

Unclassified

Spanish - Or. English

21 September 2020

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

LATIN AMERICAN AND CARIBBEAN COMPETITION FORUM (Spanish version) FORO LATINOAMERICANO Y DEL CARIBE DE COMPETENCIA - Sesión I: Obtención de pruebas en formato digital en cárteles

- Contribución de los Estados Unidos -

28 y 29 de septiembre de 2020, reunión virtual por Zoom

Se hace circular el documento adjunto elaborado por los Estados Unidos PARA SU DEBATE en la Sesión I del Foro Latinoamericano y Del Caribe de Competencia que se llevará a cabo los días 28-29 de septiembre 2020 reunión virtual por Zoom.

Sra. Lynn Robertson, Gerente MENA/Africa, LACCF ; Experto en Competencia - Lynn.Robertson@oecd.org.

JT03465569

Sesión 1: Obtención de pruebas en formato digital en cárteles

Desafíos jurídicos y prácticos asociados a la recopilación de pruebas en formato digital

- Contribución de los Estados Unidos -

1. La digitalización de la economía mundial ha supuesto un desafío para las autoridades de competencia de todo el mundo a la hora de modernizar el modo en que se investigan los cárteles y adaptarse a las nuevas formas que tienen las empresas de utilizar la tecnología para su actividad. Además, la digitalización ha revolucionado la manera en la que las personas se comunican entre sí y ha planteado cuestiones importantes relativas a la privacidad y las libertades individuales de los objetivos de una investigación de cárteles. En esta presentación, se describirán algunas de las consideraciones jurídicas y prácticas de la División Antimonopolio del Departamento de Justicia de los Estados Unidos (en adelante, la «División») con respecto a la recopilación de pruebas digitales en investigaciones de cárteles. En el primer apartado, se analiza el marco jurídico para la obtención de pruebas de empresas que prestan servicios de comunicaciones electrónicas. En el siguiente apartado, se describe el trabajo llevado a cabo por el equipo especializado en apoyo a la litigación de la División. El último apartado concluye con un debate acerca del marco jurídico para la realización de incautaciones de pruebas y los desafíos prácticos a la hora de incautar pruebas en formato digital.

1. Obtención de pruebas en formato digital de terceros proveedores de comunicaciones electrónicas

2. Los miembros de los cárteles se han adaptado al mundo digital. Las conversaciones de los conspiradores que se mantenían en «cuartos traseros llenos de humo» se han trasladado al correo electrónico y otros medios de ese tipo, incluidas las aplicaciones de mensajería cifrada. En muchos casos, los miembros de los cárteles, conscientes de la ilegalidad de su actividad, han cambiado sus cuentas de correo electrónico de la empresa por servicios de mensajería y correo electrónico personales prestados por terceros, como Gmail, de Google, o Facebook Messenger, para comunicarse con sus cómplices. Dado que los conspiradores se han vuelto más hábiles en cuanto a la forma que tienen de comunicarse entre ellos, la División ha adaptado sus técnicas de investigación y, actualmente, con frecuencia trata de obtener pruebas en formato digital de terceras empresas de comunicaciones durante el transcurso de la investigación de un cártel.

3. En los Estados Unidos, el título II de la Ley de privacidad de las comunicaciones electrónicas (en adelante, «ECPA», por las siglas en inglés) regula cómo y cuándo los organismos estadounidenses encargados de hacer cumplir la ley, entre ellos, la División, pueden obtener acceso a comunicaciones digitales almacenadas, como registros telefónicos o de correo electrónico, durante el transcurso de una investigación penal.¹ El objetivo de la

¹ Véase el título 18 del Código de los Estados Unidos, secciones 2701 a 2713.

