PRESENTACIÓN DEL LIBRO *LA EVIDENCIA ELECTRÓNICA*, DE LA LICENCIADA VIVIAN I. NEPTUNE RIVERA, DECANA DE LA ESCUELA DE DERECHO DE LA UPR

PONENCIA

LUIS RIVERA ROMÁN*

INTRODUCCIÓN

EN UN CASO FEDERAL, UNA PERSONA IMPUTADA ALEGÓ QUE NO ERA POSIBLE autenticar y vincularlo como autor de un mensaje electrónico puesto que no existe prueba que permita identificar su voz ni su caligrafía y tampoco se presentó una foto del imputado.[1] El argumento no procedió, pero ilustra cuánto ha cambiado la realidad probatoria en los tribunales. Cuando una persona utiliza un equipo electrónico para enviar un mensaje, lo determinante para identificar el autor del mensaje no será ni su voz ni la caligrafía, sino las características que quedan como un rastro tras el uso del equipo electrónico. En los años 70, 80 y a principios de los 90, resultaba impensable que se pudiera identificar a una persona como autor de un mensaje sin prueba sobre su voz, la caligrafía o su rostro. Al presente, el rastro electrónico que deja una persona resulta ser el medio que nos permite identificar al autor de un mensaje de datos.

En el diario vivir el uso de las redes sociales aumenta vertiginosamente en el ámbito privado y de igual forma en el ámbito público. Las comunicaciones entre las agencias del gobierno, las instituciones universitarias, las instituciones bancarias y las personas, ocurren de manera natural mediante el uso de equipos tales

---

* El autor es Juez retirado del Tribunal de Apelaciones y fue Presidente del Comité Asesor Permanente del Tribunal Supremo de Puerto Rico que propuso las nuevas Reglas de Evidencia de 2009.

1 U.S. v. Simpson, 152 F.3d 1241, 1249-1250 (10th Cir. 1998).

como la computadora, el iPad o los teléfonos inteligentes. Se trata del mundo presente, real y operacional. Por lo tanto, para lograr el conocimiento de la verdad en los tribunales se requiere acceso al mundo digital donde ocurren y transitan las comunicaciones entre el gobierno, el comercio y las personas. En sentido contrario, de no lograr acceso a las comunicaciones ocurridas en el mundo digital, la verdad que se conoce en los tribunales no será real ni cierta porque obvía y omite el amplio espectro de lo ocurrido en este entorno. No empece a que en el día a día utilizamos nuestros teléfonos inteligentes y computadoras con gran naturalidad y frecuencia, cuando nos enfrentamos a la interrogante de si lo dicho en el medio electrónico o digital debe ser fácilmente autenticado y admitido en el tribunal, surgen enormes obstáculos.

Nos planteamos entonces cómo procurar que ese mundo de avanzada, que es real y forma parte de la vida cotidiana de los seres humanos, logre acceso al proceso judicial. En ese entorno cobra gran relevancia el libro que hoy presentamos, *La Evidencia Electrónica*.[2]

¿Qué razones dificultan el acceso de la evidencia electrónica a los tribunales? Existen diversas razones que dificultan el acceso a los tribunales del mundo digital, pero quiero referirme particularmente a los dos asuntos que considero de mayor importancia.

I. La experiencia en los tribunales

Repasando y estudiando notas para la comparecencia de hoy, examiné decisiones del Tribunal de Apelaciones y del Tribunal Supremo de Puerto Rico. Cuál no sería mi sorpresa al descubrir que en las sentencias del Tribunal de Apelaciones el tema de la autenticación y admisibilidad de la evidencia electrónica apenas se ha discutido. De hecho, encontré un solo caso donde se discute el tema con amplitud. En el caso se debatía la autenticación y admisibilidad de un mensaje de texto enviado por un imputado a una víctima de violación a la Ley de Violencia Doméstica.

Pero mi sorpresa sería aún mayor puesto que no encontré una opinión del Tribunal Supremo en la que se discutiera los requisitos para la autenticación y admisibilidad de algún tipo de evidencia electrónica. Luego de investigar con mayor cuidado, confirmé entonces que efectivamente, ante el Tribunal Supremo, no se ha discutido el asunto sobre la autenticación y admisibilidad de evidencia electrónica y en el Tribunal de Apelaciones muy pocas veces.

