PROBLEMAS QUE ENFRENTA LA PRUEBA DIGITAL EN LOS ESTADOS UNIDOS DE NORTEAMÉRICA

Problems faced by digital evidence in U.S. Law*

Juan Carlos Marín González[**]
Guillermo J. García Sánchez[***]

Resumen: El presente artículo analiza los problemas que en el derecho de los Estados Unidos de Norteamérica enfrenta la prueba digital. Al no contar con una regulación particular para este tipo de prueba, los jueces han aplicado las normas previstas para las pruebas físicas. Lo anterior si bien ha resultado útil en muchos casos, ha generado más de algún problema que la doctrina de Estados Unidos ha criticado. Desde esta perspectiva se debe tener presente que no todas las reglas y procedimientos previstos para las pruebas físicas, se pueden aplicar sin más a la confiscación de una prueba digital.

Palabras clave: prueba digital – proceso penal en EE.UU. – cadena de custodia – normas y principios que rigen la prueba.

Abstract: This article focuses on the problems faced by digital evidence in U.S. law. As there are no specific regulations for this type of evidence, judges have applied norms contemplated for physical evidence. Although this has resulted useful in many cases, more than one problem has arisen and been criticized by U.S. doctrine. From this perspective, it is important to bear in mind that not all the rules and procedures contemplated for physical evidence can readily be applied to the confiscation of a piece of digital evidence.

Keywords: digital evidence – USA criminal process – chain custody – law of evidence.

1. Introducción

El presente artículo analiza los problemas que en el derecho de los Estados Unidos de Norteamérica enfrenta la prueba digital. Se estudian las condiciones

* Los autores desean agradecer las lúcidas observaciones formuladas por dos evaluadores anónimos de la *REJ*.

** Doctor en derecho. Profesor de tiempo completo ITAM. Profesor visitante Universidad de Houston; correo electrónico: jcmarin@itam.mx

*** LLM Harvard Law School; correoelectrónico:ggarciasanchez@gmail.com

Este artículo fue recibido el 23 de septiembre de 2014, siendo aprobada su publicación el 6 de diciembre de 2014.

bajo las que se puede admitir o desechar una prueba digital –por ejemplo el disco duro de una computadora– en dicho país. El documento aborda los antecedentes jurisprudenciales, las normas sobre la materia y la opinión de la doctrina más relevante de EE.UU. Es un trabajo especialmente descriptivo de lo que sucede con este tipo de prueba en el país del Norte, aun cuando en algunos aspectos se toma partido y se critica alguna solución. Frente a la prácticamente nula regulación de esta materia en Chile y a lo poco que se ha escrito sobre el particular, el trabajo pretende, también, servir de referente para la eventual solución de casos que involucren este tipo de pruebas en el país.

El ensayo sigue el orden de las distintas etapas que enfrenta el proceso penal en EE.UU. Desde esta perspectiva, el lector debe tener presente que esta prueba –al igual que cualquier otra– puede ser desechada preliminarmente por el juez por no haber sido autentificada de manera correcta (consideraciones relacionadas con las reglas federales de evidencia); puede ser rechazada por la forma en la cual fue obtenida (consideraciones relacionadas con la Cuarta Enmienda constitucional y el cateo); y finalmente, se puede cuestionar su credibilidad en el juicio mismo al momento de ser valorada por el jurado (consideraciones relacionadas con la forma en la que fue presentada por la autoridad). Este último aspecto no se aborda en este trabajo.

Cabe resaltar que las normas generales relativas a la prueba en los EE.UU. no han sido modificadas a pesar de los retos que representa la evidencia digital según lo mostraremos. Han sido los jueces quienes han interpretado los cánones y las reglas generales a la luz de esta particular prueba. En general, se puede afirmar que en EE.UU. existe una presunción de validez de la prueba presentada por la autoridad cuando proviene de la computadora del acusado; no así, en cambio, cuando proviene de Internet, donde las fuentes y la relación de autoría con el acusado son más débiles. Esta regla no debe ser compartida del todo.

2. Consideraciones generales respecto de la prueba digital

En principio la presentación de una prueba en el sistema judicial de los Estados Unidos se rige por las Reglas Federales de Evidencia (*Federal Rules of Evidence*).[1] Si bien cada uno de los cincuenta estados que conforman la Unión Americana tiene sus propias normas sobre la materia, las reglas federales han servido de modelo para la mayoría de ellos. El estatus de la prueba electrónica (o relacionada con la informática) no es distinto del resto de las pruebas que se pueden presentar en un proceso judicial. Los principios y reglas generales que emanan del Reglamento Federal no se han modificado frente a los nuevos desafíos que presentan los

[1] Las *Federal Rules of Evidence* –*FRE*– fueron adoptadas por orden de la Corte Suprema el 20 de noviembre de 1972. Fueron remitidas al Congreso de la Unión por el presidente de dicha Corte el 5 de febrero de 1973. Finalmente, entraron en vigor el 1 de julio de 1973. La última modificación realizada es del 1 de diciembre de 2011. Véase: http://www.law.cornell.edu/rules/fre/

sistemas electrónicos en esta materia.[2] En este sentido, toda prueba debe ser relevante, auténtica y confiable (*FRE* Nos. 402, 801 y 901).[3]

En Estados Unidos han sido los jueces quienes interpretando estos principios han adaptado las reglas a las nuevas circunstancias.[4] Al igual que ocurre con otras pruebas, los componentes u objetos informáticos deben enfrentar un proceso de autentificación (*authentication*), que puede involucrar la presencia de dos o más testigos los que deben identificar los objetos y explicar la forma en la que se relacionan con el proceso en cuestión.[5]