ECPA consiste en ofrecer a los organismos estadounidenses encargados de hacer cumplir la ley herramientas para el enjuiciamiento eficaz de delitos y, además, ofrece privacidad a las personas y garantiza la protección frente a búsquedas e incautaciones no justificadas, un concepto recogido en la cuarta ^{enmienda de} la Constitución de los Estados Unidos. La ley se aplica a los proveedores de servicios de comunicaciones electrónicas o de servicios informáticos remotos que prestan dichos servicios al público en general. Entre ellos se incluyen proveedores de mensajería y correo electrónico basados en la web y en aplicaciones, empresas de medios sociales y empresas que prestan servicios de tratamiento o almacenamiento informáticos, como los servicios en la nube, el alojamiento web o el almacenamiento de fotos en línea.

4. La ECPA posee ciertas características fundamentales que son importantes para la realización de investigaciones penales de cárteles, que son las siguientes:

- La ECPA hace una distinción entre el «contenido» de una comunicación y otros registros o informaciones que no incluyen contenido.
- La ECPA exige a las empresas preservar los datos si así lo solicita un organismo estadounidense encargado de hacer cumplir la ley.
- La ECPA permite que los organismos estadounidenses encargados de hacer cumplir la ley obtengan una orden judicial en la que se le exija a una empresa que no revele al cliente la recepción de una orden, una citación o una orden de registro durante un determinado período de tiempo.
- Una enmienda reciente de la ECPA, la Ley de aclaración del uso legítimo de los datos en el extranjero (CLOUD, por las siglas en inglés), exige a los proveedores que presten servicios en los EE. UU. que aporten pruebas independientemente de si la empresa las almacena en ese país.

5. *Datos con contenido frente a datos sin contenido.* Una de las características principales de esta ley es la distinción entre el «contenido» de las comunicaciones y otros registros o informaciones relativos a la cuenta, como los datos de identificación del cliente y los registros de las operaciones que no se consideran «contenido». La información definida como «contenido» está sujeta a un mayor nivel de protección de la privacidad. En la mayoría de los casos, los fiscales obtendrán una orden de registro para la información con «contenido», lo cual requiere una aprobación judicial y una exposición de la causa probable de que el contenido de una comunicación incluya pruebas de un delito. Dentro del «contenido» se incluyen, por ejemplo, el cuerpo de un mensaje de correo electrónico o el texto de un SMS de un teléfono.

6. En cambio, la información que no se considera contenido de una comunicación no conlleva el mismo nivel de protección. Por ejemplo, la información sobre un cliente y su cuenta, como su nombre, su dirección y sus datos de pago, no requiere la misma exposición de pruebas que se exigiría para obtener el contenido de sus correos electrónicos.

7. La información sin contenido, como la información y los registros de las operaciones de un abonado, puede resultar especialmente útil en los casos relativos a cárteles para establecer contactos entre sus miembros, aunque se desconozca el contenido de la comunicación. Por ejemplo, es posible que los encabezados de los mensajes de correo electrónico no revelen el tema sobre el que hablan los objetivos, pero mostrarán si los presuntos miembros de un cártel se estuvieron comunicando entre ellos y cuándo lo hicieron. Los registros de actividad que indiquen en qué momento los presuntos miembros de un cártel han accedido a sus cuentas y han presentado ofertas podrían indicar que esas personas trabajaron juntas de manera coordinada.

8. *Preservación de los datos.* Los proveedores de comunicaciones deben preservar los registros si así lo solicita un organismo estadounidense encargado de hacer cumplir la ley, inicialmente durante un período de 90 días, el cual se puede renovar una vez.² Esto resulta útil en los casos en los que las personas que son objeto de una investigación borran mensajes de sus teléfonos o sus cuentas de correo electrónico; los mensajes se pueden obtener directamente del proveedor mediante una orden de registro o cualquier otro proceso pertinente contemplado en la ECPA.