Ahora bien, existen delitos relacionados con la evidencia digital que fueron creados hace más de catorce años,[3] y las normas probatorias se aprobaron durante

---

2 Vivian Neptune Rivera, La Evidencia Electrónica: Autenticación y Admisibilidad (2017).

3 *Véase* Código Penal del Estado Libre Asociado de Puerto Rico, Ley Núm. 149 de 18 de junio de 2004, 33 LPRA §§ 4785-4787 (2010) (derogado 2012) (artículos 157-159 que prohibieron la producción, posesión, distribución, utilización y exhibición de material electrónico de pornografía infantil); Código Penal del Estado Libre Asociado de Puerto Rico, Ley Núm. 149 de 18 de junio de 2004, 33 LPRA § 4839

el año 2009.[4] ¿Por qué la falta de interpretación jurisprudencial? Al revisar las decisiones del Tribunal Supremo de Puerto Rico durante el año 2017 encontré tres casos en los que se utilizó un mensaje a través de las redes sociales como un elemento vital para la adjudicación del caso. Dos de estos casos se refieren a acciones disciplinarias contra jueces. Veamos. En el caso de *In re Mercado Santaella* se imputa al juez publicar en su página de Facebook comentarios alusivos a la política partidista en clara crítica a un partido y comentarios de alto contenido sexual.[5] El Tribunal Supremo resolvió que el contenido de la información escrita por el juez por Facebook constituyó una violación a los cánones de ética judicial.

El segundo caso lo fue *In re Colón Colón*.[6] En este caso se imputa a un juez publicar en las redes sociales información contenida en documentos judiciales y, además, hacer comentarios irrespetuosos y despectivos en perjuicio de ciudadanos que acudieron al tribunal en búsqueda de un auxilio judicial.

En estos dos casos, lamentablemente se omitió toda discusión sobre la autenticación y admisibilidad de los mensajes en controversia.

Un tercer caso examina el privilegio del negocio. Me refiero al caso *Ponce Advance Medical Group Network, Inc. v. Santiago González y otros*[7], en este caso un médico publicó en su página de Facebook, que identificaba con el título *Medicina Defectuosa*, unas expresiones alusivas a un grupo médico y critica como el grupo médico contrataba sus servicios profesionales. El grupo médico lo demandó en daños y perjuicios por los comentarios publicados en Facebook y reclamó un interdicto contra lo publicado en la red social. En el descubrimiento de prueba el médico demandado requirió copia de varios contratos del grupo médico. La opinión del Tribunal Supremo adjudica el asunto relacionado con el descubrimiento de prueba pero omite toda discusión sobre la autenticación y admisibilidad del mensaje publicado en Facebook.

Cuesta trabajo entender el diferendo. En la litigación ante el Tribunal de Primera Instancia continuamente se presentan mensajes de datos enviados o recibidos a través de medios digitales. En el Tribunal de Primera Instancia continuamente se solicitan órdenes de protección al amparo de la ley de violencia domestica a base de mensajes de texto o correos electrónicos. En las salas de familia se utilizan mensajes de texto, fotos de Instagram[8] o correos electrónicos para sostener o refutar alegaciones en casos de alimentos o custodia. En el ámbito penal,

---

(2010) (derogado 2012) (art. 211, Fraude por medio informático); Código Penal del Estado Libre Asociado de Puerto Rico, Ley Núm. 149 de 18 de junio de 2004, 33 LPRA § 4844 (2010) (derogado 2012) (art. 216, Apropiación Ilegal de Identidad).

4 LUIS RIVERA ROMÁN *ET AL.*, INFORME DE LAS REGLAS DE DERECHO PROBATORIO 620-73 (2007) (en las nuevas Reglas de Evidencia de 2009 se incorporaron disposiciones con el propósito expreso de facilitar la autenticación y admisibilidad de evidencia electrónica).

5 *In re* Mercado Santaella, 197 DPR 1032 (2017).

6 *In re* Hon. Colón Colón, 197 DPR 728 (2017).

7 Ponce Adv. Med. v. Santiago González, 197 DPR 891 (2017).

8 Para una descripción sobre cómo funciona la plataforma de intercambio de fotos Instagram, véase Jamie Harris, *What is Instagram? How to get the Best from the photo sharing app*, BRITISH

generalmente los casos de pornografía infantil incluyen la presentación de mensajes de texto o fotografías enviadas por equipos electrónicos. En fin, los jueces de primera instancia con frecuencia deciden sobre la autenticación y admisibilidad de evidencia electrónica. Sin embargo, en los foros apelativos se encuentran muy pocas expresiones relacionadas con la autenticación y admisibilidad de evidencia electrónica.