Cabe resaltar que los jueces tienen facultades para resolver cualquier tema preliminar respecto de la admisibilidad de una prueba digital. Así lo establece la *FRE* en su número 104: "(a) En general. El tribunal debe decidir cualquier tema preliminar relacionado con la calificación de los testigos, los privilegios existentes, o la admisibilidad de la prueba. En esta decisión preliminar, el tribunal no está obligado a seguir el Reglamento de Evidencia, excepto en lo relativo a los privilegios".[6] Esta admisión preliminar por parte del juez no significa que, ulteriormente, el jurado no pueda valorar si ella es confiable y si puede servir de base para determinar la existencia de un hecho relacionado con el proceso.[7]

3. Proceso de autentificación

En el sistema procesal estadounidense se debe acreditar la autenticidad de cualquier prueba que se desee presentar en un proceso judicial.[8] Este procedimiento recibe el nombre de "autentificación" (*authentication*) y representa uno de los retos más complicados para los abogados en EE.UU.

El proceso de autentificación enfrenta los mismos pasos procesales independientemente del tipo de prueba de que se trate.[9] Quien la propone debe mostrar:

1) que el contenido del documento es completo y no ha sido alterado;
2) que proviene de la fuente que se alega;

[2] SCOTT (2004), p.162.
[3] *Ibíd.*
[4] RICE (2008), p. xvii.
[5] *Ibíd.* p. xx.
[6] Traducción libre de los autores de la regla N° 104 de la *FRE*. El texto original en inglés señala lo siguiente: "*RULE 104. PRELIMINARY QUESTIONS.*
(a) In General. The court must decide any preliminary question about whether a witness is qualified, a privilege exists, or evidence is admissible. In so deciding, the court is not bound by evidence rules, except those on privilege".
[7] RICE (2008), p. 359.
[8] *Ibíd.*, p. 335.
[9] *Ibíd.*

3) en el caso de evidencia relativa a la existencia de relaciones contractuales, se debe probar que los individuos tenían la intención de estar vinculados a la sustancia contenida en la comunicación.[10]

Las *FRE* y las decisiones de los tribunales en Estados Unidos han desarrollado una serie de estándares y principios para evaluar estas etapas. De conformidad con las *FRE* toda prueba debe tener una relevancia lógica con el presupuesto que se intenta probar. La prueba puede, en todo caso, ser excluida si su eventual daño al proceso (por ejemplo, la dilación del mismo o la confusión que podría generar en el jurado) supera sustancialmente (*substantially overweights*) su valor probatorio.[11] Volveremos sobre este punto un poco más adelante.

Como hemos avanzado, toda la prueba digital debe ser autentificada con independencia de que la evidencia sea presentada en formato digital, o sea un testimonio basado en la información electrónica obtenida.[12] En el proceso se debe probar que tanto el autor de la evidencia digital como el testigo tuvieron conocimiento personal (*personal knowledge*) de los hechos contenidos en la misma.[13]

4. Métodos de autentificación

La *FRE* N° 901 describe el proceso por el que se puede autentificar la prueba presentada durante el juicio. En la práctica la evidencia digital ha sido interpretada conforme a las disposiciones generales de la prueba las cuales son, en principio, suficientemente flexibles para adaptarse a las nuevas circunstancias. Asimismo, prácticamente todos los métodos de autentificación empleados por los jueces pueden ser utilizados puesto que caen dentro de la definición empleada por el referido numeral N° 901. El principio rector es que cualquier medio puede ser admitido como prueba de la autenticidad de la evidencia siempre y cuando su eventual daño al proceso no sea sustancialmente mayor (*substantually outweight*) a su valor probatorio.[14]

La *FRE* N° 901 contiene una serie de métodos de autentificación que ni son excluyentes ni tienen un determinado orden de prelación. Cada uno de los

---

[10] *Ibíd.*

[11] FRE N° 403. El texto completo en inglés es el siguiente: "*RULE 403. EXCLUDING RELEVANT EVIDENCE FOR PREJUDICE, CONFUSION, WASTE OF TIME, OR OTHER REASONS. The court may exclude relevant evidence if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence.*" Los precedentes en los cuales se ha discutido lo anterior en el contexto de la prueba digital incluyen *Ruth v. Superior Consultant Holdings Corp*., 2000 WL 1769576, *6 (E.D. Mich Oct. 6, 2000) en el cual se discutió el mensaje contenido en un correo electrónico.

[12] RICE (2008), p. 336.

[13] *Ibíd.*

[14] FRE 403, supra nota 11; para ejemplos de la extensión de este principio en materia de comunicaciones digitales véase: *Whatley v. S.C. Dept of Pub. Safety*, 2007 U.S. Dist., *40-41 (D.S.C. Jan. 10, 2007). Véase *United States v. Siddiqui*, 235 F.3d 1318, 1322-23 (11th Cir. 2000); *Fenje v. Feld*, 301 F. Supp. 2d 781, 809 (N.D. Ill. 2003).

párrafos describe un método considerado como aceptable, mismo que puede ser redefinido por cada juez en el caso concreto.[15] En específico la regla anteriormente aludida establece lo siguiente: "En general. Para satisfacer los requisitos de autenticidad o para identificar un medio probatorio, quien presenta la prueba debe producir evidencia suficiente que respalde el hecho de que el medio es lo que se alega que es".[16]

Los jueces han tenido oportunidad de aplicar estas reglas, entre otros, en los siguientes procesos:

a) En *United States v. Jackson* la Corte Federal del Séptimo Circuito consideró que no existía una adecuada autentificación respecto de la información obtenida de Internet, porque no se probó que la organización a la cual se le atribuía la autoría hubiese subido dicha información a la red.[17]

b) En *Wady v. Provident Life & Accident Ins. Co. of Am*. una corte en California resolvió que no podía considerarse como autentificada cierta información obtenida de la página de Internet de la empresa demandada, puesto que no se pudo comprobar ni quién administraba el sitio web, ni quién era el autor de la información publicada ni, finalmente, la veracidad de los contenidos.[18]

c) En *St. Clair v. Johnny´s Oyster & Shrimp*, *Inc.*, una corte en Texas determinó que un sitio en Internet privado no podía ser autentificado puesto que siempre existe la posibilidad de que *hackers* modifiquen su contenido.[19]