9. *Confidencialidad.* Cabe señalar que la División puede obtener una orden judicial que impida al proveedor revelar a su cliente que la empresa ha recibido una orden de registro, una orden judicial o una citación para obtener información relacionada con su cuenta.³ A la hora de evaluar una solicitud de una orden de no divulgación, el tribunal determina si la divulgación causará la destrucción de pruebas, pondrá en grave peligro la investigación o retrasará de manera excesiva un juicio, entre otras cosas.⁴ Esta orden de no divulgación puede durar un período de tiempo determinado que el tribunal considere «conveniente».⁵ Según la política actual del Departamento de Justicia, los fiscales solo podrán solicitar órdenes que duren, como máximo, un año.⁶

10. *Ubicación de las pruebas.* En 2018, el Congreso estadounidense promulgó la Ley de aclaración del uso legítimo de los datos en el extranjero (en adelante, «Ley CLOUD»), la cual modificó la ECPA para aclarar que una empresa sujeta a la jurisdicción de los EE. UU. debe aportar los datos que estén bajo su control, independientemente de si los datos se almacenan en territorio estadounidense.⁷ Esta legislación fue, en parte, el resultado de un caso en el que Microsoft se negó a cumplir una orden de registro porque los datos estaban almacenados en un servidor en el extranjero. En 2013, Microsoft impugnó una orden de registro emitida en virtud de la ECPA por un juez de los EE. UU.⁸ En la orden de registro se exigía información sobre la cuenta y correos electrónicos de una persona investigada con relación al tráfico de drogas. A pesar de ser una empresa con sede en EE. UU., Microsoft sostenía que los correos electrónicos estaban almacenados en un servidor de Irlanda y, por tanto, no estaban sujetos a la jurisdicción de los tribunales estadounidenses. Finalmente, se presentó un recurso de apelación frente a la impugnación ante el Tribunal Supremo, pero el caso se anuló cuando el Congreso aprobó la Ley CLOUD.⁹ En consecuencia, actualmente está claro que todos los proveedores de comunicaciones electrónicas sujetos a la ECPA deben aportar las pruebas que estén «en su posesión o bajo su custodia o control» independientemente de si los datos se encuentran almacenados en los EE. UU. o en otro país extranjero.

² Véase *id.*, sección 2703f.

³ Véase *id.*, sección 2705b.

⁴ *Id.* (en la disposición se incluye una lista de cinco factores).

⁵ *Id.*

⁶ Departamento de Justicia de los EE. UU., Manual de Justicia, sección 9-13.700, <https://www.justice.gov/jm/jm-9-13000-obtaining-evidence#9-13.700>.

⁷ Véase el título 18 del Código de los Estados Unidos, sección 2713.

⁸ *In re Warrant To Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 15 F.Supp.3d 466 (S.D.N.Y. 2014); Véase también *In re Warrant To Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 829 F.3d 197, 204–205 (2d Cir. 2016).

⁹ *United States v. Microsoft Corp.*, 584 U.S. ___, 138 S. Ct. 1186 (2018).

11. *Desafíos prácticos.* La obtención de pruebas en formato digital en virtud de la ECPA puede ofrecer pruebas irrefutables y directas de la conspiración de un cártel, así como pruebas circunstanciales que demuestren que los conspiradores participaron en acciones que se ajustan a un acuerdo o en esfuerzos encaminados a ocultar la conducta, lo que indica conciencia de culpa. Como ocurre en cualquier situación, el uso eficaz de este tipo de pruebas implica desafíos prácticos. Es posible que resulte complicado y costoso tratar y revisar el volumen total de material aportado. La División también tiene que hacer frente a nuevos tipos de formatos de documentos, como los servicios basados en imágenes, que permiten a los usuarios comunicarse a través del intercambio de fotografías, *gifs*, emojis, stickers y similares. El tratamiento de estos materiales digitales y su empaquetado en un formato revisable para el personal del organismo supone un nuevo desafío para las autoridades de competencia. A continuación, se ofrece más información acerca del enfoque adoptado por el Departamento de Justicia con respecto a la gestión de los desafíos prácticos de las pruebas en formato digital.

2. Gestión de las pruebas en formato digital

12. La División cuenta con un equipo especializado en apoyo a la litigación que facilita la recopilación, el tratamiento y la revisión de pruebas en formato digital en todos los casos de la División, incluidos los casos penales de cárteles. Nuestro equipo de apoyo a la litigación está formado por profesionales con formación y experiencia en los ámbitos de la tecnología de la información (TI), la gestión de casos jurídicos y la gestión de proyectos, con un énfasis especial en la experiencia con la litigación, la exhibición de documentos electrónicos (*eDiscovery*) y las herramientas forenses.