La falta de decisiones de los foros apelativos que guíen a la profesión legal en torno al asunto crítico de la autenticación y admisibilidad de evidencia electrónica tiene que ser atendida.[9] El libro *La Evidencia Electrónica* nos llega en buen momento pues provee al abogado litigante argumentos y razonamientos para lograr la autenticación y admisibilidad de piezas de evidencia electrónica. Al juez de Instancia le brinda el fundamento en derecho adecuado para admitir o no admitir la evidencia electrónica. Al Tribunal Apelativo, le brinda los fundamentos para atender señalamientos de error relacionados con el efecto del error en la admisibilidad o exclusión de evidencia electrónica.[10]

II. EL TEMOR A LA MANIPULACIÓN DE DATOS

El mundo cambiante de la tecnología nos enfrenta a la realidad actual del uso constante de las redes sociales y los equipos electrónicos como medios de comunicación en el ámbito del gobierno, el mundo comercial, las universidades y todo tipo de empresa público o privada. El reto para los abogados es cómo posibilitar y permitir el acceso a los tribunales de todo un amplio mundo de comunicaciones digitales que pueden ser manejadas por un sinnúmero de usuarios, emisores y receptores.

El temor por la manipulación de datos o la alteración de archivos digitales se ha convertido en un obstáculo para la aceptación de la evidencia electrónica en los tribunales. La información en formato digital puede ser moldeada; por supuesto que sí. Basta pensar en los llamados *memes*[11] y la enorme capacidad de nuestro País para generar humor y crítica social plasmada en los *memes* que permiten a las personas o figuras que nunca han estado juntos colocarse en una composición gráfica que parece real. Qué bueno que existen esos medios digitales de comunicación porque, por ejemplo, a medida que íbamos recuperando las comunicaciones y dejando a un lado toda la tragedia provocada por el huracán María se desarrolló un gran volumen de arte creativo por parte del pueblo puertorriqueño haciendo sátira, humor y crítica social sobre nuestra realidad. Cómo olvidar el

---

TELECOMMUNICATIONS (19 de abril de 2018), http://home.bt.com/tech-gadgets/internet/social-media/what-is-instagram-and-how-does-it-work-11364009107701.

9 En la jurisdicción federal el asunto de la autenticación y admisibilidad de la prueba electrónica fue discutido ampliamente en un caso que marcó la pauta a los tribunales y abogados postulantes, Lorraine v. Markel American Ins. Co., 241 F.R.D. 534 (D. Md. 2007).

10 R. EVID. 104-106, 32 LPRA Ap. VI (2010).

11 Al utilizar el término *meme* nos referimos a un texto, imagen, video u otro elemento que se difunde rápidamente por Internet y que a menudo se modifica con fines humorísticos.

meme de los Reyes Magos: uno de ellos con una bolsita de hielo, otro con unas baterías y otro con una planta de emergencia.

Así, el mundo digital enfrenta el peligro de la manipulación y alteración de la información. Ello, sin embargo, no puede impedir el acceso a los tribunales de la información contenida en ese medio. Por supuesto que no queremos dar acceso a los tribunales a prueba alterada o manipulada. He aquí la gran importancia y aportación del libro *La Evidencia Electrónica*. La autora describe en el libro las garantías y salvaguardas que las Reglas de Evidencia proveen para que toda prueba presentada en el tribunal sea auténtica y admisible, y de esta forma proteger la veracidad de los hechos.

Precisamente, las normas de autenticación y admisibilidad de evidencia electrónica descritas y explicadas claramente por la autora del libro son el vehículo apropiado para garantizar que la prueba a presentarse en el proceso judicial sea confiable, creíble y de calidad. La autora nos previene del riesgo de que los sistemas tecnológicos sean utilizados para alterar o manipular información digital. También nos recuerda que, por su propia naturaleza cuando se altera o manipula un archivo digital, esto dejará un rastro en el equipo que permitirá identificar, denunciar y descartar a los actores. En el lenguaje del Derecho Probatorio, esto significa cumplir con las normas de autenticación y admisibilidad de evidencia.[12]

III. El contenido del libro

La autora identifica los principales medios de autenticación disponibles para los mensajes en redes sociales y los equipos electrónicos. Además, nos aporta una explicación clara y sencilla sobre las formas correctas de autenticar y lograr la admisibilidad de la evidencia electrónica en los procesos judiciales, que será de gran utilidad para los abogados. En cada caso enumera los requisitos dispuestos en nuestras Reglas de Evidencia y cita abundante jurisprudencia federal sobre el tema.