La regla 901(b) enumera una serie de ejemplos no exhaustivos ni limitativos que satisfacen la regla general.[20] El primer ejemplo es la declaración de personas con conocimiento. Se define como el testimonio que prueba que una cosa es lo que se alega que es (*Testimony that anitemisw hatitis claimed to be*).[21] Lo anterior ha sido interpretado en varias ocasiones frente a situaciones que involucraban evidencia digital. Algunos ejemplos son:

a) *Hardison v. Balboa Ins. Co* en este proceso el tribunal resolvió que la información contenida en una computadora quedaba autentificada puesto que un testigo con

---

[15] RICE (2008), p. 339.

[16] RFE 901, "*RULE 901. AUTHENTICATING OR IDENTIFYING EVIDENCE. (a) In General. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.*"

[17] *United States v. Jackson*, 208 F.3d 633, 638 (7th Cir. 2000).

[18] *Wady v. Provident Life & Accident Ins. Co. of Am*., 216 S. Supp. 2d 1060, 1064-65 (C.D. Cal. 2002).

[19] *St. Clair v. Johnny's Oyster & Shrimp, Inc.*, 76 F. Supp. 2d 773, 775 (S.D. Tex 1999).

[20] El texto original de la *FRE* 901(b) en inglés establece lo siguiente: "*Examples. The following are examples only –not a complete list– of evidence that satisfies the requirement:*"

[21] FRE 901 (b)1.

conocimiento directo de la máquina, señaló que los registros de la compañía se mantenían en esa máquina en particular.[22]

b) *St. Luke´s Cataract & Laser Institute P.A. V. Sanderson* en este otro proceso un tribunal de Florida resolvió que la información contenida de un sitio *web* podía ser autentificada, si se presentaba el testimonio de alguien que asegurara que tenía conocimiento del sitio como, por ejemplo, el administrador de la página *web*.[23]

c) En *Securities & Exch. Comm´n v. Berger* un testigo autentificó los documentos electrónicos presentados por otro testigo al alegar que habían sido los mismos documentos electrónicos que él había descargado de esa computadora.[24]

d) En *United States v. Scott-Emuakpor* se autentificó la información obtenida de una computadora por medio de la declaración de dos testigos que observaron cómo se extrajo la información de la máquina del demandado.[25]

e) En *Page v. State* el casete obtenido de una cámara de video donde se grabó el robo de una tienda comercial fue autentificado por un empleado que, si bien no presenció el robo, describió cómo funcionaba la grabación de la cámara hacia el disco duro de la computadora, la forma cómo accedió al disco poco después del robo, la revisión que hizo de la grabación con la policía y la entrega de la copia del video a la fuerza de orden.[26]

f) En *Am. Express Travel Related Services Co. v. Vinhnee* un tribunal determinó que la autenticidad de la información contenida en una computadora requería de un testimonio que probara la política y el sistema de control de la información en la misma, dentro de los cuales enlistaba, como ejemplos, el control de acceso a base de datos, forma en que se grababan y se modificaban los datos en la computadora, las prácticas de respaldo o *backup*, y los procedimientos de auditoría que se realizaban para asegurar la integridad de la información contenida en la máquina.[27]

Otra forma de autentificar la evidencia digital es a través de la Regla N° 901(b) (9) que establece que se puede presentar "evidencia que describa el proceso o sistema utilizado para generar un resultado, o demostrar que el sistema reproduce un producto confiable".[28] La Corte Federal del Tercer Circuito en el caso *United States*

[22] *Hardison v. Balboa Ins. Co.*, 4 Fed. Appx. 663, 669 (10th Cir. 2001).
[23] *St. Luke´s Cataract & Laser Institute P.A. V. Sanderson*, 2006 WL 1320242 en *2 (M.D. Fla. May 12, 2006).
[24] *Securities & Exch. Comm´n v. Berger* 224 F. Supp. 2d 180, 192 (S.D. N.Y. 2001).
[25] *United States v. Scott-Emuakpor*, 2000 WL 288443 en *14 (W.D. Mich. Jan. 25, 2000).
[26] *Page v. State*, 125 S.W.3d 640, 647 (Tex. Ct. App. 2003).
[27] *Am. Express Travel Related Services Co. v. Vinhnee*,.336 B.R. 437, 448-49 (B.A.P. 9th Cir. 2005).
[28] Traducción libre de los autores. El texto en inglés de la RFE 901(b) (9) es el siguiente: *"[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result*."

v. Downing determinó que este era el método por excelencia para autentificar la evidencia digital.[29]

Otro mecanismo –fuera de los establecidos en la *FRE* para cuestionar la autenticidad de la evidencia presentada– es la petición *in limine* establecida en la *Federal Rules of Criminal Procedure* regla 12(b).[30] Esta petición se puede presentar antes de que inicie el juicio y sin la presencia del jurado.[31] Lo anterior implica que el juez analice la base que fundamenta la evidencia presentada, es decir, si produce o no el resultado alegado. Normalmente involucra las declaraciones de peritos en la materia respecto de la forma en la que se extrae la evidencia o se transfiere la misma de un sistema a otro.[32] En este sentido, el *software* utilizado y la cadena de custodia presentada por los peritos forenses sobre el disco duro, durante la investigación, puede sujetarse a este proceso preliminar.[33]

