sala D, 2/03/10).

Es decir que si los documentos estuviesen firmados digitalmente, la autoría del documento por quién figura como autor y la integridad del mismo se presumiría. El fallo asimila tales efectos a los del instrumento privado cuando en realidad la presunción de veracidad e inversión de la carga probatoria de que gozan, los asemeja más a los instrumentos privados reconocidos cuyos efectos son equivalentes a los de los instrumentos públicos (Art. 1026 del Código Civil).

IV. Documentos no firmados

Los documentos con firmas ológrafas, cuyas firmas no fueron reconocidas ni su autenticidad probada por otros medios, no surten el efecto propio de los instrumentos privados reconocidos cuya eficacia entre partes equivale a la de los instrumentos públicos (Art. 1026 del Código Civil). De la misma forma, un documento electrónico con firma electrónica, respecto del cual no se consigue acreditar la validez de la firma, tampoco surtirá ese efecto entre partes (art. 5 LDFD). Este documento podrá ser considerado como instrumento particular no firmado y su eficacia probatoria será relativa.

Así ha sido interpretado por nuestros tribunales, los cuales sostienen que los correos electrónicos —sin firma reconocida o acreditada— deben ser considerados documentos particulares no firmados o bien principio de prueba por escrito en los términos del art. 1191 Código Civil[(5)].

En estos casos los documentos no tienen, por sí mismos, valor probatorio intrínseco[(6)].

V. Documentos con firma electrónica reconocida

Se han encontrado un alto número de sentencias donde los magistrados valoraron la eficacia probatoria de correos electrónicos por reconocimiento expreso de la contraparte o bien porque esta última omitió negarlos adecuadamente.

En la comentada causa **"Bunker Diseños S.A. c/IBM Argentina S.A. s/Ordinario"** la Sala D de la Cámara Nacional de Apelaciones en lo Comercial de la Capital Federal consideró suficiente para atribuirle la autoría de ciertos correos electrónicos a la demandada IBM, que en los correos electrónicos acompañados por la actora de forma impresa figuraba como dirección del remitente "ibm.com.ar", argumentando que la demandada no había desconocido que los correos hubiesen salido del servidor que gestiona el dominio **ibm.com.ar**[(7)]. Esta sentencia no es más que una consecuencia de la aplicación del famoso aforismo jurídico: "a confesión de parte, relevo de prueba".

En los autos **"García, Delia c/YPF SA s/despido"**, el trabajador discutía la legitimidad de una constatación notarial de su casilla de correo a la cual habría accedido voluntariamente de acuerdo al acta labrada por el escribano.

Del fallo puede inducirse que la casilla de correo estaba alojada en el servidor de la empresa y que por lo tanto debía estar -desde el punto de vista técnico- bajo control de la empleadora, comprometiendo la integridad de los documentos allí existentes, lo cual no habría sido objetado por el trabajador, quién cuestionó la forma en que se obtuvo la prueba pero no su contenido[(8)].

En los autos **"Balocco, Enrique E. y ot. c/ Chiesa, Ariel y otros"**, se sostuvo que no caben mayores disquisiciones para estimar los correos electrónicos reconocidos por ambas partes ya que rigen para su valoración las pautas genéricas del art. 384 del C.P.C.C.[(9)].

VI. Efectos de la firma electrónica reconocida o validada

Se plantea el problema de determinar cuáles son los efectos de la firma electrónica indubitada, es decir, reconocida o validada mediante otras pruebas y si la misma puede equipararse a una firma ológrafa (o manuscrita en los términos de la LDFD) para otorgarle el carácter de instrumento privado al documento digital y por lo tanto equiparable al documento público en sus efectos entre partes (art. 1026 del Código Civil).

Ello se debe a que la LDFD en su artículo 3 establece que cuando la ley requiera una firma manuscrita —o prescriba consecuencias para su ausencia—, esa exigencia también queda satisfecha por una firma digital. El artículo citado habla sólo de firma digital y omite la electrónica, lo cual puede llevar al error de considerar que los documentos que carecen de firma digital, aún los firmados electrónicamente con una firma validada o reconocida, no son instrumentos privados sino instrumentos particulares o principio de prueba por escrito.

Dicha solución sería contradictoria con lo dispuesto en el artículo 5 LDFD que obliga a quién invoca una firma electrónica a acreditar su validez, ya que si se busca acreditar la validez de una firma electrónica, el objetivo claramente será que surta el efecto de la firma manuscrita que es demostrar la existencia de una declaración de voluntad del firmante concordante con el contenido del documento y hacer que entre las partes tenga el mismo valor que una escritura pública (cnfr. Arts. 1028 y 1026 del Código Civil). Sería absurdo legislar la firma electrónica —y llamarla firma— si no es con el objetivo de que surta los efectos propios de una firma.

Este defecto legal es salvado en el artículo 1 del decreto reglamentario 2628/2002 que dice: *"En los casos contemplados por los artículos 3°, 4° y 5° de la Ley N° 25.506 podrán utilizarse los siguientes sistemas de comprobación de autoría e integridad: ...a) Firma electrónica..."*

Es decir que la reglamentación equipara la firma electrónica indubitada a la digital, como sistema de comprobación de autoría e integridad a los efectos del artículo 3 de la LDFD. Lo cual equivale a sostener por el juego armónico de los arts. 3 y 5 LDFD y 1 del decreto reglamentario 2628/2002 que: cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma electrónica, siempre y cuando se acredite su validez[10].

En igual sentido, el art. 288 del Proyecto de Código Civil y Comercial de la Nación dispone que "*En los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho si se utiliza un método que asegure razonablemente la autoría e inalterabilidad del instrumento.*". Esta modificación facilita la prueba de la validez de la firma electrónica cuando se justifica la razonabilidad de las medidas de seguridad empleadas y en tal caso equipara la firma electrónica validada, a la ológrafa reconocida y a la digital.

VII. Prueba anticipada

El Código Procesal Civil y Comercial de la Nación establece en su art. 326 que *"...Los que sean o vayan a ser parte en un proceso de conocimiento y tuvieren motivos justificados para temer que la producción de sus pruebas pudiera resultar imposible o muy dificultosa en el período de prueba, podrán solicitar que se produzcan anticipadamente...*

Pedido de informes...

La exhibición, resguardo o secuestro de documentos concernientes al objeto de la pretensión..."

En diversos precedentes, la fragilidad de la prueba informática y la facilidad con que pueden borrarse y alterarse los archivos ha servido por sí solo como argumento para justificar esta posibilidad de que la prueba desaparezca.

En los autos **"R.P., E.C. c/C.L., S.H. s/Divorcio y exclusión de cónyuge"**, se solicitó una prueba informativa anticipada respecto de información que se encontraba bajo el control de la contraparte.

La sala J de la Cámara Civil consideró que: 1. La facilidad con que los registros informáticos podían ser borrados fácilmente o afectados por "virus" hacían verosímil el peligro en la demora y justificaban la obtención de la prueba informativa de forma anticipada e in audita parte y 2. Que dicha medida —que afecta el derecho de la otra parte sobre su correspondencia privada—, podía ser dispuesta en sede civil[11].

En los autos **"Pardo, Rubén Ricardo c/Fernández, Juan Carlos s/Medidas precautorias"** se hizo lugar a diligencias preliminares por las cuales un perito informático constate la existencia de correos electrónicos en el disco rígido de una computadora de la demandada, in audita parte y designando al Defensor Oficial para que represente a la parte contra la cual se dispuso la medida[12].