Merece especial mención el empeño de la autora de ilustrar mediante el uso de ejemplos prácticos el interrogatorio que debe hacer el abogado para la autenticación y admisibilidad de evidencia electrónica. De hecho, se detallan ejemplos de las preguntas que deben formularse a un testigo para autenticar un correo electrónico, mensaje de texto, *GPS*, "drones", foto de pantalla (*screenshot*), entre otras.[13] La inclusión de ejercicios prácticos y preguntas modelos ayudará al abogado practicante a organizar y formular las preguntas necesarias para autenticar la evidencia electrónica a presentarse en el proceso judicial.

Conviene mencionar varios de los medios de autenticación discutidos en el libro. En la Reglas de Evidencia se identifican separadamente cada uno de los me-

---

12 Neptune Rivera, *supra* nota 2, en las págs. 15-28.

13 *Id.* en las págs. 52-63, 84-98, 128-137, 151-155.

dios de autenticación conforme se describen en la Regla 901 de Evidencia. Sin embargo, la autora aclara que en el proceso judicial con frecuencia se utilizan a la misma vez varios medios de autenticación.[14]

IV. Las características distintivas y el conocimiento personal

Examinemos algunos ejemplos de autenticación. Las empresas comerciales se esmeran y dedican recursos económicos para presentar una página de Internet con unas características propias que los distinga de su competencia y de otros medios. En el ámbito de una oficina de trabajo podemos ilustrar como una secretaria puede autenticar e identificar un documento con su observación y de esta forma confirmar si ella lo preparó. El uso de ciertos márgenes, el tamaño de la letra, el estilo de letra, el uso de ennegrecer palabras o el uso itálicas para enfatizar palabras, entre otras. Todo esto permitiría a una secretaria autenticar un documento por características distintivas que ella puede reconocer con certeza. La persona que escribe el correo electrónico o el mensaje de texto tiene conocimiento personal para autenticar el mensaje de dato.

Con frecuencia se presenta en los tribunales mensajes de texto y correos electrónicos que incluyen tanto el mensaje recibido como la contestación. Esto equivale a una conversación.[15] En tal caso la pantalla ilustra quien originó el mensaje, cuando lo envío, a quién se lo envío, el contenido del mensaje y la respuesta recibida. En estos casos, la autenticación se hace por el intercambio de mensajes que demuestra que el documento es lo que se afirma que es. Con frecuencia, los mensajes se refieren a historias solo conocidas por los participantes en el intercambio. Estos pueden incluir palabras utilizadas por las partes para identificarse por acuerdo entre ellos o claves o expresiones acordadas por los participantes. Todo ello facilitará la autenticación del mensaje siempre que declare en el tribunal alguien que puede explicar el contenido de la comunicación.

V. Foto de pantalla (*screenshot*)

Con frecuencia una persona enfrenta el dilema de decidir qué hacer con lo que recibe y lee en la pantalla de la computadora o del celular.[16] Podría tomar una foto de la pantalla inmediatamente, imprimir o podría darle *forward* para proteger la integridad del mensaje recibido. Este asunto tiene múltiples dimensiones que la autora discute en distintos capítulos de su libro.[17]

Tenemos disponible diversos medios para demostrar la existencia de la página digital. Una parte puede imprimir lo que aparece en la pantalla. En otro caso una persona puede testificar pero además utilizar la foto o impresión de lo que decía

---

14 *Id.* en las págs. 15-18, 108-111.

15 *Id.* en la pág. 41.

16 *Id.* en la pág. 83.

17 *Id.* en las págs. 69-80, 82-88.

la página de Internet para corroborar su propio testimonio. En este caso el testimonio directo se corrobora con la evidencia ilustrativa de la página de Internet.

Una foto de pantalla sobre el contenido de un correo electrónico en ocasiones puede ser suficiente para presentarse en el tribunal como medio de corroboración de lo que un testigo ha declarado. El conocimiento personal del testigo será un medio suficiente para autenticar el mensaje. La decisión en torno a la prueba necesaria para la autenticación del correo o mensaje se debe tomar caso a caso.