5. Información obtenida de computadoras y la cadena de custodia

La autentificación de la evidencia generada por medio de una computadora implica que se debe validar el contenido de los documentos.[34] Se debe comprobar que los mismos no han sido alterados desde el momento en que se volvieron relevantes y el momento en que son presentados ante el juez. La forma tradicional de hacerlo es mediante lo que se denomina la "cadena de custodia" (*chain of custody*).[35]

La cadena de custodia implica que cada uno de los custodios secuenciales de la prueba debe asegurar que no la modificó y que la protegió ante la posibilidad de que otros lo hicieran.[36] La cadena de custodia se utiliza normalmente en materia penal para proteger muestras tomadas de algunas evidencias físicas, como lo son las de sangre, residuos de narcóticos o huellas dactilares para, eventualmente, generar una nueva prueba.[37] La lógica deriva de asegurar que la sangre, cocaína o huella sean la misma que la obtenida en la escena del crimen y que ella no fue alterada en el momento en que se analizó.[38] En el caso de documentos o archivos electrónicos la cadena de custodia se puede mostrar mediante la existencia de protocolos o procedimientos internos, respecto del acceso a documentos o carpetas electrónicos con claves digitales, como son las

[29] GIORDANO (2004), p. 163 en referencia a *United States v. Downing*, 753 F.2d 1224 (3d Cir. 1985).
[30] Federal Rules of Criminal Procedure. Originalmente aprobadas por la Suprema Corte de los Estados Unidos el 26 de diciembre de 1944, enviadas al Procurador General el 3 de enero de 1945, y en vigor desde el 21 de marzo de 1946. La última modificación fue realizada el 26 de abril de 2011 la cual entró en vigor el 1 de diciembre de 2011. Disponible en http://www.law.cornell.edu/rules/frcrmp/
[31] GIORDANO (2004), p. 164.
[32] *Ibíd.*
[33] *Ibíd.*
[34] RICE (2008), p. 356.
[35] *Ibíd.*, p. 395; GIORDANO (2004), p. 164.
[36] RICE (2008), p. 395.
[37] *Ibíd.,* p. 396.
[38] GALVES Y GALVES (2004-2005), p. 44.

encriptaciones en documentos (*hashing*), con *passwords* para acceder al documento que registran los cambios y los accesos que se tuvieron al mismo, y realizando copias mediante procesos espejo (*mirror image*).[39]

Los casos más comunes en contextos de prueba digital en los cuales la cadena de custodia puede ser cuestionada, se encuentran relacionados con la confiscación de discos duros o computadoras y la subsecuente grabación de copias por parte de la autoridad.[40] En estas situaciones, salvo que exista evidencia específica que demuestre alguna alteración del objeto, los jueces tienden a concluir preliminarmente que el disco duro o la computadora son auténticos.[41] En palabras de la Corte Federal del Undécimo Distrito en el proceso *United States v. Glasser* "la existencia de un sistema de seguridad incorruptible [para prevenir que se altere la información] no es […] un prerrequisito de admisibilidad de la prueba obtenida de una computadora. Si semejante prerrequisito existiera, se volvería prácticamente imposible admitir cualquier registro generado por una computadora".[42] El anterior razonamiento fue confirmado por la Corte Federal del Noveno Circuito al argumentar que "el hecho de que sea posible alterar los datos contenidos en la computadora es insuficiente para afirmar que se debe desconfiar de su autenticidad".[43] Otro ejemplo lo encontramos en el caso *United States v. Whitaker* en donde el juez decidió que la pura especulación de alteración de evidencia no era suficiente para declarar la información obtenida de una computadora como no auténtica.[44] Lo anterior a pesar de que la autoridad que presentó la prueba no pudo probar que los agentes no manipularon la información contenida en la computadora, o en el disco incautado durante un cateo.[45]

En términos generales, los tribunales no han exigido –frente a la presentación de información digital recabada de discos duros– que la persona que exhibe la evidencia garantice cabalmente que no se ha alterado la cadena de custodia.[46] Nótese como en este caso la carga de la prueba se invierte. En principio las especulaciones infundadas de alteración de la prueba digital no son suficientes para tenerla como no auténtica. A la autoridad le basta con probar que existió una cadena de custodia razonable para que el juez, en principio, la admita.

---

[39] LUEHR(2005-2006), pp. 17-18.

[40] Ver por ejemplo *Kupper v. State*. 2004 WL 60768, en *2-3 (Ct. App. Tex. Jan. 14, 2004); RICE (2008), p. 396.

[41] RICE (2008), p. 396.

[42] Traducción libre de los autores de *United States v. Glasser*, 773 F.2d 1553 (11th Cir. 1985), 1559. El texto original en inglés es el siguiente: "*The existence of an air-tight security system [to prevent tampering] is not [. . .] a prerequisite to the admissibility of computer printouts. If such a prerequisite did exist, it would become virtually impossible to admit computer-generated records.*"

[43] Traducción libre de los autores de *United States v. Bonallo*, 858 F.2d 1427 (9th Cir. 1988). El texto original en inglés es: "*the fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrust- worthiness.*"

[44] *United States v. Whitaker*, 127 F.3d 595, 602 (7th Cir. 1997); RICE (2008), p. 397.

[45] *Ibíd.*

[46] El nivel de garantía depende de la naturaleza del objeto, de la importancia del mismo en el caso y de la facilidad con la que puede ser alterado. RICE (2008), pp. 396-397.

En cambio si se presenta por el imputado una prueba razonable de que la evidencia ha sido alterada, entonces la parte que la exhibe debe acreditar que el contenido del disco duro –o de la computadora– no ha sido alterado en ningún momento. Lo anterior podría probarse mostrando los protocolos, el *software* o la existencia de claves de acceso a la información en la computadora, o el disco duro, así como los registros documentales sobre las personas que tuvieron acceso al objeto.