En los autos **"DVA AGRO GMBH c/Ciagro SRL s/diligencia preliminar"** se concedió como prueba anticipada la constatación de correos electrónicos en computadoras de la contraparte, incluso autorizando el allanamiento de domicilio, uso de cerrajero y habilitación de feria[13].

En los autos **"Ramírez Gustavo Alejandro y otro c/ Mc Care Company SRL s/diligencia preliminar"** de la Sala VII de la cámara civil, se autorizó el secuestro de los registros de correos electrónicos (junto con los telefónicos y demás comunicaciones) en poder de la contraparte, aludiendo a que los mismos formarían parte de la historia clínica del actor que resulta de su exclusiva propiedad conforme art. 14 de la ley 26.529[14].

En los autos **"Powell Hugo Francisco c/Willis Corredores de Reaseguros S.A. y otro s/diligencia preliminar"** se consideró que procedía como prueba anticipada una pericia informática ante la posibilidad de que en el futuro la misma pueda resultar imposible o dificultosa ya que podría modificarse o destruirse la información contenida en los servidores de correo electrónico. **En consecuencia se ordenó que el perito:** 1. Se constituya en el domicilio de la demandada; 2. Compulse sus sistemas (servidores, terminales o medios de almacenamiento de back up), resguardando la privacidad

de los datos, 3. Realice un "back up" de todos los correos electrónicos que tengan al actor por remitente o destinatario entre las fechas solicitadas; 4. Se reserve la copia en el juzgado para que en la etapa de producción de la prueba se realice, eventualmente y en la medida que sea debidamente ofrecida, la pericia correspondiente, con el adecuado control de la misma por parte de la demandada a fin de resguardar el derecho de defensa en juicio[15].

Por otro lado, en los autos **"Heberle Karina Soledad c/Caktus SA y otros s/diligencia preliminar"** se negó una medida de prueba anticipada sobre sistemas que —aparentemente[16]— se encontraban bajo su propio control y sobre información que estaba en los registros del ente público Nic Argentina (titularidad de nombres de dominio) ya que no corrían un peligro inminente y podían ser acreditados en una etapa ulterior[17].

Asimismo, en un precedente de la Sala A se negó la posibilidad de producir la prueba in audita parte. Así se resolvió en los autos **"Luxury Waters Ltda. c/New Patagonia SA s/diligencia preliminar"**, donde se concedió una pericia y registro de los registros informáticos de la demandada como prueba anticipada en base al riesgo existente, por la naturaleza misma de los elementos documentales a ser examinados, de que su contenido sea adulterado y/o suprimido antes de arribarse a la etapa probatoria pero se rechazó su producción in audita parte, considerando que la petición no halló su causa en razones de urgencia sino en el riesgo existente[18]. Aparentemente se habría admitido la obtención de la prueba in audita parte pero no su producción y análisis por parte del perito, tal como se resolvió, con buen criterio, en los citados autos "Powell...".

VIII. Necesidad de acompañar una copia de los correos

En los autos **"G., D.E.c/C. SA. s/diligencia preliminar"** se equiparó los correos electrónicos a los libros de comercio y se sostuvo que no era posible ordenar una constatación judicial para probar su existencia en contra de un comerciante, sino tan sólo intimar a la parte contraria a exhibirlos en los términos del art 56 del código de comercio bajo apercibimiento de interpretar la negativa en su contra[19].

Ello porque la actora había omitido toda mención al texto de esos correos y no había siquiera acompañado copia, siendo que, por los usos y costumbres comerciales (art. 5 del Título Preliminar del Código de Comercio), la existencia de esas copias puede presumirse tanto en los propios equipos de computación de la accionante como en los de su Proveedor de Servicios de Internet (ISP), a quien tampoco individualizó.

Por ello, consideró el juez que la medida requerida aparecía violatoria del principio de igualdad procesal que el Juez debe preservar (art. 34, inc. 5° c. del Código Procesal).

IX. Necesidad de probar la recepción

La prueba del envío de un correo electrónico -aún firmado digitalmente por el emisor-, nada dice sobre su recepción por el destinatario ya el protocolo SMTP que utiliza el correo electrónico no implementa sistemas de acuse de recibo confiables.

Es decir que aún en el caso de correos electrónicos cuyo envío haya sido probado, podría ser necesario producir prueba adicional para acreditar su recepción por el destinatario.

En los autos **"Heynald SA c/Pallanch, Alberto Enrique y otros s/ejecutivo s/incidente de ejecución de honorarios"**, se consideró que no resulta fehaciente como notificación un correo electrónico enviado si no se acredita su recepción por el destinatario[20].

Es interesante la interpretación contrario sensu del fallo citado que permitiría considerar como notificación fehaciente los correos electrónicos cuya recepción por el destinatario hubiere sido acreditada.

X. La prueba

La prueba en juicio de los documentos digitales, entre ellos los correos electrónicos sólo será necesaria, como se dijo, cuando sean desconocidos por la contraria.

Para probar la autoría, integridad y recepción de documentos desconocidos por la contraria pueden ofrecerse todos los medios de prueba que admite el código procesal y será el juez quién evaluará su eficacia conforme las reglas de la sana crítica.

XI. Inferencias y sana crítica

Ante la dificultad de probar la autoría e integridad de los correos electrónicos por carecer de medidas de seguridad razonables y ante la inexperiencia de los letrados para ofrecer pruebas eficaces, los tribunales se han valido, en algunas ocasiones, de inferencias para atribuir valor probatorio a dichos correos.

Si resulta aprobado el Proyecto de Código Civil y Comercial de la Nación en su redacción actual, la prueba podrá facilitarse alegando: 1. La utilización de un método que asegure razonablemente la autoría e inalterabilidad del documento (Art. 288 del proyecto); y, 2. Los indicios surgidos de la congruencia entre lo sucedido y narrado, la precisión y claridad técnica del texto, los usos y prácticas del tráfico, las relaciones precedentes y la confiabilidad de los soportes utilizados y de los procedimientos técnicos que se apliquen (Art. 319 del proyecto).

En esta línea, en los autos **"Ferry Cecilia Alejandra c/Macren International Travel S.A. s/despido"**, se otorgó eficacia probatoria a una serie de correos electrónicos atribuidos a la demandada a partir de un informe del proveedor que confirmaba —tan sólo— la existencia de la casilla de correo a ella atribuida.

Ello a pesar de que no se pudo verificar que los correos que se habían impreso hayan existido realmente o que su contenido sea el mismo que el invocado por el actor; sólo se había podido acreditar que el demandado tenía una cuenta con el nombre alegado[21].

No resulta aconsejable extrapolar este razonamiento para elaborar una regla general ya que la existencia de una cuenta con el nombre del demandado no brinda certeza alguna sobre el contenido o existencia de los mensajes. La sentencia debe interpretarse como una solución puntual dada en un caso concreto, apoyada por otros medios probatorios y en el marco de un proceso donde en caso de duda se falla en favor del trabajador. Además es probable —aunque no surge claramente de la sentencia—, que el juez haya valorado como mala fe procesal que la parte haya desconocido ser la titular de la casilla, en cuyo caso hubiese sido aconsejable que lo valore expresamente para sentar un precedente más claro.

En sentido contrario, en los autos **"B., T.E. c/Q., C.N. s/Divorcio"** se resolvió que no correspondía otorgar valor probatorio a correos electrónicos impresos que podían haber sido modificado antes de su impresión, no bastando el reconocimiento de un testigo de que la dirección de correo pertenecía a la parte que se le imputaban[22].