En cada caso, el abogado deberá determinar si además de la foto de la pantalla necesita acceso al equipo electrónico para obtener y evaluar la otra información que surge del dispositivo electrónico donde se almacenó el archivo digital. La foto de pantalla nos permite conocer a quién se envía el correo electrónico, a quién lo dirige, la fecha, el asunto y el contenido del mensaje.

Sin embargo, el acceso al equipo electrónico permitirá conocer el rastro dejado en la máquina en que se originó el mensaje. Podremos conocer cuántos cambios, modificaciones o alteraciones ha sufrido el correo, en que equipo electrónico se originó y la fecha y el tracto que nos señala cada una de las fechas en que se modificó el mensaje.[18]

El abogado, debe plantearse el uso que dará al correo electrónico y mensaje de texto para determinar si necesita conocer todo el historial o el rastro del manejo del mensaje. La foto de pantalla (*screenshot*) en algunos casos tiene gran utilidad, pero tiene también grandes limitaciones.[19] El abogado deberá determinar, caso a caso, qué información necesita para luego preguntarse dónde la puede encontrar. ¿Será suficiente la foto de la pantalla? ¿Necesitará acceso a la computadora? El asunto tiene una dimensión ética puesto que el deber de competencia y diligencia contemplado en el Canon 18 de Ética Profesional se cumplirá en la medida en que el abogado realice el juicio correcto y presente o defienda el caso con la información necesaria y suficiente.[20]

Examinemos otro ejemplo de gran importancia mencionado por la autora. En un caso de pornografía infantil, lo que constituye el delito es el archivo del original de la foto pornográfica, por lo tanto, si el imputado envía por mensaje de texto una foto a otra persona, y ésta persona le toma un "screenshot" o foto a la pantalla y la muestra a la policía, cuando testifica podrá hablar sobre su conocimiento personal del intercambio de comunicaciones con el imputado.[21] Ahora bien, el delito de pornografía infantil requiere probar sustantivamente la existencia de la foto

---

18 *Id.* en las págs. 34-36.

19 Pensemos por un momento la investigación tradicional de un delito. Una foto del arma utilizada para cometer el delito permite mostrar la forma del arma de fuego, el modelo y el tamaño del arma. Sin embargo, si el investigador tiene físicamente el arma de fuego, podrá examinar las huellas dactilares. El perito en balística podrá examinar el martillo del arma para comparar si la bala encontrada en el cuerpo de la víctima es compatible con la bala que dispara el arma fuego o si el arma ha sido alterada para convertirla en automática. En el contexto de la evidencia electrónica la situación es más dramática. El acceso a un archivo digital permitirá más información que la que puede brindar una foto de pantalla (*screenshot*).

20 CÓD. ÉTIC. PROF. 18, 4 LPRA Ap. IX, § 18 (2013).

21 NEPTUNE RIVERA, *supra* nota 2, en las págs. 77-84.

original. La foto de pantalla no es suficiente. En estos casos se debe distinguir si el propósito es utilizar la foto como evidencia demostrativa o evidencia sustantiva, esto es, si aplicará la regla de la mejor evidencia.[22] El proponente deberá cumplir con el capítulo 9 o 10, respectivamente, de las Reglas de Evidencia dependiendo cual sea su propósito.[23]

El agente del orden público deberá obtener una orden de registro y allanamiento para ocupar el equipo electrónico donde se encuentra almacenada el original de la foto pornográfica. Luego se someterá a un perito que declare sobre el examen que realizó al equipo electrónico, en el cual localizó la fotografía pornográfica transferida al teléfono del testigo.

Detengámonos por un momento en este asunto de la orden de registro y allanamiento. En primer lugar, la persona que recibió la foto por teléfono puede declarar ante un juez para solicitar una orden de registro y allanamiento. Luego de emitida la orden, el agente del orden público podrá ocupar el dispositivo electrónico del cual se envió la fotografía en controversia. El agente llevará a cabo un cuidadoso proceso de ocupación del equipo y tomará las medidas técnicas necesarias para demostrar que protegió la integridad de la información digital y la cadena de custodia. Por lo tanto, el agente debe demostrar que lo presentado en el tribunal es lo mismo que lo que existía en el equipo electrónico al momento de su ocupación y que no fue alterada ni modificada mientras estuvo bajo su control. El agente podrá declarar en el tribunal sobre el contenido de la foto localizada en el equipo si garantiza previamente los requisitos de autenticidad tales como la cadena de custodia.[24]