De acuerdo con Paul Rice a pesar de que algunos *hackers* pueden violar estos protocolos de seguridad, es suficiente con probar *prima facie* ante el juez dichos elementos. Posteriormente frente al jurado –durante el proceso de ponderación de la evidencia– deberá acreditar que la prueba es lo que dice que es y que tiene una conexión lógica con los argumentos presentados.[47] De acuerdo con este mismo autor la lógica de la "cadena de custodia" no se encuentra muy clara en la presencia de documentos electrónicos, puesto que –a diferencia de las pruebas tradicionales– en este caso no se pretende generar alguna evidencia adicional (como, por ejemplo, exámenes de ADN de una muestra de sangre, o un perfil obtenido de una muestra dactilar o de cabello).[48]

Debe aclararse, en todo caso, que la proclividad de los jueces de admitir *prima facie* toda la información obtenida de un disco duro no afecta el hecho de que, posteriormente, el jurado pueda determinar que esta no es confiable al momento de decidir el peso específico que le dará a la evidencia. En otras palabras, en la práctica la cadena de custodia tiene mayor peso en la evaluación por parte del jurado respecto de la credibilidad de la evidencia, que en la admisión de la misma de manera preliminar por parte del juez.[49] En resumen, si no existe evidencia en contrario bastará con el testimonio de los oficiales que recabaron la evidencia, la clasificaron, resguardaron y la presentaron ante el juez para que sean admitidas como pruebas que el jurado deberá valorar, aunque esto no implique que posteriormente se cuestione su credibilidad en el juicio mismo y, en consecuencia, que el jurado le otorgue menos peso en su decisión.[50]

La admisión preliminar por parte de los jueces sin mayor cuestionamiento no parece ser del todo razonable. Si bien la prueba debe ser valorada posteriormente en el proceso, la autoridad ya ha conseguido que la prueba sea uno de los elementos de cargo que llevará al juicio. Queda la impresión de que la autoridad tiene una considerable ventaja al momento de presentar este tipo de evidencia. Es preferible ver las peculiaridades de cada caso y elaborar una regla concreta de acuerdo con las condiciones específicas que se tienen a la vista en vez de construir una regla general que, *prima facie,* altera la carga que tienen las partes en un proceso judicial. Luego veremos, con mayor detalle, un concreto manual

[47] RICE (2008), pp. 395-398.
[48] RICE (2008), pp. 398.
[49] GALVES Y GALVES (2004-2005), p. 44.
[50] RICE (2008), pág. 396; GIORDANO (2004), p. 164.

que existe en EE.UU. al momento de manejar este tipo de evidencia. En general, estos manuales pueden ser un buen instrumento para establecer en cada caso como debe ser tratada la admisión de esta prueba. No se puede olvidar que el material probatorio contenido en soporte digital es particularmente frágil y delicado. La menor manipulación puede dañarlo, alterarlo o incluso destruirlo. Además, debido a que las modificaciones a este tipo de evidencia pueden ser difíciles de detectar, es fundamental que los equipos encargados de recolectarla y conservarla lo hagan siguiendo rigurosamente los procedimientos establecidos para evitar ulteriores problemas.

Lo anterior ha llevado a la doctrina a proponer que se modifiquen las reglas respecto de la forma en la que se recolecta la prueba digital.[51] En opinión de esta doctrina las reglas actuales fueron creadas para recoger evidencia física y presencial. La prueba digital, en cambio, tiene una lógica completamente distinta. En su parecer "las reglas contemporáneas del procedimiento penal son del mundo físico que reflejan las realidades de las investigaciones en dicho mundo. Son un intento de balancear las necesidades de privacidad y de la ejecución de la ley a la luz de la forma en la que la policía recoge la prueba física y las declaraciones de testigos presenciales".[52] Lo anterior genera que en ciertas circunstancias las reglas no logren imponer ningún tipo de restricción al uso del poder por parte de las fuerzas del orden y que las mismas, en otras ocasiones, sirvan como impedimento para realizar una investigación adecuada.[53]

6. Guías o manuales en materia de prueba digital

El uso de procedimientos adecuados durante la recopilación y conservación de evidencia contenida en medios electrónicos es indispensable para garantizar el valor probatorio de la misma. Esto resulta particularmente importante en procesos de naturaleza penal en los que, debido a la importancia de los bienes jurídicos involucrados, el estándar de admisibilidad de la evidencia es especialmente elevado. Es por esa razón que en diversas jurisdicciones las dependencias encargadas de la recolección de la evidencia que será utilizada en procesos penales han creado manuales en los que se detallan rigurosos procedimientos que deben seguirse a fin de garantizar la adecuada conservación de evidencia contenida en medios electrónicos. La finalidad de estas guías es evitar que la información que se encuentra en soporte electrónico se contamine o se pierda, afectando su valor probatorio en cualquier proceso judicial. En Chile donde en general no hemos desarrollado una gran cultura sobre este tema, es conveniente que tanto la autoridad como nuestros jueces se familiaricen con este tipo de guías o manuales a efectos de no vulnerar los derechos de las personas sometidas a una investigación criminal.

[51] KERR(2005), p. 280.
[52] *Ibíd.* p. 289.
[53] *Ibíd.* p. 293.

Entre los diferentes manuales de buenas prácticas que se han desarrollado para conducir la actividad de las entidades encargadas de recopilar evidencia que será utilizada en procesos penales deseamos resaltar los publicados en Estados Unidos. Estos manuales oficiales son actualizados constantemente para garantizar que los procedimientos seguidos por las diferentes corporaciones encargadas de recopilar evidencia se ajusten siempre a los más altos estándares técnicos y respondan a los constantes cambios en el ámbito de la tecnología y la computación.