XII. Teoría de los propios actos

En materia administrativa, la Cámara Federal de Apelaciones de La Plata Resolvió que no puede ser desconocida la notificación realizada por un medio no previsto en la reglamentación vigente —correo electrónico— en tanto su validez resulte de la conducta asumida por la contraparte que la utilizó en algunas oportunidades para efectuar notificaciones, debiendo primar el principio de buena fe y la doctrina de los actos propios. (cnfr. Cámara Federal de Apelaciones de La Plata, sala I, 20/08/2009, in re: **"M., C. A. c/ U.N.L.P."**, La Ley Online: AR/JUR/31994/2009)

Este fallo se alinea con el criterio adoptado por el art. 319 del Proyecto de Código Civil y Comercial de la Nación que ordena interpretar el valor probatorio de los instrumentos particulares, sea cual fuere su soporte, conforme a las *"...relaciones precedentes..."* y los *"...usos y prácticas del tráfico..."*.

XIII. Informativa

Procede la prueba informativa cuando la gestión de los correos electrónicos o información vinculada a su envío o recepción se encuentra en poder de un tercero imparcial que pueda informar al respecto a partir de datos que obren en sus registros (art. 396 CPCC). Para ello, es necesario que dichos registros no hayan podido ser alterados antes de producirla, lo que justificaría tramitar este medio probatorio como prueba anticipada, tal como se hizo en los autos **"R.P., E.C. c/C.L., S.H. s/divorcio y exclusión de cónyuge."** que serán reseñados en el punto 8.

En los autos **"Hjelt, Ana c/ Alexander, Alberto s. despido"** se otorgó eficacia probatoria a impresiones de correos electrónicos que fueron reconocidos —mediante prueba informativa— por una tercera empresa que participó del intercambio de mensajes[23].

En los autos "López Verde Jorge Hernán c/Automóvil Club Argentino y otro s/ordinario", un caso fallado más en base al sentido común que a la regla procesal, se concedió eficacia probatoria a correos electrónicos que obraban impresos en expedientes internos de la demandada —y que ella misma desconocía— y que fueron obtenidos mediante prueba informativa[24].

Por otro lado, en los autos **"Leone, Jorge Néstor c/Maquieira, Jorge Sabino s/cobro de sumas de dinero"** se negó eficacia probatoria a un conjunto de correos electrónicos impresos, dado que de la prueba informativa surgía que la casilla no pertenecía a la parte a la que se le imputaban sino que aparentemente dicha casilla pertenecía a su esposa[25].

XIV. Testimonial

De la jurisprudencia hallada surge que la prueba testimonial es un fuerte indicio para dar validez a los correos electrónicos. Ello puede apreciarse en los autos **"Bicocca Mariela Paula c/Petrobras Energía S.A. s/despido"**[26], **"Echezarreta Javier Andrés c/Ledesma S.A. s/despido"**[27], **"Martinez Ramón Eliseo c/Fragal S.A. s/Despido"**[28] y **"V.R.I c/Vestiditos SA s/despido"**[29] donde se la valoró positivamente.

En los autos **"G., M. J. c. Honda Automóviles de Argentina S.A. y otro"** la actora había ofrecido correos electrónicos como prueba, pero las declaraciones de los testigos sobre su existencia eran contradictorias.

El tribunal, finalmente, le dio mayor valor al reconocimiento de los correos efectuado por ex trabajadores que al desconocimiento efectuado por trabajadores en actividad, considerando que tratándose de cuestiones relacionadas con sus funciones en la empresa codemandada, y que podrían comprometer su responsabilidad laboral, la imparcialidad del testigo dependiente de la codemandada no se ve garantizada[30].

En los autos **"Del Valle, Ana Belén c. Cardinal Servicios Integrales S.A."**, el tribunal consideró como un indicio en contra de la validez de los correos, que no se haya solicitado su reconocimiento a la persona a la que estaban dirigidos y que había sido citada como testigo[31].

XV. Pericial sobre sistema propio

Es común que las partes ofrezcan como prueba datos obrantes en su propia computadora, en sus servidores o en cualquier otro sistema sobre el cual esa misma parte tenga cierto control para agregar, modificar y borrar información.

Cuando las pericias se realizan sobre un sistema bajo control de la parte que alega la prueba, su efectividad debe ser juzgada de acuerdo a los mecanismos de seguridad que utilice dicho sistema, para garantizar la autoría e inalterabilidad de los documentos que se atribuyen a la contraria, regla evidente desde el punto de vista lógico, que tendrá sustento legal en el citado art. 288 del Proyecto de Código Civil y Comercial de la Nación, si resulta promulgado.

En este sentido, en los autos **"Saporiti, Pablo Alberto c/Peugeot Citroën Argentina S.A. y otro s/Despido"**, se rechazó el valor probatorio de correos existentes en la cuenta de una de las partes debido a que la otra —que había ofrecido la prueba— era la que controlaba el servidor peritado y había tenido la capacidad técnica de modificar —antes de la pericia— el contenido de los documentos que allí se almacenaban[32].

En los autos **"Soft Bar S.R.L. c/ Banco de la Provincia de Buenos Aires"**, se negó eficacia probatoria a una pericia realizada sobre la computadora de la parte que ofrecía la prueba debido a que la opinión del perito sobre la posible atribución de los correos a la otra parte se basaba en apreciaciones subjetivas y carecía de fundamentos técnicos[33].

XVI. Pericias sobre sistema de la contraparte

Cuando la pericia se realiza sobre un sistema bajo control de la parte que niega la prueba y tiene resultado positivo, es sencillo defender su validez ya que es equivalente a encontrar la prueba del delito en la casa del acusado. Para este tipo de pruebas es necesario obtener algún tipo de medida cautelar ya que al estar el sistema bajo control de la otra parte, podrían ser destruidas antes de producirse, tal como se explicó en el punto 8.

Esta situación se observa principalmente en causas penales donde cautelarmente se secuestran computadoras y soportes de almacenamiento de los imputados y se realizan pericias sobre los mismos antes de que hayan podido ser manipulados, como en los reseñados autos **"Seri, Miguel Angel; Gasparini, Diego Nazareno y otros"**.

En civil, comercial y laboral es más difícil —aunque posible— obtener este tipo de medidas.

En los autos **"Mammes, Axel c/ Gilbarco Latín América S.A"**, se otorgó eficacia probatoria a correos electrónicos y otros documentos hallados mediante pericias en las computadoras de la empleadora[34].

En los autos "Uhrin, Jorge A. c/ Bayer Argentina S.A.", la demandada pudo probar en contra del trabajador, mediante prueba pericial técnica, que un correo se encontraba en la casilla de correo electrónico personal del actor, con lo cual

se tuvo por probado por aquel el envío de correos electrónicos que lo comprometían, infiriendo que el susodicho era el único que podía acceder al mismo para su consulta o difusión mediante el ingreso de una "clave personal" que el sistema informático solicitaba, antes de ingresar a la página "Web" en la cual tenía su cuenta (Cnfr. Cámara Nacional de Apelaciones del Trabajo, Sala I, 10/04/2003, La Ley Online: AR/JUR/977/2003).

Por otra parte, en los autos **"Leone, Jorge Néstor c/Maquieira, Jorge Sabino s/cobro de sumas de dinero"** el actor no consiguió probar de forma suficiente a través de prueba informativa la autenticidad de correos electrónicos impresos y el tribunal interpretó en contra de la parte que los alegaba que *"...el actor tenía a su alcance otros medios para acreditar fehacientemente la autenticidad de los mencionados correos, como ser el secuestro del disco rígido con carácter cautelar o el ofrecimiento de perito especializado en la materia..."* (CNCiv. Sala I, 11/08/2005)

XVII. Control de la casilla

En los casos en que se consigue probar que los correos electrónicos fueron enviados o recibidos de determinada cuenta de correo (por ejemplo usuario@gmail.com), es necesario también acreditar, si la contraparte niega la titularidad de la cuenta, que aquella es la titular.