Lo segundo que debemos tener presente es el potencial de acceso que brinda una orden de registro y allanamiento en un archivo digital. En el registro y allanamiento tradicional se permite al policía entrar a una propiedad y mientras realiza el diligenciamiento de la orden, si observa alguna otra actividad criminal, podrá incautarla. El acceso que tendrá el policía se limita al instante en que diligencia la orden. No obstante, cuando se logra una orden de registro y allanamiento para entrar al archivo digital de una computadora o equipo electrónico, tendrá acceso a mucha otra información archivada. Por lo cual, se crea un grave peligro y la orden debe ser limitada con la mayor claridad posible.

VI. La prueba de referencia

Para cerrar con broche de oro la autora incluye varias consideraciones que relacionan el concepto de la prueba de referencia, sus excepciones y la prueba electrónica.[25] En esta parte dedica varias páginas a la discusión del caso *Crawford*

---

22 *Véase* R. Evid. 1001, 32 LPRA Ap. VI (2010).

23 Neptune Rivera, *supra* nota 2, en las págs. 78-80.

24 *Id.* en las págs. 12-18, 112-15.

25 *Id.* en las págs. 157-181.

v. Washington[26] y nos describe como las declaraciones testimoniales se relacionan con la prueba electrónica.

Las dos excepciones a la prueba de referencia que se utilizan en los tribunales con más frecuencia son las admisiones y el récord de negocios (actividades que se realizan con regularidad). En cuanto a las admisiones tomemos el ejemplo de una situación que se repite diariamente en los tribunales. Imaginemos una mujer que recibe un mensaje de texto de su ex pareja en el que le dicen que si la encuentran con alguien la van a golpear. En ese caso ella se plantea como debe preservar el mensaje, si debe tomar una foto de pantalla (*screenshot*). Luego, para autenticar el mensaje utilizará su conocimiento personal y podrá identificar el teléfono desde el cual se le envió el mensaje, el número de teléfono que ella conoce le pertenece a su ex pareja, que ella ha recibido mensaje de esa persona utilizando el mismo teléfono durante los años que han compartido. Además, para darle contexto al mensaje, podrá declarar que cada vez que se separan él se enoja, le envía mensajes de texto con lenguaje similar ofensivos y amenazantes y utiliza frases como la que están incluidas en el mensaje. Puede declarar que cada vez que él se enoja utiliza palabras con los mismos errores y énfasis que tiene en el mensaje recién recibido. El conocimiento personal y las características distintivas descritas por la persona testigo serán suficientes para autenticar el mensaje.[27] Habiéndose autenticado el mensaje entonces las aseveraciones que constituyen amenaza a la víctima son una admisión al amparo de la Regla 803 de Evidencia.[28]

La autora nos adelanta un tema que cobra fuerza en los casos federales y que seguramente será objeto de mucha interpretación en los tribunales durante los próximos años.[29] Me refiero a la controversia de si el certificado de autenticación que emite una red social será suficiente para autenticar la identidad del propietario de la cuenta en la red social. El asunto fue discutido por la autora al comentar el caso *U.S. v. Browne*.[30]

Con frecuencia, el gobierno solicita a redes sociales como Facebook o Instagram un certificado de identidad que sirva para confirmar la identidad del dueño de una cuenta. Se intenta lograr que se admita en evidencia bajo la excepción a la prueba de referencia de récord de negocio. A este trámite se le conoce como certificado de autenticidad.

En el caso de *U.S. v. Browne*, se discute la certificación de identidad, esto es, la persona a cuyo nombre esté registrada la cuenta brindada por las redes sociales. Los hechos del caso establecieron que Browne conoció a una menor y le solicitó fotos sexualmente explícitas. Luego de recibir las fotos, Browne amenazó a la menor con divulgarlas en las redes sociales a menos que tuvieran sexo. Ese patrón se

---

26 Crawford v. Washington, 541 U.S. 36 (2004).

27 NEPTUNE RIVERA, *supra* nota 2, en las págs. 72-77.

28 R. EVID. 803, 32 LPRA Ap. VI (2010).

29 NEPTUNE RIVERA, *supra* nota 2, en las págs. 107-11.

30 U.S. v. Browne, 834 F. 3d 403 (3d. Cir. 2016).

repitió con otros menores de edad. Por extraño que parezca, ese esquema tan burdo también ha ocurrido en Puerto Rico.