En el caso de Estados Unidos el Departamento de Justicia (*Department of Justice*) ha publicado una serie de manuales que tienen como finalidad brindar información a los agentes encargados de recopilar evidencia sobre las mejores técnicas para recabar y conservar prueba contenida en medios electrónicos. Dentro de los que se han publicado, resulta particularmente importante el manual sobre Evaluación Forense de Información Digital: Una Guía para Oficiales (*Forensic Examination of Digital Evidence: A Guidefor Law Enforcement*).

El manual en cuestión comienza señalando tres principios fundamentales que deben seguirse durante todo el proceso de recopilación, custodia y análisis de prueba digital.

1) Deben tomarse todas las acciones necesarias para garantizar que durante el proceso de recopilación de la prueba digital no se afecte su integridad (*Actions taken to secure and collect digital evidence should not affect the integrity of that evidence*).

2) Cualquier persona que realice el análisis de evidencia en formato digital debe tener los conocimientos técnicos necesarios para esta labor (*Persons conducting an examination of digital evidence should be trained for that purpose*).

3) Cualquier actividad relacionada con la recopilación, análisis, almacenamiento o transporte de información contenida en formato digital debe ser señalada en los registros adecuados, los que deben estar disponibles para su posterior revisión (*Activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review*).

El manual publicado por el Departamento de Justicia de Estados Unidos distingue cuatro etapas en el proceso que va desde la decisión de recopilar determinada prueba electrónica, hasta el registro de todas las acciones relacionadas con el dispositivo que contiene la información utilizada como evidencia. Cada una de estas etapas tiene características diferentes, ya que el riesgo de daño o alteración de la información es diferente. Sin embargo, en todas las etapas es fundamental que los agentes sigan rigurosamente los procedimientos establecidos, ya que de lo contrario la prueba recopilada carecería de valor probatorio en un juicio.

La primera etapa se refiere a la determinación de la información digital que se considera relevante para el proceso. Los agentes deben establecer si la información contenida en dispositivos electrónicos es relevante para el proceso en cuestión y garantizar que cuentan con todas las autorizaciones judiciales necesarias para proceder a la recopilación del material probatorio. Cualquier falla en esta etapa del procedimiento afectaría la posibilidad de presentar la prueba en un procedimiento judicial.

La segunda etapa a la que se hace referencia en la guía es la etapa de recopilación. En este caso el principal riesgo es que al momento de hacerse con el control de los dispositivos electrónicos los agentes alteren o modifiquen la información ahí contenida. La prueba digital es, por su propia naturaleza, especialmente frágil y puede ser dañada o modificada si no se siguen los procedimientos adecuados durante su recopilación.

La tercera etapa se refiere al análisis de la información. Antes de poder realizar el análisis de la información es necesario que esta sea extraída del dispositivo recolectado. Como en todas las ocasiones en las que se interactúa con el dispositivo, es fundamental que solo personal con los conocimientos técnicos necesarios realice la extracción de la información. En estos casos se recomienda que cualquier análisis de la prueba digital se efectúe sobre una imagen realizada de la información contenida en el dispositivo. De esta forma los oficiales podrán trabajar sobre una copia y no sobre el dispositivo. Evidentemente, solo si se siguen los más rigurosos procedimientos se puede garantizar que la información extraída del dispositivo sea exactamente la que ahí se contenía y que no sufrió ninguna alteración o modificación durante ese proceso.

Finalmente, la cuarta etapa se refiere a la conservación de registros en los que se detallen todas las acciones relacionadas con la evidencia digital. Si bien conceptualmente el proceso de registro es una etapa independiente, ésta acompaña todo el proceso de recopilación, extracción y análisis de la información. Se debe generar un registro desde el momento que los oficiales detectan el dispositivo electrónico antes de su recolección. Es fundamental señalar que estos registros deben estar disponibles para ser presentados en juicio, ya que el valor probatorio de la evidencia digital depende en buena medida de que se hayan seguido los procedimientos adecuados y eso solamente puede probarse mediante los registros correspondientes.

7. Consideraciones constitucionales respecto de la confiscación de "discos duros"

En el sistema constitucional estadounidense la Cuarta Enmienda regula las facultades del Estado para realizar cateos y recolectar evidencia, tanto en lugares públicos como privados. Esta enmienda establece lo siguiente: "El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de

pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas".[54] La anterior disposición ha sido interpretada en varias oportunidades por los jueces, estableciendo límites y pasos a seguir en los cateos realizados por la autoridad.

En principio los jueces han considerado que los mismos principios relacionados con la evidencia física se aplican a la prueba digital.[55] Es decir,debe haber una expectativa razonable de que se respetará la privacidad del individuo por lo que la autoridad está sujeta a recabar solo aquella información que esté relacionada con una causa probable (*probable cause*) del delito, so pena de ser considerada inadmisible por el juez.[56]

En casos tradicionales en los que se realizan cateos en domicilios, o en algún otro tipo de propiedad privada, la jurisprudencia ha establecido reglas muy estrictas respecto de las facultades que tienen los agentes para seleccionar el tipo de objetos que pueden retirar del domicilio.[57] Por ejemplo, la orden de cateo debe contener el lugar específico y el tipo de objetos que se están buscando recabar en el domicilio particular.[58] En este sentido, el objeto confiscado debe coincidir con lo establecido en la orden de cateo. En caso de confiscar objetos que se encontraban a "plena vista" (*plain view*) estos deben estar vinculados con la orden de cateo mediante una causa probable (*probable cause*).[59] La Corte en *Maryland v. Garrison* señaló que "los límites de un cateo legal se definen por el objeto que él tiene y por el lugar en donde existe una causa probable que justifique pensar que el objeto se puede encontrar ahí".[60] Lo que se busca evitar son cateos generales e invasivos (*wide-ranging exploratory searches*) que permitan a los oficiales investigar indiscriminadamente en la propiedad de la persona.[61]