En los autos **"Mullins, María c/Stratford Book Services S.A. s/despido"** se negó eficacia probatoria a correos electrónicos cuando de las probanzas surgía que la casilla figuraba a nombre de una persona distinta de aquella a quién se le imputaban[35].

En los autos **"Leone, Jorge Néstor c/Maquieira, Jorge Sabino s/cobro de sumas de dinero"** ya reseñados en el punto "14", se negó eficacia probatoria a un conjunto de correos electrónicos, en los cuales la titularidad de la cuenta no era de la parte a la que se le imputaban, sino aparentemente de su esposa.

Además de la titularidad, el control que la parte detente de la cuenta es el elemento que permite imputarle la autoría de los correos que provengan de aquella.

Así se decidió en los autos **"López, Marcela Edith c/ C.C.R. S.A. Concord Consumer Comunication Research Development S.A."** donde se señaló que no podía imputársele la autoría de determinados correos electrónicos a una de las partes si las computadoras y el software de donde fueron enviados eran utilizados indistintamente por todos los empleados de la empresa[36].

XVIII. Conclusiones

La eficacia probatoria de los correos electrónicos —y de los documentos en general— dependerá de que sea posible probar su autoría, integridad y recepción a través de los mecanismos de seguridad propios de la tecnología que empleen.

En los casos en que dicha prueba no sea concluyente, será posible brindarles eficacia probatoria a través de otros medios (testimonial, informativa, pericial) o de indicios (costumbre, actos anteriores de la partes, hechos concordantes, mecanismos de seguridad no concluyentes), evaluados siempre a través de la sana crítica.

Ahora bien, en el Código Civil vigente, los códigos procesales y la LDFD, establecen reglas para tecnologías específicas; el Código Civil para los documentos escritos y la LDFD para los documentos con un específico sistema de firma electrónica regulado minuciosamente por el estado (firma digital). Sin embargo, no existe legislación vigente que aporte reglas claras sobre el valor probatorio de documentos electrónicos sin firma digital, La LDFD dice que corresponde a quién alega una firma electrónica probar su validez, pero no dice cómo.

Ante la ausencia de reglas tecnológicamente neutras, los jueces se han visto obligados a un esfuerzo interpretativo para adaptar por analogía las normas vigentes, cuando las partes utilizan técnicas de seguridad distintas de las legisladas[37].

Por el contrario, el Proyecto de Código Civil y Comercial de la Nación:

1. Establece la libertad de formas para la contratación.

2. Elabora reglas de prueba sencillas y tecnológicamente neutras:

a. Para los documentos electrónicos, se debe probar que se utilizó un método que razonablemente permita acreditar su autoría e integridad (art. 288).

b. Para los instrumentos particulares —entre ellos la correspondencia electrónica— autoriza expresamente la ponderación de indicios y procedimientos de seguridad sin limitarse a técnicas específicas (art. 319).

Si el Proyecto de Código Civil y Comercial resulta aprobado, la simplicidad y flexibilidad de las reglas citadas deberían permitir la proliferación de sistemas de comunicación relativamente seguros que utilicen firma electrónica.

Ello por cuanto los actos celebrados de forma electrónica entre privados tendrán mayor previsibilidad en el proceso de prueba, seguridad jurídica y eficacia probatoria, sin necesidad de utilizar firma digital, la cual ni se encuentra comercialmente disponible, ni es indispensable, en la mayor parte de las comunicaciones entre privados.

Este artículo se encuentra publicado en **Sup. Doctrina Judicial Procesal 2013 (marzo), 01/03/2013, 13 - DJ27/11/2013, 91.**
Cita Online: AR/DOC/5408/2012

(*) Sobre la base del Proyecto de Código Civil y Comercial de la Nación presentado por el Poder Ejecutivo Nacional.

(1) http://tools.ietf.org/html/rfc5321.

(2) "Artículo 319. Valor probatorio. El valor probatorio de los instrumentos particulares debe ser apreciado por el juez ponderando, entre otras pautas, la congruencia entre lo sucedido y narrado, la precisión y claridad técnica del texto, los usos y prácticas del tráfico, las relaciones precedentes y la confiabilidad de los soportes utilizados y de los procedimientos técnicos que se apliquen." (Art. 319, Proyecto de Código Civil y Comercial de la Nación enviado al senado por el Poder Ejecutivo bajo el Mensaje 884/12).

(3) "Una firma electrónica sería simplemente cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita. En este concepto amplio y tecnológicamente indefinido de firma...tendrían cabida técnicas tan simples como un nombre u otro elemento identificativo (por ej. la firma manual digitalizada) incluido al final de un mensaje electrónico, y de tan escasa seguridad que plantean la cuestión de valor probatorio a efectos de autenticación, aparte de su nula aportación respecto a la integridad del mensaje..." ("Apolonia Martínez Nadal, "Comercio Electrónico. Firma Digital y Autoridades de Certificación", Colección Estudios de Derecho Mercantil, Segunda Edición, Civitas, Madrid, 2000, pág.40, cit. por José Fernando Márquez y Luis Moisset de Espanés, "La formación del consentimiento en la contratación electrónica", http://www.acaderc.org.ar/doctrina/articulos/artcontratacionelectronica/at_download/file, quienes señalan que "Concluye la autora en que debe dudarse de la condición de firma de estas técnicas, atento a su nula o escasa utilidad").

(4) La ley de Firma Digital (en adelante LDFD) define la firma digital como el "...resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante encontrándose esta bajo su absoluto control..."que "...debe ser susceptible de verificación por terceras partes tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma..." (Art. 2 LDF). La ley delega en la autoridad de aplicación la reglamentación de los procedimientos tecnológicos aplicables pero indirectamente por la forma en que está definida, sugiere la implementación de mecanismos de criptografía asimétrica que son el estándar en la industria.

(5) Cnfr. CNCiv. Sala I, in re: "Leone, Jorge Néstor c/Maquieira, Jorge Sabino s/cobro de sumas de dinero", 11/08/2005; ídem CNCom. Sala D, 2/03/10, "Bunker Diseños SA c/IBM Argentina SA s/ordinario).

(6) "En cuanto a los correos electrónicos que alegó haber intercambiado la actora con su contraparte, cabe decir que por ser la firma condición esencial de todo acto bajo forma privada (CCiv: 1012) no cabe asignar, como regla, valor probatorio a un correo electrónico que no cumple con los requisitos exigidos por la Ley 25506: 2 y 5 sobre firma digital, considerados como recaudo esencial en la formación del denominado documento electrónico" (CNCom Sala A, "Cooperativa de Vivienda, Crédito y Consumo Fiduciaria Ltda. c/Becerra Leguizamón, Hugo", 27.6.06)."No cabe asignar, como regla, valor probatorio a un correo electrónico que no cumple con los requisitos de la ley 25506: 2 y 5 sobre "firma digital" (conf. CNCom. sala A, 27.6.06, "Coop. de Viv. Créd. y Cons. Fiduciaria Ltda. c/Becerra Leguizamón, h.", ll 24.10.06, fallo n° 110.898), ya que el elemento de autenticación o certificación es un requisito esencial en la formación del denominado documento electrónico..." (cfr. Nieto Melgarejo, p., "derecho del comercio electrónico", lima, 2005, págs. 126/127, citado por CNCom, sala D, "Baires Inter Trade SA c/Otro Mundo Brewing Company SA s/medida precautoria",4/10/07)."...como regla, asignar valor probatorio a un correo electrónico que no cumple con los requisitos de los arts. 2 y 5 de la ley 25.506 sobre 'firma digital' (conf. CNCom. Sala A, 27/6/06, 'Coop. de Viv. Créd. y Cons. Fiduciaria Ltda. c. Becerra Leguizamón, H.', LL 24/10/06, fallo n° 110.898), ya que el elemento de autenticación o certificación es un requisito esencial en la formación del denominado documento electrónico (conf. Nieto Melgarejo, P., Derecho del Comercio Electrónico, Lima, 2005, págs. 126/127)..." (CNCom. Sala D, autos: "Henry Hirschen y Cía. S.A. c. Easy Argentina S.R.L.", 16/02/2007, La ley online: AR/JUR/904/2007).