El tribunal resolvió que los chats de Facebook no fueron correctamente autenticados utilizando el certificado de identidad presentado por Facebook. Sin embargo, la prueba extrínseca que desfiló en juicio incluía testimonio de los menores que describían los mensajes que intercambiaban con el acusado, la dirección electrónica a la que se enviaba, las respuestas que recibían del agresor, las conversaciones telefónicas ocurridas con el acusado y algunas admisiones del propio acusado fueron suficiente para autenticar debidamente la prueba y lograr su admisibilidad en juicio.

En un caso criminal no basta con establecer que hubo un intercambio de mensajes entre dos direcciones de correo electrónico. Además, se tiene que establecer que una de las direcciones electrónicas corresponde a la persona imputada, así que tiene que vincularse la persona imputada con la dirección electrónica. El caso ilustra además que comúnmente se combinan medios de autenticación para lograr la admisibilidad del elemento vital de la identidad del imputado.[31]

VII. EL ESTÁNDAR DE AUTENTICACIÓN Y VALOR PROBATORIO

Por supuesto, cabe aclarar que la parte contra la cual se presenta la evidencia electrónica tendrá siempre la oportunidad de demostrar que la prueba no es confiable o que ha sido alterada. El estándar para acreditar la autenticación de una prueba se evalúa bajo el crisol de la Regla 109 de evidencia (determinación preliminar de admisibilidad).[32]

Acreditada por una parte la autenticación y admisibilidad, entonces podrá la otra parte cuestionar la suficiencia de la prueba. El hecho de que un archivo digital o electrónico sea auténtico y sea admisible, ello no es suficiente para demostrar la veracidad del hecho. La parte contraria podrá cuestionar la veracidad y suficiencia de esa prueba.[33]

En fin, la aportación de la Decana Neptune con su libro *La Evidencia Electrónica* es extraordinaria. El valor académico del libro *La Evidencia Electrónica* se presenta en el uso de un lenguaje claro y sencillo, comprensible al neófito en la materia y, a la misma vez, comprensible al conocedor que desea tener disponible un medio sencillo para repasar conocimientos y para utilizarlo como una guía de trabajo en la preparación de un caso.

La autora incluye una descripción precisa de las formas de autenticar los mensajes de datos en las principales redes sociales y equipos electrónicos. En cada caso, identifica jurisprudencia federal y tratadistas que ayudan a entender el medio electrónico utilizado. La discusión presentada por la autora permite entender

---

31 *Véase id.*, en las págs. 408-17.

32 R. EVID. 109, 32 LPRA Ap. VI (2010).

33 NEPTUNE RIVERA, *supra* nota 2, en las págs. 27-28.

cada tema sin inmiscuirnos en detallados análisis teóricos que comprenderían solo expertos en la materia.

Conclusión

En el libro la autora nos confiesa el origen de su interés por el tema de la evidencia electrónica. Quienes la entrevistaron en el año 2006 para una plaza en el área de Derecho Probatorio tuvieron el propósito de reclutar a una persona que ayudara a la Facultad de Derecho de la UPR en el tema de la evidencia electrónica. Que honor compartir la enseñanza de la materia del Derecho Probatorio con la persona que más conoce sobre evidencia, que más ha escrito sobre el tema de evidencia y que comparte generosamente sus conocimientos con estudiantes y abogados. Me refiero al profesor Ernesto L. Chiesa Aponte. La tarea que le fue encomendada fue cumplida con excelencia.

La autora señala además que la designación al comité asesor que revisó las Reglas de Evidencia de Puerto Rico y el trabajo que tuvo a su cargo al presidir el subcomité que revisó el cuerpo de las reglas para procurar su modernización y el acceso de la evidencia electrónica a los procesos judiciales. Recuérdese que estábamos en los años 2007, 2008 y 2009. En aquel momento sabíamos que el mundo digital cambiaba rápidamente pero, ni siquiera entonces, podíamos anticipar la enorme transformación del mundo digital y toda la evolución que en las comunicaciones entre personas a través de la diversidad enorme de aplicaciones tendría cabida en nuestra realidad diaria. Con su trabajo en el subcomité, se logró incorporar al texto de la Reglas de Evidencia de Puerto Rico un lenguaje amplio y flexible, que al presente continúa siendo apropiado para posibilitar el uso de evidencia electrónica en los tribunales. También cumplió con excelencia esa encomienda.