13. Según la experiencia de la División, la comunicación y la coordinación entre los equipos de investigación y el personal informático de la División es fundamental para garantizar una recepción y un tratamiento eficaces de las pruebas en formato digital. El personal debe estar cualificado para emplear de forma eficaz las herramientas tecnológicas destinadas a revisar esas pruebas. Cada investigación de la División se asigna a un gestor de casos del equipo de apoyo a la litigación que forma parte del equipo de investigación desde el inicio del caso hasta su resolución, incluido el juicio. El gestor de casos está disponible para ofrecer orientación sobre una serie de temas relacionados con la aportación de pruebas en formato digital y ayuda a gestionar el tratamiento de estas para su revisión, incluidas tanto las pruebas incautadas como las aportadas en respuesta a una citación o una solicitud voluntaria.

14. El equipo de apoyo a la litigación de la División incluye además personal con conocimientos técnicos especializados que realiza consultas a los equipos de investigación de la División sobre diferentes temas, como el uso de plataformas de revisión de bases de datos, la creación de imágenes y la codificación de documentos, la aportación de adquisiciones forenses y el *software* de presentación de juicios.

15. Otra función importante del equipo de apoyo a la litigación es asesorar con respecto al desarrollo y la aplicación de protocolos para que los equipos de investigación los sigan a la hora de aportar, tratar y revisar las pruebas. Además, el equipo de apoyo a la litigación ofrece formación al personal jurídico y económico sobre cómo utilizar las distintas herramientas tecnológicas que emplea la División, incluidas las plataformas de revisión de bases de datos.

16. Además del equipo de apoyo a la litigación, el abogado principal de exhibición de documentos electrónicos de la División actúa como enlace entre este equipo y nuestro personal jurídico y económico, y dirige el desarrollo y la aplicación de las mejores prácticas y la orientación sobre temas que van desde el uso de términos de búsqueda a la preservación de documentos y la negociación de la aportación de pruebas en formato digital. Además, nuestro abogado principal de exhibición de documentos electrónicos dirige un grupo de trabajo sobre exhibición de documentos electrónicos, formado por personal perteneciente a la División. Para abordar específicamente los crecientes desafíos que suponen los casos de cárteles, la División contrató hace poco a una abogada procesalista especializada que se centra en la exhibición de documentos electrónicos en los casos penales de cárteles. Se le asignan algunos de los casos más complejos de la División y ella aporta conocimientos especializados y orientación sobre temas relacionados con las pruebas en formato digital a lo largo de una investigación.

3. Incautación de pruebas en formato digital – Obtención de pruebas directamente de los sujetos

3.1. Aspectos jurídicos y prácticos

17. *Proceso jurídico para las incautaciones.* Una de las herramientas que utilizan frecuentemente las autoridades de competencia para la detección y el enjuiciamiento de cárteles intrínsecamente nocivos es la inspección no anunciada o «sorpresiva», que se realiza tanto en empresas como en locales privados. En los Estados Unidos, la versión que tiene la División de una «inspección sorpresiva» es la ejecución de un registro tras obtener una orden de registro. En virtud del derecho estadounidense, la cuarta enmienda de la Constitución de los Estados Unidos protege a las personas de los registros y las incautaciones no justificadas, y establece los requisitos básicos de las órdenes de registro emitidas para la realización de registros e incautaciones. La norma 41 de las Normas federales de enjuiciamiento criminal explica además el proceso de obtención y ejecución de una orden de registro.¹⁰ La realización de una inspección no anunciada en un caso penal antimonopolio se lleva a cabo de acuerdo con una orden de registro conforme a la norma 41, emitida por un funcionario judicial neutral, normalmente un juez federal, una vez que se demuestre que existe una causa probable para creer que se ha cometido un delito y que es probable que la prueba de este se encuentre en una determinada ubicación indicada en la orden de registro.¹¹