(7) "...No puede otorgarse un valor de convicción preeminente a los documentos que carecen de firma digital, por no cumplir con los requisitos de la Ley 25506: 2 y 5, sobre "firma digital" puesto que el elemento de autenticación o certificación es un requisito esencial de autenticidad; sin embargo, no existe impedimento para que se los ofrezca como medio de prueba (CPR: 378-2°), considerándoselos principio de prueba por escrito como había aceptado la doctrina de los autores antes de la sanción de la citada Ley 25506; tal valor probatorio se sustenta en las normas del CCIV: 1190, 1191, 1192, pues aunque por no estar firmados no alcancen la categoría de documento privado es admisible su presentación en juicio para probar un contrato siempre que emanen del adversario, hagan verosímil el hecho litigioso y que las restantes pruebas examinadas a la luz de la sana crítica corroboren su autenticidad...1. La accionada nunca negó el carácter de empleado de la accionante, de la persona con quien estuviera en tratativa para la fabricación de los materiales en cuestión, la que, además, envió los e-mails desde una casilla institucional; y, considerando como un hecho público y notorio (cfr. Couture E. "Fundamentos del Derecho Procesal Civil", nro. 150, p. 233, ed. 1993), en este sentido, que una dirección de correo electrónico es individual y que no pueden registrarse dos iguales; puede presumirse sin ninguna duda razonable que la sigla institucional pertenece a la accionada (cfr. Leguisamón, H. "Las presunciones judiciales y los indicios", cap.IX, nro. A.2, p. 92, ed. 1991). 2. Tampoco desconoció los mensajes de correo electrónico agregados por la accionante y cursados a la dirección institucional y en algunos casos respondidos, así como el dirigido a otra dirección institucional ante un pedido de cotización, los cuales revelan que eran usuales las tratativas precontractuales y post contractuales entre las partes por ese medio." (CNCom. Sala D, 2/03/10, "Bunker Diseños SA c/IBM Argentina SA s/ordinario").

(8) "No obstante la extorsión alegada, cabe entender que la prueba se obtuvo de modo legítimo si la trabajadora no redarguyó de falsedad el acta notarial de la que surge que proporcionó libremente su clave personal de acceso a la casilla de e-mail de la empresa y su conformidad para la apertura del correo al escribano público" (CNTrab. Sala X, "García, Delia c/YPF SA s/despido.", 13/08/03).

(9) Cámara Comercial Civil y Comercial de Morón, autos: "Balocco, Enrique E. y ot. c. Chiesa, Ariel y otros", 04/09/2007, La Ley Online: AR/JUR/6626/2007.

(10) En igual tesitura se sostuvo que "...cuando la firma electrónica resulta irreductiblemente reconocida (6), satisface el requerimiento de autógrafo que cada vez disponga el sistema normativo, esto es, que sendas firmas —en punto a sus efectos jurídicos— quedan equiparadas.El paralelismo de

las firmas informáticas con las ológrafas, en el sentido de que -en sus casos- las primeras equivalen —jurídicamente— a las segundas, en el sistema argentino está instaurado, tanto respecto de la firma digital, como de la firma electrónica por supuesto que excluyéndose, en el caso de las últimas, íntegramente, a todas las que, ante el mundo jurídico argentino, no excedan la categoría de dubitadas." (González Gómez, Pedro M., "Equiparación a la ológrafa de la firma informática argentina", La Ley, Sup. Act. 12/04/2007).

(11) "La prueba anticipada puede comportarse como una verdadera medida cautelar o precautoria, ya que sin perder su naturaleza probatoria, la adquisición de ciertas pruebas debe realizarse in audita parte. Ello, por cuanto su anticipación en el conocimiento de la otra parte, puede permitir que a través de maniobras de diverso tipo, oculte, modifique, destruya, altere o cambie el objeto probatorio en cuestión. 2-Las medidas de instrucción previa tienden a recoger pruebas útiles para un proceso futuro o en trámite. Su finalidad, aunque de naturaleza cautelar, no es asegurar el cumplimiento futuro de la sentencia, sino posibilitar la solución conservando pruebas. 3-La inviolabilidad de la correspondencia es un elemento que hace a la configuración del derecho a la intimidad, sin embargo no es absoluta sino relativa. Es que, si bien el correo electrónico puede resultar asimilable a la correspondencia epistolar y darle la protección constitucional prevista en el art. 18 de la Constitución Nacional, lo cierto es que la limitación de los derechos fundamentales no son competencia exclusiva de algunos magistrados y la falta de legislación en el tema, no significa su prohibición como tampoco su total facultad para intervenir. Por ello, los jueces penales no son los únicos que pueden restringir derechos fundamentales de la inviolabilidad de la propiedad, de la correspondencia, también pueden ser competentes los jueces civiles. 4-La prueba acerca de la existencia de e-mails así como de archivos informáticos puede desaparecer o tornarse impracticable con el transcurso del tiempo, ya que con solo apretar una tecla del equipo de computación, podrían desaparecer los registros, sin olvidar la posibilidad de que fuesen afectados por un virus que volviera su lectura imposible. 5-En consecuencia, si se encuentra acreditado prima facie que la parte que solicita la medida-en el caso, pedido de libramiento de oficio a Google a los efectos de que realice una copia y la remita al juzgado con todos los correos electrónicos intercambiados entre la dirección de e-mail de una de las partes y la dirección de correo electrónico de un tercero-está expuesta a perder la prueba o que le resultará de imposible o muy dificultosa ejecución en la etapa pertinente, corresponde hacer lugar al pedido. (Sumario N°21502 de la Base de Datos de la Secretaría de Jurisprudencia de la Cámara Civil)." (CNCiv. Sala J, 22/11/11, "R.P., E.C. c/C.L., S.H. s/divorcio y exclusión de cónyuge")

(12) "Las medidas previstas por los arts. 326 y 327 del Código Procesal, denominadas de "instrucción previa", tienden a recoger pruebas útiles para un proceso futuro o en trámite. Su finalidad, aunque de naturaleza cautelar, no es asegurar el cumplimiento futuro de la sentencia, sino posibilitar la solución conservando pruebas. De tal manera, no se advierte que con la pericia que realice un licenciado en sistemas informáticos a fin de constatar en el disco rígido de una computadora la fecha e intercambio de correo electrónico efectuado entre las partes, indicando las direcciones a donde fueron dirigidos o donde recibidos y mediante la extracción de copias se pueda adelantar el pronunciamiento que, en definitiva, recaerá sobre el objeto de las actuaciones. 2- En cuanto al derecho de defensa previsto en el último párrafo del art. 327 del Código Procesal, este tipo de medidas deben ser dispuestas "inaudita pars" y ello sin que se violente el principio de bilateralidad, produciéndose un aplazamiento del mismo al momento de producción de la prueba. Esto torna necesaria la intervención del Defensor Oficial a los efectos de representar a la parte contra la que se lleva la medida, la cual no puede ser notificada ya que su anticipación en el conocimiento de la medida puede permitir que se oculte, modifique o destruya el objeto probatorio a adquirir. Fundamentos de la Dra. Brilla de Serrat: Es innecesaria la intervención del Defensor Oficial cuando la medida anticipada habrá de cumplirse en el propio ámbito de la accionada, toda vez que le posibilita así su contralor." (CNCiv. Sala J, "Pardo, Rubén Ricardo c/Fernández, Juan Carlos s/ medidas precautorias", 15/08/06, Sumario N°17080 de la Base de Datos de la Secretaría de Jurisprudencia de la Cámara Civil - Boletín N°1/2007).