Ahora bien, la doctrina ha puesto de relieve que al aplicar estas reglas tradicionales del cateo a la recolección de prueba digital, como sucede en un disco duro, se han generado algunos problemas que los tribunales no han resuelto del todo. Por ejemplo, bajo estos criterios autores como Orin Kerr consideran que es

---

[54] La versión en español oficial fue obtenida de la página del gobierno de los Estados Unidos en http://www.archives.gov/espanol/constitucion.html.
[55] *United States v. Chan,* 830 FS Lipp. 531, 535 (N.D. Cal. 1993).
[56] GALVES Y GALVES (2004-2005), p. 40.
[57] KERR (2005), p. 299.
[58] Por ejemplo ver *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).
[59] KERR (2005), p. 299.
[60] Traducción libre de los autores. El texto completo en inglés es el siguiente: "*The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit. Thus, the scope of a lawful search is defined by the object of the search and the places in which there is probable cause to believe that it may be found.*" *Maryland v. Garrison*, supra nota 58, p. 1016.
[61] *Ibíd.*

difícil justificar que se confisque toda la computadora, a pesar de que por razones prácticas sea lo más lógico.[62] Las computadoras en la mayoría de los casos son un medio de almacenamiento de la evidencia, mas no la prueba en sí, puesto que la prueba del delito puede ser un documento o registro digital contenido en el disco duro, mas no el disco duro *per se*. El disco duro puede contener información personal o confidencial no relacionada con el delito; sin embargo, al confiscarlo en busca del archivo específico se le priva al individuo de todos los documentos contenidos en él. En este sentido, usando las reglas tradicionales de la Cuarta Enmienda, confiscar todo el disco duro sería contrario a los derechos consagrados constitucionalmente tratándose de cateos invasivos. En cierta manera, de acuerdo con Orin sería lo equivalente a confiscar el edificio de una oficina por el hecho de que la policía considera que en sus inmediaciones se encuentra un archivo o un objeto relacionado con el crimen.[63]

Lo anterior es un punto que los jueces tuvieron que atender en el caso *United States v. Tamura* (1982), en donde se cuestionó la legalidad de la confiscación de miles de archivos con el propósito de encontrar un documento que se presumía había sido escondido en los archiveros.[64] En ese caso la Corte Federal del Noveno Circuito resolvió que solo aquellos archivos que habían sido enumerados en la orden de cateo podrían ser retirados del lugar para ser inspeccionados en otro recinto. Lo contrario sería demasiado invasivo. Si la autoridad considera que los demás archivos estaban relacionados podía inspeccionarlos *in situ*, pero para retirar otros objetos no enumerados tendría que haber probado que su naturaleza incriminatoria era inmediatamente aparente.[65]

En el caso concreto de pruebas digitales, los tribunales estadounidenses han tenido que resolver esta tensión entre el derecho a la privacidad y la necesidad de buscar evidencias contenidas en un equipo electrónico. Por ejemplo, en *Davis v. Gracer*, la Corte Federal del Décimo Circuito resolvió que la confiscación de la computadora en el contexto de la búsqueda de evidencia del delito de pornografía infantil no era una exageración en el uso de la discreción otorgada a la policía para catear propiedad privada.[66] En su razonamiento, la Corte rechazó la analogía de que la computadora era como un contenedor, y resolvió que los discos duros constituían un instrumento del crimen. El hecho de que fueran utilizados también para otros fines no impedía que hubiera un vínculo lógico con la probabilidad de haber sido utilizados para el crimen, y en consecuencia su confiscación era válida. Sin embargo, la Corte también resolvió

---

[62] KERR (2005), p. 299.
[63] *Ibíd.*, p. 300. En *Kremen v United States* la corte resolvió que era ilegal la confiscación de una casa y la remoción de todos sus contenidos para buscar evidencia relacionada con el delito. *Kremen v. United States*, 353 U.S. 346 (1957).
[64] *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982).
[65] *Ibíd. United States v. Ewain*, 88 F.3d 689, 692-93 (9th Cir. 1996). En palabras del tribunal en *United States v. Ewain*: "*[o]nce the police are lawfully searching in a place for one thing, they may seize another that is in plain view, if its incriminating nature is immediately apparent.*"
[66] *Davis v. Gracey*, 111 F.3d 1472, 1478-80 (10th Cir. 1997).

que lo anterior no podría realizarse válidamente si no formaba parte de la orden de cateo, e incluso insinuó que se requeriría una nueva orden de cateo para revisar los correos encontrados dentro del disco duro si existía una causa probable de que estuvieran relacionados con el delito.[67]

En otro caso relacionado con la confiscación de computadoras para la búsqueda de documentos vinculados con el crimen, la Corte Federal en *United States v. Gorshov* resolvió que el hacer una copia del disco duro *in situ* no equivalía a una violación de la Cuarta Enmienda, puesto que no privaba de su propiedad al individuo.[68] Lo anterior es consistente con el criterio sostenido en *Arizona v. Hicks* y *United States v. Thomas*, en donde se resolvió que la copia de un número de serie o las fotocopias de documentos no constituyen una confiscación puesto que no privan al individuo de la posesión del objeto.[69]