18. Para obtener una orden de registro, un funcionario encargado de hacer cumplir la ley de EE. UU. debe facilitar una declaración jurada en la que se aleguen los hechos que demuestren la causa probable y se especifique la ubicación que se debe investigar y los bienes que se deben incautar. En el caso de los fiscales de la División, es importante garantizar que los registros y las incautaciones se realicen de acuerdo con la legislación y la protección procesal conferida por la cuarta enmienda para evitar la posible eliminación de la prueba en el futuro por parte del tribunal durante un juicio. La División trabaja en

¹⁰ Cuarta enmienda de la Constitución de los Estados Unidos; norma 41 de las Normas federales de enjuiciamiento criminal. Existen varias excepciones muy limitadas al requisito necesario para la emisión de una orden de registro, entre las que se incluye el consentimiento, un registro realizado con motivo de un arresto preventivo y la doctrina *plain view* (según la cual podrá incorporarse todo material que se haya encontrado a simple vista).

¹¹ Véase *id.*

estrecha colaboración con nuestros socios encargados de hacer cumplir la ley a nivel federal tanto en la preparación de las órdenes de registro como en la planificación de su ejecución.

19. Los registros realizados conforme a una orden constituyen una herramienta de investigación fundamental que emplea la División. Los registros generan un mayor miedo a ser descubiertos que desestabiliza a los cárteles e incentiva las declaraciones voluntarias.¹² Asimismo, en el Manual de la División se aborda la importancia de los registros en la obtención de pruebas de los cárteles intrínsecamente nocivos y se resalta que el uso de los registros «reduce al mínimo la oportunidad de destruir y ocultar documentos, impide que no se aporten documentos de respuesta, ya sea de forma deliberada o por inadvertencia, y a menudo estimula la búsqueda de clemencia».¹³

20. Normalmente, la realización de un registro de un local privado o de una empresa implica la incautación de pruebas en formato digital que se pueden almacenar en un dispositivo o en un servidor. Los ordenadores, servidores y teléfonos inteligentes de las empresas pueden contener pruebas de la existencia de un cártel, pero, además, pueden contener otros documentos e informaciones que no estén relacionados con nuestra investigación. Por lo general, no es factible hacer una revisión archivo por archivo de las pruebas en formato electrónico para determinar qué documentos son realmente pertinentes durante la operación de registro *in situ*. En los casos en los que esa revisión no resulte factible, en el apartado e) 2) B) de la norma 41 se establece un proceso compuesto por dos fases para la incautación de pruebas en formato digital. Los medios digitales se incautan o se copian *in situ* durante la ejecución del registro de la orden y, a continuación, se revisan para determinar qué contenidos se encuentran dentro del alcance de la orden.¹⁴

21. *Secreto profesional e incautación de pruebas.* Uno de los aspectos jurídicos fundamentales en la incautación de pruebas en formato digital en una investigación de cárteles es la protección de la confidencialidad entre los abogados y sus clientes. La incautación de pruebas empresariales en un caso relacionado con cárteles puede implicar la incautación de comunicaciones en formato digital tanto con abogados internos como externos, y es posible que algunas de estas comunicaciones sean confidenciales. La confidencialidad entre los abogados y sus clientes es un antiguo privilegio reconocido en el derecho estadounidense que protege las comunicaciones entre un abogado y su cliente. Puede hacerse valer en respuesta a las exigencias jurídicas de exhibición de pruebas y otras divulgaciones obligatorias, como el testimonio. Se utiliza tanto en asuntos civiles como penales y se puede aplicar tanto a particulares como a empresas e incluso clientes gubernamentales.