(13) "Resulta procedente que la orden judicial de libramiento del mandamiento necesario para la producción de la prueba anticipada destinada a constatar la existencia de ciertos correos electrónicos y archivos adjuntos en las computadoras de la accionada, relacionada a correspondencia dirigida a la accionante autorice a allanar domicilio, requerir el uso de la fuerza pública y solicitar los servicios de cerrajero, toda vez que de no autorizarse tales facultades la producción de la prueba solicitada podría frustrarse; facultades éstas que están fundadas en la fuerza coactiva de las decisiones judiciales y en la necesidad de que ellas puedan ejecutarse..."."Resulta procedente la habilitación de la feria judicial a los efectos de que pueda producirse la prueba anticipada solicitada, tendiente a constatar la existencia de ciertos correos electrónicos y archivos adjuntos en las computadoras de la accionada, relativa a la correspondencia dirigida a la peticionaria, dada la urgencia derivada de la propia naturaleza y vulnerabilidad de los registros informáticos." (CNCom. Sala de feria, 28/01/09, "DVA Agro GMBH c/Ciagro SRL s/diligencia preliminar").

(14) CNTrab. Sala VII, "Ramirez Gustavo Alejandro y otro c. MC Care Company SRL s/diligencia preliminar", expte. 52.193/2011, 23/4/2012, www.cij.gov.ar

(15) CNTrab. Sala X, "Powell Hugo Francisco c/Willis Corredores de Reaseguros S.A. y otro s/diligencia preliminar", 28/06/2012, publ. en elDial.com - AA78C6, facilitado al autor por el Dr. y Carlos Oscar Lerner para un trabajo realizado en el Instituto de Derecho Informático del CPACF).

(16) Aparentemente el sistema estaba bajo control de la parte, que solicita la certificación ya que de otra forma no se podría haber provisto al secretario acceso al sistema para certificarlo.

(17) "A criterio del Tribunal no le asiste razón a la recurrente, pues la parte actora peticiona para que el Actuario (Secretario del Juzgado) certifique la existencia del dominio de internet que indica, y asimismo, el correo electrónico vinculado al mismo, y también los mails y comunicaciones intercambiadas desde y hacia ese correo electrónico.Se advierte que la Sra. Juez al decidir rechazar la petición de la parte actora, tuvo en cuenta lo dictaminado por la Sra. Agente Fiscal, a fs. 11, respecto de que el anticipo preventivo de prueba importa la admisión excepcional de una medida en una etapa que no es propia, con fundamento en la eventualidad de la desaparición de la prueba. Además, es correcto lo decidido por la Sentenciante, al concluir que no se demostraron en autos los requisitos de verosimilitud del derecho y peligro en la demora, que deben caracterizar estas medidas.Cabe señalar que el dictado de una diligencia preliminar a realizarse en forma de medida precautoria es de carácter extraordinario, por lo que debe reunir los requisitos de toda medida cautelar, a saber: la verosimilitud del derecho y el peligro en la demora. Además, debe ser analizado de manera restrictiva, a fin de no vulnerar el derecho de defensa de las partes." (CNTrab. Sala VII, causa N. 23.539/2011. "Heberle Karina Soledad c/Caktus SA y otros s/diligencia preliminar", 30/9/11).

(18) "Cuando, como en el caso, fue requerida y concedida la producción de una medida de prueba anticipada, consistente en una pericia informática con el objeto que el experto que resulte designado, examine los registros informáticos de la demandada (cuentas de correo electrónico, computadoras, discos rígidos, etc.) y se expida sobre determinados puntos, con base en que la naturaleza del material a ser analizado, podría ser fácilmente adulterado, por lo que la medida requerida estaría expuesta a perderse; en ese marco, resulta improcedente la petición de la accionante que la medida se concretara sin la intervención de la contraparte. Ello así, en tanto tal petición no halló su causa en razones de urgencia —Cpr: 327— sino en el riesgo existente, por la naturaleza misma de los elementos documentales a ser examinados, que su contenido sea adulterado y/o suprimido antes de arribarse a la etapa probatoria. Frente a ello, la citación de la futura parte contraria a fin de conferirle participación en la prueba se evidencia ineludible. No debe perderse de vista que la télesis del instituto es procurar medidas para el proceso que de otro modo podrían perderse, mas no otorgar a una de las partes ventajas sobre la otra al permitirle realizar una medida probatoria inaudita parte." (CNCom. Sala A, 8/10/2010, "Luxury Waters LTDA c/ New Patagonia SA s/diligencia preliminar").

(19) Como fundamento de la negativa, se equiparó el correo electrónico a la correspondencia epistolar y se consideró que "...la exhibición de la correspondencia entre comerciantes con motivo de una negociación debe asimilarse a la parcial de los libros de comercio, que es admitida por la legislación mercantil en caso de pleito pendiente, o como medida preliminar, pues reposa en el principio de la comunidad de los asientos (art. 59, Código de Comercio; cfr. Fernández - Gómez Leo, ob. cit., t. II, p. 127 y sgtes.)..." que "...ello no autoriza a efectuar esa exhibición en forma compulsiva, ya que la negativa trae aparejada la sanción prevista por el art. 56, es decir, el litigio será resuelto en función de los libros de su adversario (cfr. Fernández - Gó-

mez Leo, ob. cit., t. II, p. 137).." y que "... el art. 388 del código procesal no autoriza al Juez al secuestro o exhibición compulsiva de esos documentos sino tan sólo a considerar la negativa a presentarlos, como una presunción en contra del renuente, en concordancia también con la mencionada normativa del Código de Comercio" (cnfr. Juzgado Comercial Nro. 18, Secretaría 36, autos "G., D.E.c/C. SA. s/diligencia preliminar", 23/10/2001, http://tinyurl.com/fallogdcsa, facilitado al autor por la Dra. Tatiana Anabel Fij para un trabajo realizado en el Instituto de Derecho Informático del CPACF).

(20) Se consideró que a los efectos de la renuncia de la representación de un apoderado (Cpr: 53), la documentación consistente en cierto correo electrónico que habría sido enviado, en principio por la ejecutante, no resulta fehaciente a los fines perseguidos. Ello pues"...aquella documentación de la cual se desprendería la recepción del telegrama internacional de renuncia, no implica la efectiva recepción de su destinataria..." (CNCom. Sala F, 27/08/10, "Heynald SA c/Pallanch, Alberto Enrique y otros s/ejecutivo s/incidente de ejecución de honorarios").