Los precedentes referidos no implican que se resuelva el cuestionamiento respecto de la privacidad del resto de los documentos contenidos en el disco duro. Lo anterior es algo que ni los tribunales ni las normas legales han resuelto cabalmente en Estados Unidos. El hecho de que se pueda retirar el disco duro o que se realice una copia del mismo de forma que no sea violatorio de la Cuarta Enmienda, no conlleva a que la revisión de la información pueda llegar a ser considerada por algunos como una violación a la privacidad cuando se inspeccionan todos los archivos contenidos dentro de la computadora. [70] El precedente más cercano sobre este tema se dio en el caso de *Andersen v. Maryland* en el contexto de un cateo realizado en las oficinas de un abogado y donde el juez resolvió que es natural que se inspeccionen *in situ* varios documentos para determinar si están relacionados con el delito, a pesar de no estar cada uno enumerado en la orden de cateo, pero que correspondía a cada oficial asegurarse de que el cateo se llevare de una forma que minimizara las intrusiones a la privacidad (*conducted in a manner that minimizes unwarranted intrusión supon privacy*).[71]

No obstante lo anterior, el criterio no implica que puedan buscarse evidencias relacionadas con otros crímenes. Es decir, los tribunales podrían declarar como violatoria de los derechos constitucionales la prueba encontrada durante el cateo, que no estuviera directamente relacionada con el delito referido en la orden para así evitar el abuso de la policía.[72] Algunos jueces han resuelto que

---

[67] *Ibíd.*

[68] *United States v. Gorshkov*, No. CROO-550C, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001).

[69] *Arizona v. Hicks*, 480 U.S. 321, 324 (1987); *United States v. Thomas*, 613 F.2d 787, 793 (10th Cir. 1980).

[70] KERR (2005), pp. 301 y 302.

[71] *Andersen v. Maryland*427 U.S. 482, 2739. (1976).

[72] *United States v. Ross*, 456 U.S. 798, 824 (1982).*United States v. Van Dreel*, 155 F.3d 902, 905 (7th Cir. 1998). En palabras de la corte en *United States v. Van Dreel*: "*[U]nder Whren [...]once probable cause exists, and a valid warrant has been issued, the officer's subjective intent in conducting the search is irrelevant*"; *United States v. Ewain*, 88 F.3d 689, 694 (9th Cir. 1996). En *United States v. Ewain:* "*Using a subjective criterion would be inconsistent with Hoton, and would make suppression depend too much on how the police tell their story, rather than on what they did*".

el Gobierno no puede ampararse en los precedentes que permiten la incautación de evidencia que se encontraba a plena vista (*plein view*) al revisar un disco duro, puesto que este tuvo que abrir el archivo para revisar el documento.[73] Una vez más lo anterior demuestra la tensión que existe entre la búsqueda de información física y la información digital.

Finalmente, es importante resaltar que no existen precedentes ni reglamentos que establezcan límites respecto del tiempo que la autoridad puede retener un disco duro o la computadora. De acuerdo con los propios tribunales, ni la Cuarta Enmienda, ni las *FRE*, ni los precedentes judiciales establecen un límite de tiempo dentro del que los oficiales deben regresar los objetos digitales incautados.[74] En el último caso, *United States v. Hill*, una corte federal decidió que era "razonable" y en consecuencia constitucional que los oficiales confiscaran el disco duro, puesto que no podía pedírseles que se mantuvieran *in situ* indefinidamente buscando en el disco duro los documentos.[75]

Conclusión

En el presente documento hemos analizado las dificultades que en el derecho de EE.UU. enfrenta la prueba digital, principalmente al estudiar su admisión o rechazo como prueba de cargo en un proceso judicial. En general los jueces han adaptado las reglas generales de autentificación de la evidencia física al momento de analizar este medio de prueba. Probablemente la situación más delicada dice relación con la forma como las autoridades manejan la cadena de custodia de la prueba digital y las consecuencias que de ello se siguen para su validez. La admisión preliminar que los jueces de EE.UU. han desarrollado de esta prueba debe ser criticada. Parece mucho más razonable analizar cada caso en particular y no operar con una regla *prima facie* que ha producido, en los hechos, el desplazamiento de la carga probatoria. En este sentido puede ser muy útil analizar el grado de cumplimiento que la autoridad hace de los procedimientos que sobre el manejo de la prueba digital existen en EE.UU., para establecer una regla sobre su admisión o rechazo. Esta situación, incluso, puede servir como modelo para los jueces y las autoridades chilenas cuando enfrenten un problema de admisión, nulidad o valoración de este peculiar medio probatorio.

---

[73] *Véase United States v. Carey,* 172 F.3d 1268, 1273 (10th Cir. 1999); *United States v. Walser,* 275 F.3d 981, 986 (10th Cir. 2001). Para otro punto de vista de vista véase: *United States v. Mcvell,* 45 M.J. 406, 422 (C.A.A.F 1996).

[74] *United States v. Hernández*, 183 F. Supp. 2d 468, 480 (D.P.R. 2002). En *United States v. Hernandez*: "*[Rule 41 does not provide]for a specific time limit in which a computer may undergo a government forensic examination after it has been seized pursuant to a search warrant*".

[75] *United States v. Hill*, 322 F. Supp. 2d 1081, 1091-92 (C.D. Cal. 2004).

BIBLIOGRAFÍA:

- GALVES, Fred y GALVES, Cristine (2004-2005): "Ensuring the Admissibility of Electronic Forensic Evidence and Enhancing its Probative Value at Trial", 19 CRIM. JUST. 37.
- GIORDANO, Scott M. (2004): *Electronic Evidence and the Law*, INFORMATION SYSTEMS FRONTIERS 6:2.
- LUEHR, Paul H. (2205-2006): "Real Evidence, Virtual Crimes. The Role of Computer Forensic Experts", 20 CRIM. JUST. 14.
- KERR, Orin S. (2005): "Digital Evidence and the New Criminal Procedure", 105 COLUM. L. REV. 279.
- RICE, Paul R. (2008): *Electronic evidence, law and practice*, 2a. ed., ABA Publishing.