Guiada por su vocación académica, la Decana publicó dos artículos de revista jurídica que han sido fuente de información y orientación para toda la profesión legal, a saber: *Los Retos de la Evidencia Electrónica* (2007);[34] y *Las Redes Sociales y los Mensajes de Texto* (2010).[35] El libro que hoy presentamos constituye un esfuerzo adicional de la Profesora Vivian Neptune Rivera para orientar e ilustrar a la profesión legal sobre las formas apropiadas para la autenticación y admisibilidad de la evidencia electrónica. Esa tarea también ha sido cumplida con excelencia.

Ahora bien, el problema de ser joven, de tener su inteligencia y capacidad de trabajo, de tener un compromiso serio con la academia, los estudiantes, la profesión legal y nuestra sociedad, es que no puede dar por concluido su trabajo sobre el tema de la evidencia electrónica. La academia le provee el ambiente adecuado para continuar educando en un tema de constante evolución como lo es la evidencia electrónica y el mundo digital.

Pensemos por un momento en controversias que se ciernen en el horizonte del Siglo XXI, como por ejemplo:

---

34 Vivian I. Neptune Rivera, *Los Retos de la Evidencia Electrónica*, 76 Rev. Jur. UPR 337 (2007).

35 Vivian I. Neptune Rivera, *Las Redes Sociales y los Mensajes de Texto: Autenticación bajo las nuevas Reglas de Evidencia de Puerto Rico*, 44 Rev. Jur. UIPR 285 (2010).

1. El carácter universal de acceso a la Internet versus las leyes que en cada país aprueban para reglamentar la Internet y que solo pueden aplicarse en su territorio.
2. ¿Cómo armonizar el balance entre el derecho a la intimidad y el derecho a la propia imagen de las personas versus el derecho al libre acceso a la información en Internet?
3. ¿Qué protección tendremos en cuanto a datos sobre nuestra persona almacenados en el mundo digital y utilizados sin nuestro permiso? ¿Cómo armonizar los derechos del internauta que navega libremente en la Internet, los buscadores de datos como Google y el derecho a la intimidad de las personas cuya información se almacena en el mundo digital? En la Unión Europea esto ha sido denominado como el *derecho al olvido.*[36]
4. ¿Quién decide lo que se almacena en la red sobre nuestra persona y por cuánto tiempo?
5. ¿Cómo evaluar el problema que enfrenta las personas con su privacidad? La privacidad vista en el ambiente de Internet se encuentra en constante movimiento y evolución. La Internet da acceso a la información en tiempo inmediato y a costos mínimos. Ello constituye una gran ventaja, pero también nos expone a grandes riesgos; pues cuando afecta la intimidad y la privacidad, esto ocurre rápidamente y se deposita en varios ordenadores a través del mundo en fracciones de segundo. Es difícil la protección de datos por lo rápido que discurre la información en la Internet.
6. ¿Cómo entender la magnitud y omnipresencia del rastro que dejamos en cada entrada a un archivo digital? Todo lo que hacemos en Internet deja un rastro. La red no olvida, sino que almacena y lo hace en distintos lugares de almacenamiento en fracciones de segundo. En la red el concepto de borrar no es borrar. Realmente la información se almacena en otro archivo.

Son estas algunas interrogantes que se ciernen en el horizonte del Siglo XXI que tienen el potencial de afectar la vida de los seres humanos.

No es momento de escribir el capítulo final. Más bien partiendo del vasto conocimiento que la Decana Neptune tiene sobre el tema de la evidencia electrónica, lo cual queda plenamente demostrado con el libro que hoy presentamos, ella está en las condiciones ideales para enfrentar los nuevos retos.

Mis sinceras felicitaciones por un libro bien logrado, que representa una aportación extraordinaria a nuestro Derecho Probatorio y a nuestra comunidad legal.

Enhorabuena.

---

36 Caso C131/12, Google Spain SL y Google Inc. v. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, 2014 (en el cual se resolvió mediante un balance de intereses entre los derechos de la persona que solicita que retiren la información de la Internet, Google (buscador de datos) y el internauta común que utiliza la Internet).