(21) "...destaco un elemento que no resulta de la sentencia de grado y que, al fin de cuentas, y a su modo, constituye un indicio más que respalda el reclamo de pagos "en negro": destaco en este sentido que entre fs. 29 y 37 la actora ha acompañado una serie de impresiones de mails o mensajes de correo electrónico cruzados entre la cuenta ceciliaferry@macrentravel.com.ar y un dominio identificado como "Hugo Renzini - MacrenInt. Travel SA", de donde se desprende que todos los meses existía un diálogo por el cual, desde la primera cuenta se requería a la segunda el pago de haberes que restarían percibir. Tales elementos, desconocidos en forma expresa en oportunidad del responde (v. fs. 81), aparecen respaldados con el informe de la firma Mesi SRL (v. fs. 147), empresa que se reconoce como proveedora de los servicios de alojamiento web y de correo electrónico corporativo que utiliza la demandada, y que si bien indica que no retiene información acerca del contenido de los mensajes ni da fe de la existencia de la casilla que se imputa como de pertenencia de la actora, sí reconoce que había una casilla activa identificada como hugorenzini@macrenttravel.com.ar, y la falta de cuestionamientos acerca de lo indicado en esa respuesta por parte de la accionada me inclina a darle eficacia como un indicio a favor de la tesis del escrito inicial (arts. 163 inc. 5 y 386 del CPCCN)." (CNTrab. Sala IV, 31/8/2011, "Ferry Cecilia Alejandra c/Macren International Travel S.A. s/despido").

(22) "...3- Si bien se encuentra negado el derecho a controlar la correspondencia dirigida al otro esposo, todo depende de cómo se ha obtenido el acceso y las motivaciones que llevaron a efectuarlo. Ahora bien, sin perjuicio de la forma de obtención de la comunicación a través de internet, corresponde descartar los e-mails obtenidos como prueba, si de la pericia surge que pueden haber sido modificados antes de su impresión. Es que, no basta solamente el reconocimiento de la dirección de correo electrónico por parte de un testigo para acreditar que fue esa la correspondencia habida entre las partes." (CNCiv. Sala J, "B., T.E. c/Q., C.N. s/divorcio.", 6/10/11, Sumario N°21424 de la Base de Datos de la Secretaría de Jurisprudencia de la Cámara Civil).

(23) "El demandado desconoce los documentos de fs. 57/60 (v. fs. 113), que no son más que impresiones de un intercambio de mensajes vía mail anterior a la compra de los pasajes correspondientes al viaje que de la actora. Pues bien, en esa prueba figura la respuesta de la empresa Despegar.com al pedido de reserva solicitado por Ana Hjelt. El intercambio de mails fue reconocido por esa firma según el informe de fs. 188 (aunque allí se aclara que el intercambio fue más extenso) y lo que llama la atención es que la actora se comunicó por el dominio web dreamontheatre.com.ar de propiedad del demandado según el informe de fs. 156 (Ministerio de Relaciones Exteriores, Comercio Internacional y Culto), mientras que la firma Virtucom Networks SA (v. fs. 191), informa que entre las casillas de correo electrónico que funcionaron bajo ese dominio, se encuentra la de anna@dreamontheatre.com.ar, utilizada por Hjelt para la compra de ese pasaje, lo que demuestra que esta última se valía de los instrumentos de propiedad de Alexander, con los que este organizaba la empresa." (CNTrab. Sala III, in re: "Hjelt, Ana c. Alexander, Alberto s. despido", 26/09/2009, La Ley Online AR/JUR/26588/2009)

(24) "...dicho correo electrónico integraba la prueba informativa remitida por el "ACA", probanza que no fue impugnada de falsedad por ninguna de las partes conforme lo normado por el CPCC: 403, razón por la cual ha de considerársela auténtica....Tales actuaciones implican el reconocimiento de los extremos afirmados por el accionante. En esa línea, nótese que obra en dichas actuaciones copia del intercambio de correos electrónicos habidos entre las codemandadas..." (CNCom. Sala A, 28/6/2011, "López Verde Jorge Hernan c/Automóvil Club Argentino Y otro s/ordinario").

(25) "...Cabe destacar la fragilidad de la prueba aportada, pues si bien es cierto que a fs. 7/13 se acompañan las copias de los e-mails que se dicen intercambiados por las partes, no existe prueba sobre la autenticidad de los correos electrónicos atribuidos a Maquieira, enviados a través de la casilla que se le adjudica. En primer lugar, porque "Ciudad Internet" en su calidad de proveedora del servicio de internet atribuida a Maquieira informa que la casilla mencionada pertenece a una persona distinta —la Sra. Ana Kairuz de Maquieira—, aparentemente su esposa..." (Cnfr. CNCiv. Sala I, in re: "Leone, Jorge Néstor c/Maquieira, Jorge Sabino s/cobro de sumas de dinero", 11/08/2005)

(26) "La versión del testigo Gracia Salgueiro luce corroborada por el reconocimiento volcado por la testigo Zaietta (fs. 217) del correo electrónico obrante en copia en el sobre de prueba de la actora..." (CNTrab. Sala I, "Autos: "Bicocca Mariela Paula c/Petrobras Energía S.A. s/despido", 17/6/2011).

(27) "El recurrente cuestiona que la comunicación rescisoria no cumple con los recaudos del art. 243 LCT, mas a mi juicio, los hechos imputados en dicha misiva eran de pleno conocimiento por el reclamante. Ello, en razón de que antes de formalizarse el despido, el actor había tenido oportunidad de expedirse cuando contestó el correo electrónico por el cual se le pedían explicaciones, y cuando contestó las preguntas en oportunidad de efectuarse la auditoría (fs. 26/35). Si bien, estos dos sucesos se desprenden del informe de auditoría, el cual fue desconocido por el accionante (111 I/112 I), lo cierto es que la prueba testimonial ha dado cuenta de que dicha documentación es eficaz como medio probatorio" (CNTrab. Sala III, 28/2/2012, Causa Nº 37.055/09 "Echezarreta Javier Andrés c/Ledesma S.A. s/despido").

(28) "El actor agregó en autos la fotocopia de un correo electrónico mediante el cual con fecha posterior a los hechos que se ventilan en autos, se habrían dado instrucciones precisas respecto del manejo del fondo de caja (ver fs. 73). La demandada se limitó a desconocer dicha documental, pero lo cierto es que tanto de los dichos de Gómez (fs. 136) como del testigo López (fs. 141/145) que declaró a propuesta de la accionada, se desprende que en el establecimiento de esta última existía la modalidad de dar instrucciones vía correo electrónico, habiéndose demostrado incluso que esos correos se guardaban en una carpeta. Sin embargo, la demandada no aportó documentación alguna relevante ni ninguna otra prueba para sostener su desconocimiento de la documental en cuestión, actitud que en el presente caso considero insuficiente en el marco de un proceso en el que existe la obligación del Juez de sostener el principio de primacía de la realidad, principio que debe operar también en la aplicación de las normas rituales" (CNTrab. Sala III, 31-10-2011, "Martínez Ramón Eliseo c/Fragal S.A. s/Despido").

(29) "...En el tema que nos ocupa o sea el atinente a la utilización por parte de V. del correo electrónico de su principal para la recepción y reenvío del abundante material que (por completo ajeno a su labor) manipulara la actual reclamante, interpreto como concordantes y no contradictorios a la totalidad de los testimonios recepcionados en estos Estrados, declaraciones que, en forma llamativa, fueran producidos inauguralmente por dos testigos cuya deposición ofreciera, justamente, la propia actora, circunstancia que, frente al aspecto en análisis, fortalece el valor probatorio de los dichos testimoniales de marras los cuales, por otra parte, no han sido objeto de impugnación o tacha alguna por los litigantes..." (Juzgado Nacional de Primera Instancia del Trabajo Nro. 24, Autos: "V.R.I c/Vestiditos SA s/despido", 27/05/2003, http://www.elderechoinformatico.com/jurisprudencia/Fallo_Vestiditos_Argentina.pdf).