22. Al igual que ocurre con muchas doctrinas del derecho anglosajón, la confidencialidad entre el abogado y su cliente cuenta con algunos elementos esenciales. La persona que haga valer la confidencialidad debe ser un cliente, y la comunicación debe establecerse con un abogado habilitado. La definición de abogado es amplia e incluye a los abogados internos, los abogados del Estado, los abogados privados y aquellas personas a las que estos contratan para ayudarlos (expertos, asistentes jurídicos y personal de apoyo). No obstante, no todas las comunicaciones establecidas con un abogado son confidenciales. La comunicación debe estar relacionada con el asesoramiento jurídico; si un abogado de empresa está aportando asesoramiento de tipo comercial a su empresa, esta comunicación

¹² Véase, p. ej., Departamento de Justicia de los EE. UU., Richard A. Powers, asistente adjunto del fiscal general, *Matter of Trust: Enduring Leniency Lessons for the Future of Cartel Enforcement* (San Francisco, California, 19 de febrero de 2020), <https://www.justice.gov/atr/page/file/1250346/download>.

¹³ Véase Departamento de Justicia de los EE. UU., Manual de la División Antimonopolio, pág. III-90.

¹⁴ Véase apartado e) 2) b) de la norma 41 de las Normas federales de enjuiciamiento criminal.

no estaría sujeta a dicha confidencialidad. Además, existen excepciones, entre las que se incluye la excepción de confidencialidad por intenciones fraudulentas, que se aplica en situaciones en las que es posible que un abogado esté involucrado en un delito o preste asesoramiento sobre cómo cometerlo, como aconsejar a un cliente corporativo cómo participar en acuerdos de precios.¹⁵

23. En la práctica, la protección de la confidencialidad entre los abogados y sus clientes implica que, si tenemos algún motivo para creer que entre los materiales incautados hay documentos que pueden ser confidenciales, la División tomará medidas para eliminar dichos documentos de la recopilación de material incautado antes de que el equipo de investigación pueda revisarlos. Este proceso se puede llevar a cabo de distintas maneras. La División puede realizar su propia revisión de documentos potencialmente confidenciales a través de un equipo de abogados que sean independientes del equipo de investigación, que, en ocasiones, reciben el nombre de «equipo de filtrado». El equipo de filtrado separará cualquier material potencialmente confidencial y, a continuación, proporcionará al equipo de investigación acceso al resto de materiales que no incluyan ese tipo de información. Como alternativa, el abogado de la empresa o del particular podrá llevar a cabo la revisión de materiales confidenciales tras la incautación y antes de que el equipo de investigación revise los materiales incautados. El equipo de investigación solo revisará los materiales que el abogado de la empresa o del particular considere no confidenciales.

24. El secreto profesional también es un aspecto fundamental en el contexto internacional. La globalización de la aplicación de la normativa sobre cárteles plantea cuestiones sobre la forma de abordar la confidencialidad entre los abogados y sus clientes, y presenta problemas difíciles a la hora de conciliar las tradiciones del derecho civil y el derecho anglosajón. Muchas jurisdicciones de derecho civil que no reconocen la confidencialidad entre los abogados y sus clientes han promulgado normas reglamentarias de confidencialidad que prohíben a los abogados divulgar información confidencial que el cliente les haya facilitado. No obstante, a menudo esto se aplica solo al abogado y no al cliente, y es posible que se refiera únicamente al abogado externo. En consecuencia, es posible que una inspección sorpresiva de las oficinas del cliente o una solicitud de documentos dirigida al cliente y no al abogado no proporcionen ningún tipo de protección con respecto a la información confidencial del cliente. Aunque este enfoque era viable en una época en la que los clientes visitaban las oficinas de su abogado para proteger el asesoramiento y el intercambio de información, en un mundo de comunicación digital y empresas globales, se trata de una laguna fundamental en la protección de la confidencialidad. La División apoya la labor encaminada a establecer unas prácticas comunes con respecto a la confidencialidad entre los abogados y sus clientes con el fin de impulsar las normas fundamentales del debido proceso.¹⁶

25. *Técnicas forenses y cifrado.* A la hora de incautar pruebas en formato digital, es importante recordar que los ordenadores y otros dispositivos no solo contienen archivos, carpetas y aplicaciones a los que el usuario accede. El análisis forense de un dispositivo revelará los metadatos y otros artefactos que pueden proporcionar información útil sobre cómo se ha utilizado un dispositivo, cuándo se ha accedido a los archivos y cuándo se han

¹⁵ *Clark v. United States*, 289 U.S. 1, 15 (1933) («La confidencialidad desaparece cuando la relación presenta un abuso. Si un cliente consulta a un abogado para obtener un asesoramiento que le ayude a cometer un fraude, no tendrá ninguna ayuda desde el punto de vista legal»).