(30) Juzgado Nacional de 1era Instancia en lo Civil Nro. 110, autos "G., M. J. c. Honda Automóviles de Argentina S.A. y otro", La ley Online: AR/JUR/3918/2008, quién asimismo cita a Daray, Hernán: "Derecho de daños en accidentes de tránsito", Astrea, Buenos Aires, 2001, t. 2, pág. 462, sumario 45 quién asimismo cita a la CNCiv. Sala I, 17/8/1995).

(31) "...con respecto a esta documentación, que su valor probatorio es relativo, ya que la solicitud ha sido desconocida por la parte actora y porque el correo electrónico ni siquiera fue exhibido a la testigo Ventura, a quien — según se desprende- habría sido dirigido..." (CNTrab. Sala II, autos: "Del Valle, Ana Belén c. Cardinal Servicios Integrales S.A.",25/07/2008, La Ley Online: AR/JUR/5904/2008).

(32) "...el resultado de la pericial informática, resulta claro y preciso, lo que a mi criterio lo torna contundente en cuanto a que no se logró acreditar que haya sido el actor quien enviara los emails con contenido confidencial tal como denuncia su empleadora. Lo antes señalado surge de la pericial informática y sus aclaraciones (fs. 250/263 y 281, 379/387), ya que a fs. 261 indica que se ha verificado la existencia de falencias de seguridad, y detalla que el personal de la demandada, tenía control absoluto sobre los elementos que a posteriori fueron objeto de peritación, por lo tanto, tenían la posibilidad de alterar el contenido de los elementos que luego fueron objeto de estudio. Considero oportuno y clarificante, para la resolución de este conflicto, transcribir las conclusiones finales del experto informático (fs. 386) "... Si bien se encontraron los mensajes de fechas 27.12.06 y 31.01.07, que figuraban como enviados desde una cuenta de correo electrónico que la parte demandada afirma le pertenecía al actor, la única relación cierta que se relevó fue la vinculación entre la denominación de la misma y de la dirección de correo con el nombre del actor; pero como ya indicara en reiteradas oportunidades esto no es suficiente, ni siquiera necesario, para poder confirmar que dichos e-mails fueron enviados por una cuenta propiedad de actor y mucho menos que esa persona física haya creado y/o enviado los mensajes peritados..." ("Saporiti, Pablo Alberto c/Peugeot Citroen Argentina S.A. y otro s/Despido", CNTrab - Sala VII - Juzgado Nº 3).

(33) "...el escueto informe presentado por el experto (fs. 368 y explicaciones en fs. 389) carece de fundamentos técnicos que comprueben que efectivamente los correos electrónicos acompañados hubieran sido enviados por algún funcionario o gerente del Banco de la Provincia de Buenos Aires habilitado al efecto. En rigor, el experto sólo introduce valoraciones subjetivas, mediante las cuales infiere que las siglas de la cuenta de mail de donde se recibieron los correos pertenecerían al "servidor dependiente del banco" (fs. 389). Pero no brinda una explicación técnica que corrobore sus dichos, como podría ser un análisis de las cuentas de correo del Banco de la Provincia o algún medio verificatorio del remitente de los correos electrónicos. Es más, el peritaje fue únicamente realizado sobre la computadora de la actora, y consistió en la impresión de cierta cantidad de e-mails recibidos por "diseño bar". En tales condiciones, no cabe asignar a ese dictamen pleno valor probatorio de conformidad con las normas de la sana crítica (conf. art. 477, Código Procesal)."(CNCom. Sala C, autos: "Soft Bar S.R.L. c. Banco de la Provincia de Buenos Aires", 11/09/2009, La Ley Online: AR/JUR/34729/2009).

(34) "...En cuanto al pago del "bonus", advierto que la sentencia de grado tuvo especialmente en cuenta para considerar la procedencia de aquél el resultado de la pericia técnica. A través de esta última quedó demostrada la autenticidad del correo electrónico enviado por el Sr. Tobal —vicepresidente de la empresa— mediante el cual se comunicó al actor su incorporación al plan de incentivos anuales por bonus (fs. 85 reconocido a fs. 249). Este punto, de vital importancia para la solución del debate en la tesitura del sentenciante de grado, fue soslayado por el apelante incumpliendo así con el art. 116 de la LO. Además, el rango gerencial resulta no sólo de las declaraciones testimoniales sino también del organigrama de la empresa, en especial el obrante a fs. 289 extraído del sistema informático de la demandada por el perito técnico, así como el correo electrónico de fs. 282 que corrobora el de fs. 83, consistente en una comunicación remitida por Tobal anunciando que Mammes había sido nombrado "gerente de ingeniería para marketing applications". Propongo pues desestimar este segmento de la queja..." (CNTrab. Sala I, autos: "Mammes, Axel c. Gilbarco Latin America S.A.", 26/11/2007, La Ley Online: AR/JUR/9377/2007).

(35) "Las copias de los mensajes de correo electrónico acompañados no son hábiles para arribar a una conclusión razonable sobre los hechos expuestos en este caso, toda vez que no son eficaces para identificar a la persona que los mandó pues la casilla estaba a nombre de otra persona y si bien en la firma figura el nombre de la actora, o su apodo, ello no se asimila a la firma digital, por lo que en este caso tales documentos no tienen más valor que el de un indicio, pues tampoco fueron corroborados por ningún otro elemento probatorio, deficiencia que deberá asumir la parte en los términos del art. 377 del CPCCN."(CNTrab. Sala VIII, "Mullins, María c/Stratford Book Services S.A. s/despido", 31/10/05).

(36) "Tampoco se invocó y menos se acreditó que la actora utilizara para fines personales a través de su correo electrónico la máquina proporcionada por la empresa como también Internet, y que redactara y enviara mensajes destinados a terceros ajenos a la empresa. En tal sentido, no puede entenderse fundado el despido, ya que con las declaraciones testimoniales que obran en la causa (ver fs. 133, 135, 137 y 148), se desprende que las PC eran utilizadas por todos los empleados de la compañía, teniendo libre acceso a ella" (CNTrab. Sala X, Autos: "López, Marcela Edith c. C.C.R. S.A. Concord Consumer Comunication Research Development S.A.", La Ley DT 2009 (febrero), 166, con nota de Héctor A. García; DJ11/03/2009, 626).

(37) "...Ante circunstancias como la descripta cualquier observador advierte que se plantea una alternativa en los términos binarios que señalaba Josserand: o el Derecho se adecua a la nueva realidad, o ésta prescinde del Derecho, porque una regla sólo está viva si está en marcha, como toda sociedad y todo hombre. Y aunque la ley por lo general controla los temerarios saltos hacia el futuro con la mano fuerte del pasado y combate la tecnología de hoy con instrumentos de ayer, va de suyo que cuando los hechos prescinden del Derecho, la juridicidad es puesta en crisis y la sociedad también deja de lado a los operadores jurídicos (conf. Alterini, Atilio Aníbal 'Respuestas ante las nuevas tecnologías: sistemas, principios y jueces' La Ley on line 03/12/07)." (Cita realizada por la Corte Suprema de Justicia de Mendoza, al resolver sobre la constitucionalidad del nuevo sistema de notificaciones electrónicas implementado en el poder judicial de la provincia, autos: "C.G.T. y otros c. Provincia de Mendoza", 13/03/2008, La Ley Online: AR/JUR/699/2008).