¹⁶ Véase Departamento de Justicia de los EE. UU., Roger Alford, asistente adjunto del fiscal general. *Observaciones del acto celebrado en la Universidad Nacional Autónoma de México (UNAM) bajo el patrocinio de la Comisión Federal de Competencia Económica (COFECE)* (Ciudad de México, México, 30 de mayo de 2018), <https://www.justice.gov/opa/speech/file/1066916/download>.

modificado, el historial de búsqueda de Internet, la conexión de dispositivos de almacenamiento USB y otros rastros de información que indican cómo utiliza el dispositivo una persona. Este tipo de información forense puede resultar útil para demostrar conocimientos o intenciones, para corroborar declaraciones de testigos y para contrarrestar las afirmaciones de los acusados de que no tenían conocimiento ni control sobre determinados documentos o espacios de red compartidos. Cabe señalar que un registro forense también puede revelar información contenida en la memoria de un ordenador que puede resultar de ayuda a un organismo para descifrar un dispositivo cifrado. Este tipo de análisis forenses pueden llevar mucho tiempo y deben realizarse de acuerdo con los expertos en análisis forense certificados especialmente formados en la manipulación de datos recopilados mediante técnicas forenses.

26. *La importancia de la planificación previa a la incautación.* La ejecución de un registro que implique la incautación de pruebas en formato digital exige prestar una atención rigurosa a las cuestiones jurídicas mencionadas anteriormente. Asimismo, los registros presentan numerosos desafíos prácticos. La revisión de dispositivos incautados o imágenes forenses de medios digitales para determinar qué elementos están dentro del alcance de la orden y qué materiales pueden ser confidenciales requiere tiempo. El tratamiento y la carga en bases de datos de revisión de grandes volúmenes de pruebas en formato digital requieren tiempo. Según la experiencia de la División, la clave para abordar de manera eficaz estos desafíos jurídicos y prácticos es la planificación previa a la incautación y la comunicación entre el personal jurídico que dirige el caso, el organismo encargado de hacer cumplir la ley que ejecuta el registro y el personal de apoyo a la litigación de la División. En estas conversaciones de planificación previas a la incautación, el personal jurídico y de apoyo a la litigación de la División y el organismo encargado de la incautación pueden colaborar para, entre otras cosas, elaborar estrategias de registro más específicas que permitan tratar un volumen menor de materiales, debatir el calendario de los registros y la organización de los materiales, elaborar un sistema de seguimiento y registro de los bienes incautados, y diseñar un plan para manipular materiales confidenciales.

4. Conclusión

27. Aunque en este documento se exponen algunos de los regímenes jurídicos básicos de los EE. UU. que regulan la recopilación de pruebas en formato digital, es importante tener en cuenta que este ámbito de la ley se encuentra en constante evolución. Dado que la tecnología avanza rápidamente y la forma en la que las personas interactúan con ella y la utilizan en su vida cotidiana continúa cambiando, seguirán existiendo desafíos con respecto a las leyes y los precedentes jurídicos que establecen el modo y los casos en los que los organismos estadounidenses encargados de hacer cumplir la ley pueden acceder a los correos electrónicos, los mensajes de texto y otras comunicaciones en formato digital de una persona. La División cuenta con fiscales penales nombrados como especialistas en delitos informáticos, quienes controlan los cambios en este ámbito del derecho y proporcionan formación, orientación y apoyo a otros abogados y miembros del personal. Tal y como se ha mencionado previamente, la División también cuenta con personal específico de apoyo a la litigación que trabaja para adaptar las prácticas de la División a los nuevos avances en la esfera de la tecnología y el derecho. Dado que las autoridades de competencia de todo el mundo trabajan para adaptarse a estos nuevos desafíos, la División espera compartir experiencias con nuestros socios internacionales y aprender de ellos.